Secure Key Sharing in Mobile Ad hoc Network using Content Invisibility Scheme

A. JEGATHEESAN
Assistant Professor, Department of Information Technology
Cape Institute of Technology, Levengipuram, Tamilnadu
INDIA
jegatheese@gmail.com

D. MANIMEGALAI
Professor and Head, Department of Information Technology
National Engineering College, Kovilpatti, Tamilnadu
INDIA
megalai_nec@yahoo.co.in

Abstract: In mobile ad hoc network (MANET) privacy protection and efficient use of memory is a challenging task due to mobile and dynamic behavior. Existing schemes provides anonymity, unlinkability and unobservability, but they consume more memory space and also result in computation overhead and communication delay. In our proposed scheme, key is established only between neighbors, which reduce memory storage, computational overhead and communication delay. In our scheme, ID Based Encryption is proposed. By using this scheme we can overcome the internal and external attacks. Also we achieve privacy in terms of anonymity, unlinkability and unobservability.

Keywords: Security, Hash function, Key Exchange, Authentication, MANET, ID-Based Encryption

1. Introduction

Mobile Ad hoc Network (MANET) is a rapidly growing technology which is considered to be the future network. It is a decentralized network which is built spontaneously as devices connect in network. Rather than relying on a base station to coordinate the flow of messages to each node in the network, the node itself forwards and receives packets with other nodes. It does not require a router or a wireless base station. The nodes within a range communicate with each other using radio waves and if the node is outside the range, using multi hop transmission principle data packets relay on sequence of intermediate node. The communication between these mobile nodes is carried out without any centralized control [1]. This network can be used in the fields where infrastructure is unavailable or unreliable such as military battlefield, undersea operations and rescue operations .

Privacy preserving of MANET is exigent than that of wired due to its mobility and dynamic behavior. Privacy is achieved in terms of anonymity, unlinkability and unobservability [2]. A number of privacy preserving routing schemes that depend on public key cryptography has been proposed whereas they provide only anonymity and partial unlinkabilty. Anonymity is of three types i) Identity Anonymity ii) Route Anonymity and iii) Location Anonymity which are achieved in existing schemes but information like packet type, sequence number are exposed to attackers which breaks unlinkability and unobservability. However, unlinkability is achieved by providing stronger decryption in encrypted packet which incurs high computation overhead and cost. Among these requirements unobservability is strong which indirectly achieves both anonymity and unlinkability. Unobservability is of two types i) Content Unobservability ii) Traffic Pattern Unobservability. Traffic pattern unobservability is achieved in the existing systems whereas whole content protection of packet is not achieved yet.

In our work, to reduce memory storage and computational overhead, the key is established only to the neighbor. As keys are established between only the neighbors, the communication delay is reduced. Also we achieve privacy in terms of anonymity, unlinkability and unobservability.

The rest of the paper is organized as follows. In the next section existing routing schemes for mobile ad hoc networks are discussed. Section 3 discuss about Content Invisibility Scheme for mobile ad hoc networks. In section 4 implementation and performance evaluation of Content Invisibility scheme is presented. Finally conclusion is drawn in section 5.

2. Related Work

Many routing schemes are already existing which provide privacy to ad hoc network. Most of them provide only anonymity and partial unlinkability.

In ANODR [3] trapdoor information are broadcasted, which provides route anonymity and location privacy. It meets untracebility by following route pseudonymity approach,in which nodes share route pseudonyms. During route discovery phase, onion routing is used which provides unlinkability, at the same time it exposes information to the intermediate nodes. As the packets are publicly labeled, it violates the rule of unobservability. In onion routing, each intermediate node has to create one time public/private key to encrypt/decrypt, which need tedious computation and generates high cost.

A pairing based cryptosystem is used in MASK [4] where neighborhood node authenticates each other using dynamically changing pseudonyms. It is very expensive to engender adequate pair of secret points and pseudonyms and also it depends on public key cryptosystem. Even though MASK is resistant to passive adversaries, an active adversary can easily link RREQ packets as destination identity is clearly mentioned in it.

Anonymous Routing Protocol for Mobile Ad hoc Networks ARM [5] make use of probabilistic padding and TTL scheme in which node in the network will not be able to determine which node is communicating. ARM achieves anonymity by making use of one time public/private key [6] which produce computation overhead and high cost. The passive adversary can identify the source of fresh message which provides observability.

To facilitate complete anonymity of nodes, links and source routing paths ODAR [6] scheme is proposed which make use of bloom filters. It is advantageous than ARM because it makes use of long term public/private key. As the entire packets are not protected with session key in ODAR, it provides only anonymity but not unlinkability.

PRISM [7] provides protection against both active and passive adversaries. By using group signature scheme and AODV protocol, anonymity and unlinkability is achieved. The content of the packet is observable in PRISM.

In USOR [8], anonymity, unlinkability and unobservability are achieved. Key sharing is flooded throughout all the nodes in the network. As node increases, it results in computation overhead and increases storage capacity. Every node in the network involves in key decryption and so it causes communication delay. Wormhole attacks, which cannot be prevented by USOR. DoS attacks against unobservable routing Scheme is a challenging task in this Scheme.

Existing anonymous routing schemes for MANET provides anonymity, unlinkability and unobservability. Even though they achieve security, those schemes results in computation overhead [9] and communication delay. The current existing method protects the packet as a whole but authentication is not achieved and it consumes more storage space.

In TQOS [10], the routing protocol can notice the difficult internal attacks and the trustworthiness are incorporated into the routing metrics, which contains the QOS requirement on the links along a route. Here, the majority of external attacks against routing protocols can be detected and prevented. It requires additional cost in processing the routing packets due to the use of security mechanisms. Power consumption is also high. The issues like trust among a node and its neighbors are not mentioned.

When the size of MANETs increase, nodes join and node leave will result in all MANET nodes’ key update. This will bring some problems such as traffics and computations increase [11]. In order to solve this problem, we must classify all nodes by different security levels. So, we can get the following network topology structure: all nodes are classified as multi-cluster and the cluster head is selected. The cluster head is responsible for special tasks such as key management and trust management [12].

3. Content Invisibility Scheme

Our proposal is to provide a Secure and Authenticated Key Exchange scheme for MANET. In MANET, the most important factor is to reduce memory storage and computational overhead. In our paper, the pair- wise shared key is generated in the destination node, which is established between source and destination through the intermediate nodes. So, it reduces the memory space consumption. The only one shared key is used between source and destination. Shared key encryption is done in destination; decryption is done in source node. In our scheme, we used non cryptographic technique XOR encryption since the intermediate node cannot extract the key. The shared keys for intermediate hops are not used in our scheme for secure communication. So it reduces the computation overhead and communication delay. Also privacy in terms of anonymity, unlinkability and unobservability is achieved in our proposed content invisibility scheme.

Symbols	Definitions
CA	Certificate Authority
RS	Random String
K_{A+}/K_{A-}	Public/Private Key of node A
K_{CA+}/K_{CA-}	Public/Private Key of Certificate Authority
ID_X	Identity of Node X
$Auth$	Authenticated Value
V	Value
S_n	Sequence Number
K_{AB}	Pairwise session Key of A and X

Table 1 Symbols and Abbreviations

3.1. Initialization Phase

Initially a pair of public/private key will be issued to each node by Certificate Authority (CA). When each node registers with its identifier and public key, a certificate consisting of Identification(ID) and public key of the corresponding node will be provided by the CA.

For example, consider node A has public/private key denoted as K_{A+}/K_{A-}.

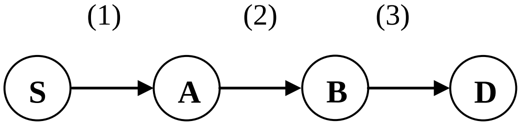
Node A register with CA as follows

$$A \rightarrow CA: ID_A, K_{A+} \tag{1}$$

On receiving the ID and public key from A, CA shares certificate to A which is denoted as

$$CA \rightarrow A: [ID_A, K_{A+}]\ K_{CA-}, K_{CA+} \tag{2}$$

After receiving certificate, node A verifies and authenticates.



(1) $ID_S^{'}, ID_D^{'}, V: Auth_D$
(2) $ID_A^{'}, ID_D^{'}, V: Auth_D$
(3) $ID_B^{'}, ID_D^{'}, V: Auth_D$

Fig.1. Route Request Phase

3.2. Route Request Phase

A secure anonymous route must be established before communication in MANET. The route request messages flood throughout the whole network. There is a node S (source) intending to find a route to a node D (destination), and S knows the identity of the destination node D. Without loss of generality, we assume two intermediate nodes (A and B) between S and D. The proposed scheme provides complete anonymity of the nodes. The process is as follows.

Step 1:

Initially, the source node performs hashing on identity of source and destination.

$$ID_S' = H(ID_S) \quad (3)$$

$$ID_D' = H(ID_D) \quad (4)$$

Then the source node generates a random string (RS) and performs Ex-OR with ID_S' to produce a value V.

$$V = ID_S' \oplus RS \quad (5)$$

This V is again Ex-ORed with ID_D' to produce an authentication value.

$$Auth_D = V \oplus ID_D' \quad (6)$$

Finally source node broadcast the unnamed and unidentified request as

$$SREQ = Broadcast[ID_S', ID_D', V: Auth_D] \quad (7)$$

Step 2:

The neighboring node, say A receives the request and check whether it matches with the received destination ID.

$$ID_A' = H(ID_A) \quad (8)$$

The hashed ID value generated by node A and the destination value present in the request is compared and will find unequal, so that the request is again broadcasted as

$$AREQ = Broadcast[ID_A', ID_D', V: Auth_D] \quad (9)$$

The node updates the ID_S'. The process continues still it reaches destination.

Step 3:

Finally the destination receives the request as

$$BREQ = [ID_B', ID_D', V: Auth_D] \quad (10)$$

The hashed ID value generated by node D and the destination value present in th e request message is compared and will find equal, so that the request is explore $V: Auth_D$. By performing Ex-OR on ID_D' and V, it would find out successfully that it matches the received Authentication and so that it is the destination node.

$$ID_D' = H(ID_D) \quad (11)$$

$$Auth_D = ID_D' \oplus V \quad (12)$$

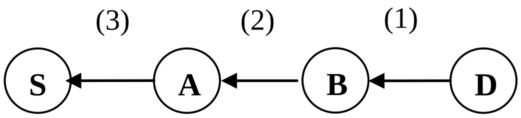
D may receive multiple numbers of route requests from same source and have the same destination from different path. But it replies to the first arrived request and drops rest of them.

Pseudo code for Route Request Phase

```
Output: A secured and Unidentified Route.
Source $S \rightarrow$ Selects a Random String $RS$
Performs $ID_S' = H(ID_S)$ , $ID_D' = H(ID_D)$
Calculates $V = RS \oplus ID_S'$
Calculates $Auth_D = V \oplus ID_D'$
Broadcast $RREQ$
while (true)
{
    hop receives the $RREQ$
    Verifies certificates of the packet
    if(packet non valid)
        Drop packet;
    Generates $ID_X' = H(ID_X)$
    Also generates $Auth_X$
    verifies with received Auth from $RREQ$
    if($Auth_X$ = = $Auth_D$)
        Stores $V$ and updates the Route
        Break;
    else
        Update $ID_X'$ to $RREQ$
        Rebroadcast the packet
    endif
}
```

3.3. Key Generation and Route Reply Phase

As soon as D found out that it is the destination node, it needs to reply to S in order to establish route between them. In this phase, unicast instead of broadcast is used to save communication cost. The key generation and key exchange is performed concurrently with the route reply process. The steps involved are as follows.



(1) $ID_B^{'}: V^{*}: Auth_D^{'}$
(2) $ID_A^{'}: V^{*}: Auth_D^{'}$
(3) $ID_S^{'}: V^{*}: Auth_D^{'}$

Fig.2 Key Generation and Route Reply

Step 1:

The destination node D generates a key (K^{*}) and perform Ex-OR operation with V which is in the request message to compute V^{*}.

$$V^{*} = K^{*} \oplus V \tag{13}$$

It also generates authentication by performing

$$Auth_D^{'} = V^{*} \oplus ID_D^{'} \tag{14}$$

Then D replies the reply message as

$$DREP: [ID_B^{'}: V^{*}: Auth_D^{'}] \tag{15}$$

Step 2:

The intermediate node B will receive the packet and verifies its authentication as

$$Auth_B^{'} = V^{*} \oplus ID_B^{'} \tag{16}$$

As authentication doesn't match, B forward it depending upon the sequence number as

$$BREP: [ID_A^{'}: V^{*}: Auth_D^{'}] \tag{17}$$

Other intermediate nodes also perform the same operation as B does. Finally route reply is sent back to the source node S by A as

$$AREP: [ID_S^{'}: V^{*}: Auth_D^{'}] \tag{18}$$

Step 3:

Finally Source S receives the reply message and verifies using

$$Auth_D^{'} = V^{*} \oplus ID_D^{'} \tag{19}$$

Now S ensures that D has successfully opened the route request packet. S also computes

$$V^{'} = V^{*} \oplus RS \tag{20}$$

$$K^{*} = V^{'} \oplus ID_S \tag{21}$$

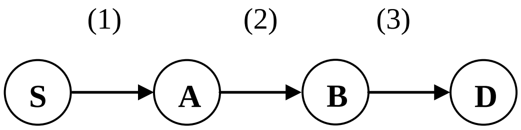
Till now S has successfully found the route to the destination node D and also established a key between source node S and destination node D.

Pseudo code for Route Reply & key setup phase

Input : Reply Packet from Destination
Output: A secured key exchange

```
Destination generates $K^{*}$ Randomly
Performs $V^{*} = K^{*} \oplus V$
Performs $Auth_D^{'} = V^{*} \oplus ID_D^{'}$
Replies $RREP$ using $V^{*}$, $Auth_D^{'}$ and $S_n$
while (true)
{
    hop receives the $RREP$
    Generates $Auth_X^{'}$
    Verifies with received Auth from $RREP$
    if($Auth_X^{'}$ = = $Auth_D^{'}$)
        $V^{'} = V^{*} \oplus RS$
        Performs $V^{'} \oplus ID_S$ to extract the
        key $K^{*}$
    else
        $RREP$ to the next hop according to
        the $S_n$
    end if
}
```

3.4. Data Packet Transmission Phase



(1) $DATA: \begin{bmatrix} Auth_D^{'}, ID_D^{'}, ID_A^{'}, \\ EK_{SD}(payload) \end{bmatrix}$
(2) $DATA: \begin{bmatrix} Auth_D^{'}, ID_D^{'}, ID_B^{'}, \\ EK_{SD}(payload) \end{bmatrix}$
(3) $DATA: \begin{bmatrix} Auth_D^{'}, ID_D^{'}, ID_D^{'}, \\ EK_{SD}(payload) \end{bmatrix}$

Where $K_{SD} = K^{*}$

Fig.3. Data Packet Transmission

The source node S successfully finds a route to the destination node D, S can start data transmission by use of the received key. Data packets from S must traverse A, B to reach D. The data packets sent by S take the following format:

$$DATA: [Auth_D^{'}, ID_D^{'}, ID_A^{'}, EK_{SD}(payload)] \quad (22)$$

Where $K_{SD} = K^*$. Receiving the message from S, A knows that this message is for him according to the ID.

After decrypting the key, A knows this message is a data packet and should be forwarded to B based on its ID. Hence it composes and forwards the following packet to B:

$$DATA: [Auth_D^{'}, ID_D^{'}, ID_B^{'}, EK_{SD}(payload)] \quad (23)$$

Data packet is forwarded by other intermediate nodes until it reaches the destination node D . The following data packet is received by D:

$$DATA: [Auth_D^{'}, ID_D^{'}, ID_D^{'}, EK_{SD}(payload)] \quad (24)$$

4. Simulation And Performance Metrics

4.1. Simulation Environment

The Simulation has been carried out on the Content Invisibility Scheme to evaluate its performance in different metrics. The proposed scheme is implemented on Java and evaluated in Network Simulator NS2. The MAC Layer IEEE 802.11 is used in our simulation work. The nodes are spread randomly in the network with a constant motion. To perform network connectivity between the nodes in the network, NS2 Constant Bit Ratio (CBR) is used. Then to perform network connectivity from nodes to the different random seeds, Java UDP concepts are used. Every node in the network generates request packets uniformly.

The Random String is used to perform mobility between the nodes. Approximately 1000 packets are generated at a time and requested at the same. The Ad Hoc On-Demand Distance Vector (AODV) routing protocol is used for both NS2 and Java.

4.2. Security Analysis

In ad hoc networks, both internal and external attacks are taken into account for security analysis. Encryption methods and key exchanging techniques are used for analyzing internal and external attacks.

4.2.1.Internal Attack

In internal attack, the malicious nodes act as a trusted node and participate in the network after verifying the certificates. Later on, in key exchanging phase and communication phase there is a chance to extract the key and the secured data shared between the source and destination. In our work, even though the malicious nodes have the certificate for participating in the network, it cannot find the ID of the nodes. Also if other node shares the information to the malicious node, without the ID, the malicious node cannot open the information. Also the IOI's (Items of Interests) cannot be identified by the malicious node.

Using the Random String and the ID of the node, a value V is computed and this value is used in request message. Then using that value and the hashed ID of the destination node, an authentication value is generated as a result of the XOR operation between them. Then pair wise key is used for encryption of message and it cannot be decrypted by the malicious nodes in the network. So from the above mentioned technique, there is no way to attack the data transmission in the network.

4.2.2.External Attack

In the external attack, malicious nodes are involved in the attack. There is a need to rule-out participation of the malicious nodes in the network. To rule-out the participation of the malicious nodes in the network, network certificates are used. Certificate Authority (CA) issues certificates to those nodes which requests to join the network. The function of the CA is to verify the certificates of the nodes that requests. After verifying the certificates, CA allows the nodes to participate into the network. So the nodes are verified based on the certificates in the initialization phase itself.

4.3. Memory Management

The proposed work shares a single key between source and destination for the secure communication. It utilizes less memory to establish key management, compared with existing schemes. The existing schemes are in need of pre key distribution as well as flooding of requests, and each node needs to store a number of keys between the neighborhood nodes and the destination node, which consumes more memory than the proposed system.

In Existing schemes, every single node shares a local broadcast key and a session key between the neighborhood nodes and the destination for communication. In our proposed scheme, it shares a single key between source and destination node to communicate. It consumes less memory [13].

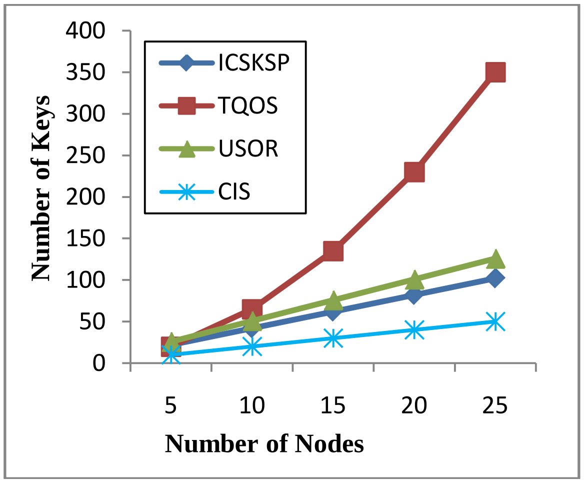


Fig.4. No. of keys shared during communication between source and destination

Fig. 4 shows the number of keys utilized by the network, once the number of hops increases from source to destination. And it clearly shows that the proposed content invisibility scheme utilizes less number of keys per hop. Unlinkability and unobservability are also achieved using less memory consumption in our method compared with existing strategies.

4.4. Computation Cost

Computation cost is an important factor for MANET since each node in a network is equipped with low memory and fewer numbers of processors. Our proposed method uses a hash function and ID based encryption. And also uses a XOR function to share a key between the source and the destination. On comparing with previous existing protocols, our protocol requires low computation cost which is portrayed in Fig.5.

On the other hand, the existing schemes utilize more memory since each node in a network ought to do encryption process for sharing the keys. In the proposed content invisibility scheme, route request and route reply phases require 8 computation steps for each. Here key sharing is performed simultaneously with the route reply phase. So the total requirement of computation steps in our method is 16. It is clearly shown that the proposed content invisibility method requires fewer numbers of computation steps (computation cost) compared with existing protocols.

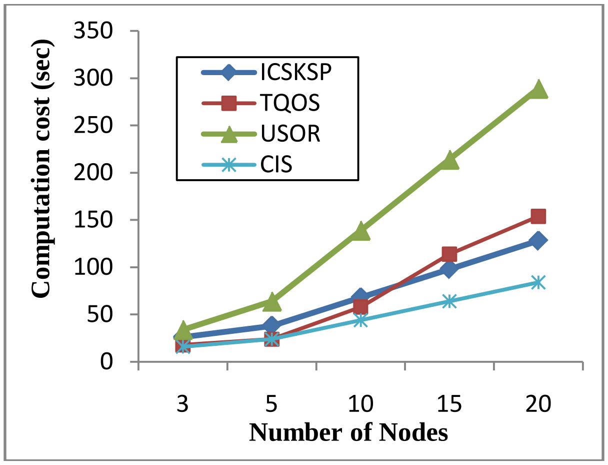


Fig.5.Comparison of computation overhead

4.5. Performance Analysis

In this section, the performance of the Content Invisibility approach is analyzed with the metrics Packet Delivery Ratio, End to End Delay, Throughput, Latency Time and Average Routing Load**.** Further, proceed with following figures which shows the performance of content invisibility and the existing schemes.

The schemes are compared using increasing packet rates and varying traffic loads. The traffic loads are selected according to the performance of standard AODV implementation in ns2.

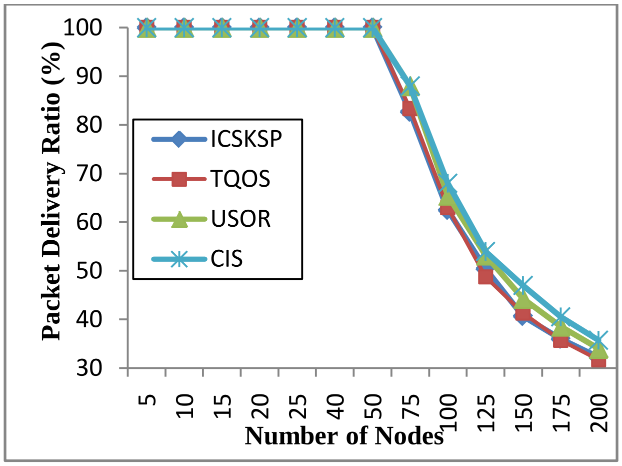


Fig.6.Packet Delivery ratio.

Fig. 6 shows that, for same traffic loads Content Invisibility offers higher Packet Delivery Ratio when compared to other protocols. Number of packets is inversely proposed to Packet Delivery Ratio. When we increase the number of packets, Packet Delivery Ratio decreases. Under traffic load, the performance is downgraded in existing strategies however the Content Invisibility is remains its rate. Due to the smaller packet size and less computation process in our proposed system packet drop is minimized.

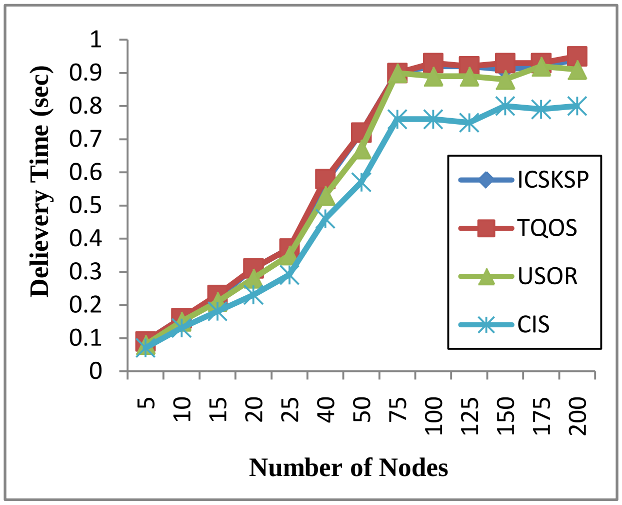


Fig.7.Delivery Time

From Fig. 7, it is determined that the Content Invisibility Scheme has the least delivery time in comparison with the other existing protocols. When the number of node increases, the delivery time of existing protocols varies compare with Content Invisibility Scheme that is portrayed in figure.

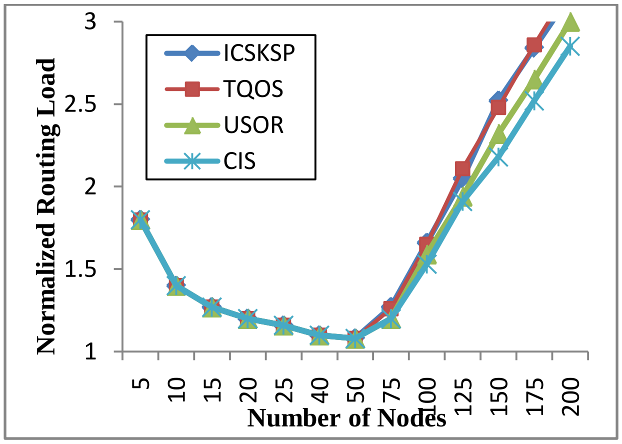


Fig.8.Average Routing Load

Fig. 8 illustrates the routing load between the previous methods and the Content Invisibility Scheme that states the cost for delivering a unit of data payload. In Content Invisibility Scheme, there are three types of routing control packets namely routing request packet, routing reply packet, and routing error packet. However, other schemes need more control packets to maintain anonymous routing information [14]. In Content Invisibility

Scheme, the key sharing and the anonymous routing is performed via request packet and reply packet. Additional routing packets are needed for the performance of key sharing and anonymous routing in existing schemes. Thus, on comparing the routing load between the existing schemes and Content Invisibility Scheme, the proposed **s**cheme performs well.

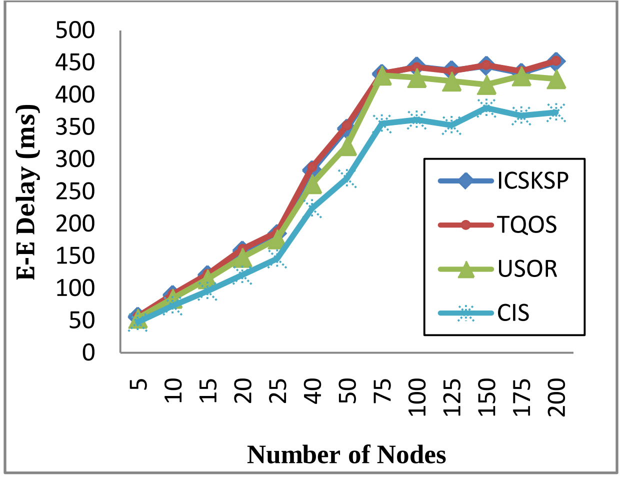


Fig.9.End to End Delay

Fig. 9 shows the end to end delay time between the secure key sharing methods. In Content Invisibility Scheme, the increase in number of packets causes a small variation within the performance whereas others report a significant delay. It is stated that the end-to-end delay time of Content Invisibility Scheme is not up to the previous schemes, due to the heavy computation process and increased nodes.

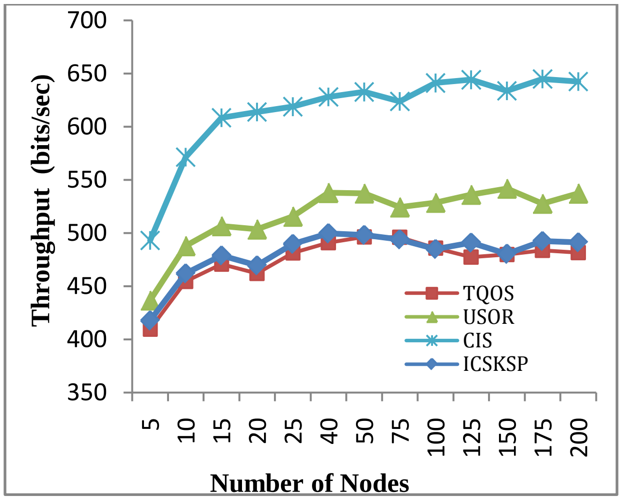


Fig.10.Throughput

Fig. 10 illustrates the throughput between the existing security schemes and the Content Invisibility scheme. Throughput increases in both protocols, even though it is increased more dramatically in Content Invisibility Scheme whereas slight increase in other schemes.

5. Conclusion

In this paper the Content Invisibility Scheme based on ID Based Encryption is proposed. The proposed scheme shares the key between source and destination which is more resistant against internal and external attacks. The design of our scheme offers strong privacy protection - complete unobservability, unlinkability and anonymity - for ad hoc networks. Our proposed scheme can make it computationally difficult for attackers to obtain the correct secret key. One way hash function is used for key generation, which is used to avoid collision between nodes. Key is shared between neighbors, so computation overhead as well as communication delay is reduced. The security methods used in this scheme allows secure communication between source and destination. Our proposed scheme requires significantly less key storage space than existing methods since it uses single session key. Our proposed Content Invisibility Scheme is well suited for the key establishment for MANET. The revoking of key is another direction where revoking is the major concern in key management mechanism when a particular key is not reaching the appropriate destination. In future, we consider other than performance based and Cost based metrics like dependability and configuration.

References:

[1] Bagwari. A, Jee. R, Joshi. P, Bisht. S, Performance of AODV Routing Protocol with Increasing the MANET Nodes and Its Effects on QoS of Mobile Ad Hoc Networks, *Proceedings of International Conference on Communication Systems and Network Technologies* , 2012, pp. 320-324.

[2] Wan. Z, Kuiren & Gu. M, USOR: An Unobservable Secure On-Demand routing

Protocol For Mobile Ad Hoc Networks, *IEEE Transactions On Wireless Communications*, Vol. 11, No. 5, 2012, pp.1922-1932.

[3] Kong. J & Hong. X, ANODR: ANonymous On Demand Routing with Untraceable Routes for Mobile Ad-hoc Networks, *Proceedings of 4th ACM international symposium on Mobile ad hoc networking & computing*, 2003, pp.291-302.

[4] Zhang. Y, Liu. W & Lou. W, Anonymous Communications in Mobile Ad-hoc Networks, *Proceedings of 24th Annual Joint Conference of the IEEE Computer and Communications Societies*, 2005, pp.1940-1951.

[5] Seys. S & Preneel. B, ARM: Anonymous Routing Protocol for Mobile Ad-hoc Networks, *Proceedings of IEEE International Conference on Advanced Information Networking and Applications,* 2006, pp. 133-137.

[6] Sy. D, Chen.R & Bao. L, ODAR: On-Demand Anonymous Routing in Ad-hoc Networks, *Proceedings of IEEE Conference on Mobile Adhoc and Sensor Systems*, Vol.4, 2006, pp. 721-730.

[7] Defrawy. K. E & Tsudik. G, PRISM: Privacy-Friendly Routing in suspicious MANETs, *Proceedings of IEEE International Transaction on Network Protocols*, 2008, pp. 258-267.

[8] Defrawy. K. E & Tsudik. G, Privacy-Preserving Location-Based On-Demand Routing in MANETs, *IEEE Journal on Selected Areas in Communication*, Vol. 29, No. 10, 2011, pp. 1926- 1934.

[9] Capkun. S, Hubaux. J. P& Buttyan. L, Self-Organized Public-Key Management for Mobile Ad Hoc Networks, *IEEE Transaction on Mobile Computing,* Vol. 2, No. 1, 2003, pp. 52-64.

[10] Yu. M & Leung. K. K, A Trustworthiness-Based QoS Routing Protocol for Wireless Ad Hoc Networks, *IEEE Transactions on wireless Communications,* Vol. 8, No. 4, 2009, pp. 1888-1898.

[11] Zhou. Y & Fang. Y, Scalable and deterministic key agreement for large scale networks, *IEEE Transaction on Wireless Communication*, Vol. 6, No. 12, 2007,pp.4366-4373.

[12] Wan An Xoing, Yao Huan Gong, Secure and Highly Efficient Three Level Key Management Scheme for MANET, *WSEAS TRANSACTIONS on COMPUTERS*, Vol. 10, No 10, 2011.

[13] D'Souza. R. J, Varaprasad, G. G. S. M, Digital Signature-Based Secure Node Disjoint Multipath Routing Protocol for Wireless Sensor Networks, *IEEE sensors Journal*, Vol.12, No.10, 2012, pp. 2941-2949.

[14] Hong. X, Xu. K & Gerla. M, Scalable routing protocol for mobile ad hoc networks, *IEEE Network*,Vol.16,No.4, 2002, pp.11-21.