Available online at www.elixirpublishers.com (Elixir International Journal)

Electrical Engineering

Elixir Elec. Engg. 108 (2017) 47622-47627

ISSN: 2229-712X

SRTURP: Secure Routing Through Unobservable Routing Protocol for Mobile Ad-Hoc Networks

Santhosh Gupta Dogiparthi , Jagadeesh Thati and V. Anil Kumar
Assistant Professor, Department of ECE ,Tirumala Engineering College, Jonnalagadda, Narasaraopet.

ARTICLE INFO

Article history:
Received: 3 June 2017;
Received in revised form:
30 June 2017;
Accepted: 11 July 2017;

Keywords
Privacy-preserving Routing,
Unobservability,
Id-based encryption.

ABSTRACT

A mobile ad hoc network consists of mobile nodes that communicate in an open wireless medium. Adversaries can launch analysis against the routing information embedded in the routing message and data packets to detect the traffic pattern of the communications; thereby they can obtain the sensitive information of the system, like the identity of a critical node. Privacy-preserving routing is crucial for some ad hoc networks that require stronger privacy protection. A number of schemes have been proposed to protect privacy in ad hoc networks. However, none of these schemes offer complete unlinkability or unobservability properties since data packets and control packets are still linkable and distinguishable in these schemes. In this paper, we define stronger privacy requirements regarding privacy-preserving routing in mobile ad hoc networks. Then we propose an unobservable secure routing scheme Secure Un-Obseravable Routing Protocol to offer complete unlinkability and content unobservability for all types of packets. On- Demand secure Routing protocol is efficient as it uses a novel combination of group signature and ID-based encryption for route discovery. Security analysis demonstrates that SRTURP can well protect user privacy against both inside and outside attackers. This Secure Routing Protocol is implemented on ns2, and evaluated its performance by comparing with Ad-hoc On Demand Distance Vector and MASK. The simulation results show that SRTURP not only has satisfactory performance compared to Ad-hoc On Demand Distance Vector, but also achieves stronger privacy protection than existing schemes like MASK.

Introduction

Mobile Ad Hoc Network is a network in which a set of mobile nodes communicate directly with one another without using an Access Point (AP) or any connection to a wired network. The nodes are free to move randomly and organize themselves arbitrarily. Every node communicates via wireless radios that have limited transmission efficiencies. Due to this limitation on transmission, not all nodes are within the transmission range of each other. If a node wants to communicate with another node outside its transmission range, it's mandatory that it needs the help of other nodes in building up a multi-hop route. An important challenge in MANET is that, communication has to be made possible by changing network topology due to node mobility. Despite all its advantages, mobile ad hoc network has the potential vulnerability by means of misbehaving nodes. A node can misbehave and fail to establish route or route the data due to its malicious nature to disrupt the network and take control of the system. Misbehaving deeply impacts a node's anticipation of other's behaviour anddecisions during interaction.

The contribution of this paper is:

•A thorough analysis of existing anonymous routing schemes and demonstrate their vulnerabilities.

• To analyze the routing protocols based on mobility models.

• To reduce the effect of attackers.

• To develop the authentication based security scheme in the network.

• To compare the performance of routing protocols in terms of the delivery ratio.

Security Goals Of Ad Hoc Networks

Anonymity: In a set of anonymous nodes the ability to stay away from being identified is called anonymity.

Unlinkability: The ability to maintain contents of the message being unlinkable by the adversary is called unllinkability.

Unobservability: The ability to maintain item of interest in indistinguishable state of their presence or absence, to all unrelated subjects.

So far a number of schemes for secured routing scheme are proposed by different researchers, every researcher concentrated mainly on the anonymity and unlinkability. But they achieved only partial anonymity and unlinkability. But due to partial nature some of the contents like packet type, sequence number etc can be acquired by the adversary. Using this information of sequence number there are chances for the adversary to reconstruct or trace back the original data by aligning them in order. On the other hand, by acquiring the type of packet and the sequence number will make the content to be observable.

To focus on, unllinkability is not alone is not enough in hostile environments as important information will be available to the attackers.

Tele:
E-mail address: gupta4512@gmail.com

Table 1. Comparison Of Anonymous Routing Protocols.

	cryptosystem	Sender anonymity	Receiver anonymity	Observable info.
ANODR	One time PKC	yes	yes	Sequence no., trapdoor info., RREQ/RREP tag
ASR	One time PKC	yes	Yes	Sequence no., trapdoor info., RREQ/RREP tag
ARM	One time PKC	Yes	yes	Trapdoor info., RREQ/RREP tag
AnonDSR	One time PKC	Yes	yes	Trapdoor info., RREQ/RREP tag
ARMR	One time PKC	Yes	Yes	RREQ/RREP tag
SDAR	Long-term & One time PKC	Yes	Yes	Trapdoor info., RREQ/RREP tag
ODAR	Long-term & One time PKC	Yes	Yes	Trapdoor info., RREQ/RREP tag
ALARM	Long-term PKC	Yes	Yes	RREQ/RREP tag,location
PRISM	Long-term PKC	Yes	Yes	RREQ/RREP tag, location
MASK	One time pairing	yes	NO	RREQ ID,Dest ID

Using this passive attacker can analyse traffic based on packet type. It is needed to maintain the traffic completely unobservable to the outside attackers by allowing them to receive some random noises.

The need for providing hint which specifies the key that should be used to decrypt will demand a careful design to remove linkability. Another drawback of most systems is that they heavily rely on public key cryptography, and thus incur a very high computation overhead.

Of the requirements specified above unobservability is the strongest as it provides us with both anonymity and unllinkability. So in this paper we concentrate mainly on unobservability. The routing scheme proposed should provide unobservability for both content and traffic pattern. Hence it is refined into two types: 1)Content unobservability, which refers to un-extractable content of any message. 2) Traffic pattern unobservability, referring to no useful information can be obtained from frequency, length and source destination patterns of message traffic. In this paper we mainly focus on content unobservability, which is orthogonal to traffic pattern unobservability to achieve truly unobservable communication.In this paper, we propose a routing scheme called SRTURP using which we can obtain content unobservability through the use of anonymous key. The unobservable routing scheme is executed in two phases after each node in the group are provided with a group signature signing key and ID based private key using an offline key server or by using a key management scheme available. The first phase deals with the construction of secret key between the nodes. Then the second phase starts to search for routes available to contact the destination node.

Through this paper we mainly contribute 1) A thorough analysis of existing schemes and their vulnerabilities. 2) Complete picture of the proposed scheme to a level of our best knowledge. 3) Comparison of proposed system with the previous existing schemes. 4) A graphical images generated using ns2 for comparison of proposed scheme and AODV.

II Related Work

So far a number of schemes are proposed for ad-hoc networks in recent years, of which most of them mainly rely on the PKC (Public Key Cryptosystem) to achieve anonymity and unlinkability. But PKC will not just provide a better support for privacy protection but also brings in a significant overhead.

ANODR is the first to propose anonymity and unlinkability for routing in ad-hoc networks. This scheme uses one time PKC for communication. It provides both sender and receiver anonymity. But fails to provide security for the contents like sequence number, trapdoor information and also the type of packet that is travelling in the system(i.e. whether it is RREQ/RREP packet).

Then came another scheme ASR which is similar to ANODR, which also use one time PKC and maintains both sender and receiver anonymity. Even this scheme leak contents leaked while using ANODR.

There came algorithms ARM and AnonDSR which use onetime PKC, maintain sender and receiver anonymity. These algorithms proposed a better security which hides the sequence number of the packets. But these algorithms are also prone to leak some information like trapdoor information and RREQ/RREP tags.

Following ARM another algorithm called ARMR came into existence which further provides security to trapdoor information along with sequence number. But this algorithm also failed to provide security to packet tags RREQ/RREP.

Then the algorithms SDAR and ODAR were proposed. These algorithms use a onetime but long term PKC. Even though these provide sender and receiver anonymity these algorithms failed to provide content unobservability for trapdoor information and packet tags. To overcome this problem of leakage of trapdoor information another algorithm ALARM followed by PRISM were proposed. These use a long term PKC and also provide sender and receiver anonymity. Along with sequence number trapdoor information was made secured. But these fail to provide security to packet tags and location of the sender or receiver are observable.

Then came another algorithm called MASK which uses onetime PKC to provide sender anonymity. But this algorithm fails to maintain receiver's anonymity as its packet tag and destination id are observable to the intermediary nodes. Table1 provides comparison of all anonymity based routing schemes in existence.

III. SRTURP: An Unobservable Routing Scheme

We present an efficient unobservable routing scheme for ad hoc networks in this section. Both the control and data packets are made to look indistinguishable from dummy packets for the outside attackers. Using this algorithm in the network only valid nodes in the network can decrypt the entire information present in the packet. The main intuition behind this scheme is "a node present in the network will establish a unique key with all the neighbouring codes before moving to data exchange phase". Hence when a packet is broadcasted from the node all the neighbouring nodes try to find whether that packet is intended for them or not using their pairwise key established with that node. For the nodes to support both unicast and broadcast they need both the group key and pairwise key. This result SRTURP to comprisesof 1)anonymous key establishment and 2) unobservable route discovery.This routing scheme aims to offer the following privacy properties.

Anonymity: All the nodes (i.e. sender, receiver and intermediate nodes) should not be identifiable within the whole network.

Unlinkability: No two items of interest and messages should linkable by the outside attackers. Even the information that two messages belong to the same node should be unidentifiable.

Unobservability: Packets broadcasted or unicasted in the network should not be distinguishable from dummy packets to the outsider. Not just the content of the packet but also the packet header like packet type are protected from eavesdropper. It is only the pseudonym identities that should be available to the other nodes about the particular nodes in action (i.e. sender receiver and intermediary nodes).

A. Assumptions, System Setup and Attack Model

Assumptions**:** we use the same assumptions and definitions as proposed by the researchers of the schemes group signature and id based encryption. We mainly use the Diffie-Hellman key exchange scheme to exchange the private encryption key between nodes in action. Both the group signature and ID-based schemes are based on the pairing of elliptic curve groups of order of a large prime (e.g. 170 bit long), so that they have same security strength as the 1024 bit RSA algorithm.

System Setup: We consider an ad-hoc network consisting n nodes with same communication range and each node can move around within the network. A node can communicate with the nodes outside its range through the nodes within its range (i.e. sender node communicate with nodes that which can provide a route to the destination node). We avoid physical addresses like MAC addresses in data frames to stay off from their identification.

Before an ad-hoc starts up, by following the group signature scheme, we use a key server which generates a group public key Gpk which is publicly known by everyone, and we use this server to generate a private group signature key gsk_x for each node x. Hence a group signature scheme ensures full anonymity, which means a signature does not reveal the signer's identity but everyone can identify its validity.

Attack Model: To find the perfection of any model one needs to use an adversary model, assuming which one can verify that the proposed scheme will overcome the problems that may arise with that adversaries affect. For this purpose we also consider an adversary who can monitor and record content, time and size if each packet sent over the network, and we also consider that they can analyze the obtained information to find who is sending to whom etc. We also consider that the adversary can attack afar and nearby, e.g. injecting, modifying and dropping packets within the network. An adversary cannot attract large amounts of network traffic using a wormhole attacks. To make his attacks more successful an adversary needs to compromise one or more nodes, but each node will have an uncompromised node after node attack. To overcome this adversary tries to break the aforementioned privacy properties. We assume that the adversary has only bounded computation capability, as we use a Diffie-Hellman key exchanging scheme which will not allow the adversaries to find the apt key used in encryption.

B. The Unobservable Routing Scheme

This unobservable scheme comprises of two phases 1) Anonymous key establishment, in which we construct a set of session keys with neighbouring nodes anonymously.

2) We initiate the route discovery process using the protected session keys. The notations used to deal with these two phases are listed in the table2 below.

Table 2. Notations.

A	A node in the ad hoc network, and its real identity
S	The master secret key owned by the key server
Q	A 170-bit prime number
P	Generator of the elliptic curve group G1
Hi(*)	Secure one-way hash functions, *i* = 1, 2, 3 †
gsk_A	Node *A*'s private group signature key
Gpk	The public group signature verification key
K_A	Node *A*'s private ID-based key which is $s \cdot H1(A)$
EA(*)	ID-based encryption using *A*'s public key
K_{A*}	A local broadcast key within *A*'s neighbourhood
K_{Ax}	A pairwise session key shared between *A* and *X*
Nym_A	The pseudonym only valid within *A*'s neighbourhood
Nym_{Ax}	The pseudonym shared between *A* and

1) Anonymous Key Establishment: In this phase we generate unique session keys with each and every neighbouring node in the range of sender node. Prior to this in the available group of nodes one of the node is selected as leader node and the rest of the nodes in the group act as normal nodes. This leader node generates a key to the group signature key and it shares that key with all its neighbours. And each node will also hold a private group key which will further be used in the future. Let us see how these keys are established between the nodes using the example shown in Fig1.

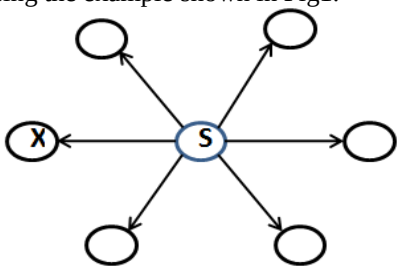

Fig.1. Anonymous key establishment. S broadcasts the first message to its direct neighbours. Each of S's neighbours does the same thing as X does to learn S's local broadcast key $K_{sx} = H_2(r_s r_x P)$.

For anonymous key establishment procedure, S does the following:

1) S generates a random number $r_S \in Z_q^*$ using which we compute the group signature key using the expression $SIG_{gsk_S}(r_S P)$. Where P is the generator of G1. It then broadcasts $\langle r_S P, SIG_{gsk_X}(r_S P)\rangle$ to its neighbours.

2) Immediately after the reception of message X verifies the signature in the message. If the key matches it chooses its own random number $r_x \in Z_q^*$ and computes $r_x P$. Now X also computes group signature using the expression $SIG_{gsk_X}(r_x P)$ using its own signing key gsk_X. After this X computes the session key $K_{sx} = H_2(r_s r_x P)$. And then replies S with a message $\langle r_x P, SIG_{gsk_X}(r_s P | r_x P), E_{k_{sx}}(k_{x*} | r_s P | r_x P)\rangle$ Where $\bar{K}_{X*}$ is X's local broadcast key.

3) After receiving reply from X, S verifies the signature inside the message. If it is valid it starts to compute the session key between the node X and itself as $K_{sx} = H_2(r_s r_x P)$.

4) S then generates its own local broadcast key $\bar{K}_{s*}$, and sends the message holding $E_{k_{sx}}(\bar{k}_{s*} | \bar{k}_{x*} | r_s P | r_x P)$ to X.

5) X upon receiving the message from S computes the session key $K_{sx} = H_2(r_s r_x P)$ it then decrypts the message to get the local broadcast key $\bar{K}_{s*}$.

The key establishment protocol used is designed following the principle of KAM which employs Diffie-Hellman key exchange and secure MAC code.

This will prevent replay attacks and session key disclosure attacks; meanwhile it achieves key conformation for established session keys. KAM has been proved to be secure under the oracle Diffie Hellman assumption and hash Diffie Hellman assumption.

2) Privacy Preserving Route Discovery: This phase mainly relies on the keys established in the previous session. Like the normal routing schemes this also comprises of route request and route reply processes. The route request message is a broadcast message but the route reply message is a unicast message as it knows the source node. Let us consider an example like as shown in figure 2 where a node S needs to find a route to the node D, where there are several intermediary nodes present in the route.

RREQ (Route Request): S uses the random number chosen in the previous session and also uses the identity of the node D to encrypt trapdoor information that only can be opened with D's private ID-based key, this yields $E_D(S,D,r_S P)$ then S chooses another random number N_S as route pseudonym (Nym). And then S chooses a Nonce (number used once) and calculates the pseudonym as $Nym_S = H_1(\bar{k}_{S*}|Nonce_S)$. Each entry maintains a temporary entry (like sequence number, pseudonym of previous and next nodes, previous and next hops details). But as no node knows the real identity of its upstream and downstream node the temporary entry table will hold (sequence number,-,N_S, -,-). Using the session keys available it sends a route request to its neighbours.

$Nonce_S, Nym_S, E_{KS*}(RREQ, N_S, E_D(S,D,r_S P), seqno)$

Upon receiving this message from S node A will try all its session keys, if any key turns to be true it sees whether it is intended for it, if it turns true it decrypts the data using its ID (as the data will be encrypted using destination nodes ID), else it will forward the information by broadcasting it to all its neighbours using pseudonym ID's. This process continues until it is reached to D. At node D it identifies that the message is intended for that and then decrypts the data using its ID. Then D updates its route table entry record by <seqno,N_C, −, C, −>.

Table 3. Route table for all nodes in the example: each node is provided with one row that belongs to the process that took place.

	Seqno	P_RNym	N_RNym	Prev_Hop	Next_Hop
S	seqno	-	N_S	-	k^*_A
A	seqno	N_S	N_A	k^*_s	k^*_B
B	seqno	N_A	N_B	k^*_A	k^*_C
C	seqno	N_B	N_C	k^*_B	K^*_D
D	seqno	N_C	-	k^*_C	-

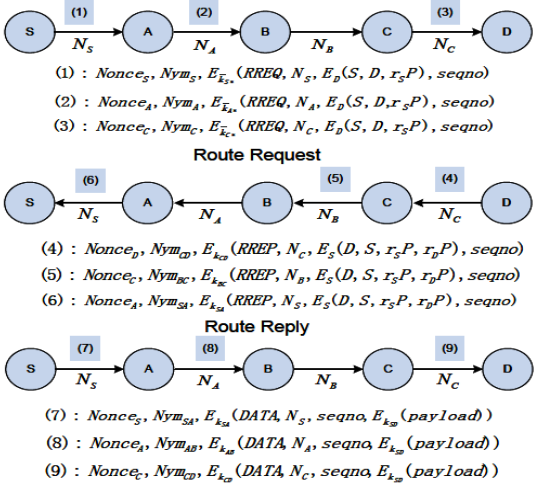

Fig.2. Route Request, Route Reply and Data Packet Transmission.

RREP (Route Reply): After receiving the route request message D replies back to S conforming that it is ready to exchange data. This will be a unicast message. This message will pass through all the available routes to reach S. First the message packet will be passed to node C using the session keys established between them and the message format will be

$Nonce_D, Nym_{CD}, E_{K_{CD}}(RREP, N_C, E_S(D, S, r_S P, r_D P), seqno)$

Upon receiving this message C node verifies the sender of the message by evaluating the pseudonym acquired. Then it verifies the route to which this reply is intended to by evaluating route pseudonym N_C and sequence number. C then searches its routing table and modifies the temporary entry<seqno,N_B,N_C,B,−> into<seqno,N_B,N_C,B,D >. After this C chooses a new nonce and computes the respective Nym shared between B and C. It then generates a message holding the content

$Nonce_C, Nym_{BC}, E_{K_{BC}}(RREP, N_B, E_S(D, S, r_S P, r_D P), seqno)$

This process continues till the reply reaches back to S. Upon receival of this message S decrypts the cipher text using the right key K_{SA} and verifies that the function is composed faultlessly. Then it updates its temporary route table entries as $< seqno, -, N_S, -, - >$ into $< seqno, -, N_S, -, A >$. The final route table for each node is shown in table 3 below.

Unobservable Data Packet Transmission: Once after the security session keys are established between the sender and receiver and a route is made available for further transmission of data the data packets will be transmitted. These data packets are encrypted using the pseudonyms and keys. Hence here s starts the communication by sending the packet

$Nonce_S, Nym_{SA}, E_{K_{SA}}(DATA, N_S, seqno, E_{K_{SD}}(payload))$

Further the same operation will be continued by the intermediary nodes after verifying the route using the pseudonym and seqno. And all the intermediary nodes will make use of new pseudonyms andnonces. When the message reaches the destination node D it decrypts the message using the ID of its own.

Ivsecurity and Private Metric Analysis

The security analysis of this protocol can be verified by the way that how it fulfils the requirements.

Anonymity: User anonymity is implemented by group signature which can be verified without disclosing anyone's identity. Group signature is what is used to establish session keys between neighbouring nodes, so that they can authenticate each other anonymously. And subsequent routing discovery procedure is built above these session keys. Hence SRTURP fulfils the anonymity requirement under both passive and active attacks, as far as the group signature is secure.

Unlinkability: Let's consider the three types of packets. In these packets, they are identified by pseudonyms which are generated from random nonce along with secret session keys. The nonces and pseudonyms are never reused, they are used only once. Exception of that of the random nonce and the pseudonym, the remaining part of the message, which includes the trapdoor information in the route request, is decrypted and encrypted at each hop. Hence even for global adversaries who can eaves drop every transmission within the network, it is impossible for him to find linkage between messages without knowing any encryption key.Hence unlinkability is achieved

Unobservability: In SRTURP RREQ, RREP and data packets are indistinguishable from dummy packets to a global outside adversary.

Also, the nodes involved in the routing procedure are anonymous to other valid nodes. Consequently, SRTURP provides unobservability as defined for ad hoc networks. First of all, a global adversary cannot distinguish different packet types, and neither can he distinguish a meaningful cipher text from random noise. Moreover, the nonce is chosen randomly by any node and never reuses it. The nonce is updated each time after it is used, so there is no linkage between the pseudonyms which are calculated from nonces. Only those mobile nodes with a valid session key can recognize valid pseudonyms and decrypt the corresponding cipher texts to obtain meaningful plaintexts from them. Hence unobservability is achieved.

Node Compromise: Node compromise is easy for the Adversary and highly possible in ad hoc networks, hence it is crucial for a privacy-preserving routing protocol to withstand security attacks due to node capture. Suppose a node is compromised by an attacker, his private signing key and ID-based encryption key are disclosed to the attacker. The attacker now is able to establish keys with neighbouring nodes, but only the following information can be obtained by the attacker:

1) The type of a received packet 2) Data or RREP packets sent to or via the compromised node 3) The headers of the packets relayed by the compromised node 4) RREQ packets sent from the compromised node's neighbours. The attacker is not able to gain more beyond this information.

Attacks

Collusion Attacks: For the intruding outsiders, privacy Information is completely protected with SRTURP. As the attacker is unable to distinguish a meaningful packet from a dummy Packet, SRTURP can provide complete protection for privacy with an appropriate traffic padding technique. Even if the target node is encompassed by more than one attack node, given the assumption that no node is totally surrounded by compromised nodes, the attacker is unable to perceive anything except some random dummy packets. If appropriate dummy traffic is injected into the network, the colluding outsiders cannot gain any privacy information about the network at all. For the colluding insiders, SRTURP still offers unobservability as promised. Though information disclosure is unavoidable for colluding insiders, and the adversary knows a few keys, and the information that the colluding insiders can gain is largely restricted by SRTURP.

Sybil Attacks: In the Sybil attack, a single node presents multiple fake identities to other nodes in the network. Sybil attacks are subjected to a great threat to decentralized systems like Peer-to-Peer networks and geographic routing protocols. In SRTURP, the centralized key server generates group signature signing keys and ID-based keys for network nodes. Thus, it is impossible for the adversary to obtain other valid identities except the compromised ones. Nevertheless, the anonymity feature of SRTURP allows the adversary to launch Sybil attacks which are similar to collusion attacks discussed above. SRTURP is able to count such attacks effectively.

V. Implementation and Performance Evaluation

Network performance refers to the service quality of a communications product as seen by the customer. There are different ways to measure the performance of a network, as each network is different in nature and design.

1) Packet delivery ratio: The ratio of the number of delivered data packet to the destination. This illustrates the level of delivered data to the destination.

2) Packet delivery latency: The time a packet takes to traverse a system is called packet delivery latency.

Result:

In this paper, we analyzed network parameters such as packet delivery latency and packet delivery ratio. Result shown fig 3 is packet delivery ratio, the graph shown in fig 4 is packet delivery latency graph, and from these results we can know SRTURP has more latency than normal AODV.SRTURP performance is better than normal AODV even latency is more; the reason is security of SRTURP is very high so latency is ignorable in this case.

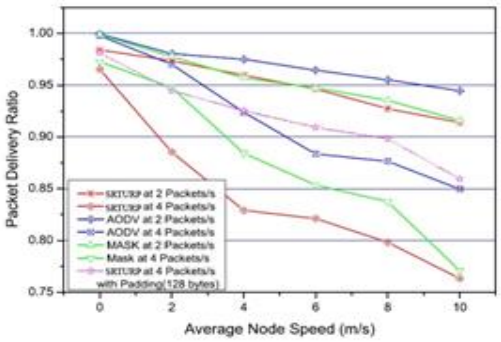

Fig.3. Packet Delivery Ratio.

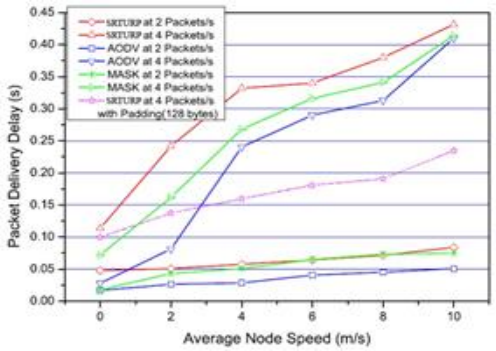

Fig.4. Packet Delivery Latency.

VI. Conclusion and Future Work:

The scheme proposed in this paper uses ID based encryption and group signature to provide security. From the analysis, it is also proved that the proposed scheme SRTURP provides a stronger protection with complete unlinkability and content unobservability for ad-hoc networks and it is also proved that, this scheme not only provides better security but also provides a high resistance against the attacks due to node compromise. We implemented the protocol using ns2 and examined its performance, which proved that this scheme has satisfactory performance in terms of packet delivery ratio, latency and normalized control bytes.

The areas like shielding against the DoS and Wormhole attacks need to be implemented in future as the proposed scheme SRTURP cannot resist against these attacks.

References

[1] J. Kong and X. Hong, "ANODR: aonymous on demand routing with untraceable routes for mobile ad-hoc networks," in Proc. ACM MOBIHOC' 03, pp. 291–302.

[2] Pfitzmann and M. Hansen, "Anonymity, unobservability, and pseudonymity: a consolidated proposal for terminology," draft, July 2000

[3] Y. Dong, T. W. Chim, V. O. K. Li, S.-M. Yiu, and C. K. Hui, "ARMR: anonymous routing protocol with multiple routes for communications in mobile ad hoc networks," Ad Hoc Networks, vol. 7, no. 8, pp. 1536–1550, 2009.

[4] L. Song, L. Korba, and G. Yee, "AnonDSR: efficient anonymous dynamic source routing for mobile ad-hoc networks," in Proc. 2005 ACM Workshop on Security of Ad Hoc and Sensor Networks, pp. 33–42.
[5] S. Seys and B. Preneel, "ARM: anonymous routing protocol for mobile ad hoc networks," in Proc. 2006 IEEE International Conference on Advanced Information Networking and Applications, pp. 133–137.
[6] Y. Zhang, W. Liu, and W. Lou, "Anonymous communications in mobile ad hoc networks," in 2005 IEEE INFOCOM.
[7] I. R. Jeong, J. O. Kwon, and D. H. Lee, "A Diffie-Hellman key exchange protocol without random oracles," in Proc. CANS 2006, vol. LNCS 4301, pp. 37–54.
[8] 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 Proc. 2004 IEEE LCN, pp. 618–624.
[9] Z.Wan, KuiRen and Ming Gu, "USOR: unobservable on-demand routing protocol for mobile ad-hoc networks" in 2012 IEEE Trans. Wireless communication, vol. 11, no.5, pp. 1922-1932.
[10] D. Sy, R. Chen, and L. Bao, "ODAR: on-demand anonymous routing in ad hoc networks," in 2006 IEEE Conference on Mobile Ad-hoc and Sensor Systems.
[11] K. E. Defrawy and G. Tsudik, "ALARM: anonymous location-aided routing in suspicious MANETs," IEEE Trans. Mobile Comput., vol. 10, no. 9, pp. 1345–1358, 2011.
[12] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in Advances in Cryptology–Crypto'01, Lecture Notes in Computer Science, vol. 2139, 2001, pp. 213–229.

Mr.Santhosh GuptaDogiparthi received his B.Tech (ECE) degree from Amara Institute of Engineering and technology affiliated to JNTU, Kakinada and M.Tech (DSCE) degree fromNarasaraopeta Engineering College, Narasaraopet, Guntur District, Andhra Pradesh, India.Presently , Working as an Assistant Professor since December 2014 in Tirumala Engineering College, Jonnalagadda. His area of interests include Image Processing, Embedded Systems and Communications.

Mr.JagadeeshThati is currently working as Associate Professor in Department of ECE at Tirumala Engineering College, Jonnalagadda, Narasaraopet, Guntur (dt). He has worked as dasa5 developer in Dasa Control systems AB Hammerdalsvgen 3, SE-352 46 Vxjo, Sweden. He did his MS from BTH, Sweden. He has published 23 international journals, 8 international conferences and two Books. He has appointed as reviewer for various journals.

He has professional memberships in IETE and ISTE.He received best Teacher award from Tirumala Engineering College in 2012. His areas of Interests are Signal Processing, Digital Image Processing, Computer Vision, Neural Networks and Nano Technology.

Mr. V. Anil Kumar received his B.Tech (ECE) degree from Nalanda Institute of Engineering and technology affiliated to JNTU, Kakinada and M.Tech (CSP) degree fromBapatla Engineering College, Bapatla, Guntur District, Andhra Pradesh, India.Presently, Working as an Assistant Professor since June 2015 in Tirumala Engineering College, Jonnalagadda. His area of interests include Smart Antenna, Communications, Signal and Image Processing.