

Secure Hybrid Routing Protocol Based on Unobservable Identity in MANET

A.Menaka, N.Kumaratharan*

Department of Information Technology, Sri Venkateswara College of Engineering, Sriperumbudur– 602117, Tamil Nadu, India
*Corresponding Author: kumaratharan@rediffmail.com

Copyright © 2014 Horizon Research Publishing All rights reserved.

Abstract Mobile Ad-hoc Networks (MANETS) are particularly useful and well-suited for critical scenarios, including military, law enforcement as well as emergency rescue and disaster recovery. An unobservable secure hybrid routing protocol (USHR) scheme achieves content unobservability by employing anonymous key establishment based on group signature for improving the performance of a routing protocol in terms of packet delivery ratio (PDR) is proposed in this paper. USHR is efficient it uses a novel combination of group signature and ID-based encryption for route discovery. The main objective of this work is to develop a privacy preserving routing protocol scheme that consumes low network delay, minimum packet loss, and maximize the network capacity. By implementing a USHR protocol using advanced hashing technique in NS2 and designed by using spread spectrum technique, the performance of USHR Protocol is improved and the same is proved through NS2 simulation compared with USOR protocol. Due to incomplete content protection complete unlinkability and unobservability are not guaranteed. The simulation results show that USHR not only has performance compared to USOR, and also achieves stronger privacy protection than existing schemes like USOR.

Keywords Anonymity, Privacy-Preserving, Unobservability

1. Introduction

Mobile ad-hoc networks are rapidly evolving as an important area of mobile mobility. MANETs are infrastructure less and wireless in which there are several routers which are free to move arbitrarily and can manage themselves in same manners. The network topology changes very rapidly and unpredictably in which many mobile nodes moves to and from a wireless network without any fixed access point where routers and hosts move, so topology is dynamic. It has to support multi hop paths for mobile nodes to communicate with each other and can have multiple hops over wireless links and also connection point to the internet

may also change. If mobile nodes are within the communication range of each other than source node can send message to the destination node otherwise it can send through intermediate node. Now-a-days mobile ad-hoc networks have robust and efficient operation in mobile wireless networks as it can include routing functionality into mobile nodes which is more than just mobile hosts and reduces the routing overhead and saves energy for other nodes. Hence, MANETs are very useful when infrastructure is not available, impractical, or expensive because it can be rapidly deployable, without prior planning or any existing infrastructure. Mostly mobile ad-hoc networks are used in military communication by soldiers, planes, tanks etc, operations, automated battlefields, emergency management teams to rescue, search, fire fighters or by police and replacement of a fixed infrastructure in case of earthquake, floods, fire etc, quicker access to patient data about record, status, diagnosis from the hospital database, remote sensors for weather, personal area network, taxi cab network, sports stadiums, mobile offices, yachts, small aircraft, electronic payments from anywhere, voting systems, vehicular computing, education systems with set-up of virtual classrooms, conference rooms, meetings, peer to peer file sharing systems, collaborative games with multi users. Several routing schemes were proposed to achieve the unlinkability and unobservable identity in mobile Ad-hoc networks. Self-Organized Public-Key Management scheme allows users to generate their public-private key pairs, to issue certificates, and to perform authentication. This scheme provides different level of privacy protection at different cost [1]. Secure Distributed Anonymous Routing Protocol (SDAR) guarantees security, anonymity and high reliability of the established route in a hostile environment. It requires more computation effort because more scalable to network size [2]. Anonymous Communications gives a wide range of adversarial attacks and the setup of MASK is quite expensive [3]. ARM fails to protect all content of packets from attackers Privacy offered by hiding routes in limited broadcast groups, and padding messages [4]. Anonymous Dynamic Source Routing protocol (AnonDSR) provides a strong security and anonymity protection. This protocol fails to protect linkability or observability of messages [5].

On-Demand Anonymous Routing protocol enables complete anonymity, this protocol fails to provide unlinkability, and also the entire RREQ/RREP packets are not protected with session keys [6]. PRISM reveals less topology and more privacy-friendly [7]. Anonymous Location-Aided Routing in MANET (ALARM) still leaks a lot sensitive privacy information network topology and Location of every node [8].

The paper is organized as follows: Section II describes the routing protocols by the proposed system. The details of system setup are explained in section III. The performance evaluation and simulation results are presented in section IV, and the conclusion is arrived at section V.

2. Routing Protocol

Routing in a MANET depends on many factors, including modeling of the topology, selection of routers, initiation of a route request, and specific underlying characteristics that could serve a heuristics in finding the path efficiently. The low resource availability in MANET necessitates efficient resource utilization. Also, the highly dynamic nature of these networks places severe restrictions on any routing protocol specifically designed for them a network configuration is also called network topology. An ad-hoc routing protocol is a convention, or standard, that controls how nodes decide which way to route packets between computing devices in a MANET. MANETs routing protocols are characteristically subdivided into three main categories. These are Proactive routing protocols (Table-driven Routing Protocol), Reactive (Source-initiated on-demand Routing Protocol) and Hybrid Routing Protocols.

2.1. Proactive or Table-Driven Routing Protocol

The Proactive or Table-driven routing protocols attempt to maintain consistent, up-to-date routing information from each node to every other node in the network. These protocols require each node to maintain one or more tables to store routing information, and they respond to changes in network topology by propagating updates throughout the network in order to maintain a consistent network view. The areas in which they differ are the number of necessary routing-related tables and the methods by which changes in network structure are broadcasted. Example, Destination-Sequence Distance Vector Routing (DSDV) and Wireless Routing Protocol (WRP).

Destination Sequence Distance Vector Routing Protocol (DSDV): Destination Sequence Distance Vector Routing Protocol (DSDV) is a table-driven routing scheme for Ad-hoc mobile networks based on the Bellman-Ford algorithm. The main contribution of the algorithm was to solve the Routing Loop problem. Each entry in the routing table contains a sequence number, the sequence numbers are generally even if a link is present; else, an odd number is used. The number is generated by the destination, and the

emitter needs to send out the next update with this number. Routing information is distributed between nodes by sending full dumps infrequently and smaller incremental updates more frequently. DSDV was one of the early algorithms available. It is quite suitable for creating Ad-hoc networks with small number of nodes. Since no formal specification of this algorithm is present there is no commercial implementation of this algorithm. Many improved forms of this algorithm have been suggested. DSDV requires a regular update of its routing tables, which uses up battery power and a small amount of bandwidth even when the network is idle.. Thus, DSDV is not suitable for highly dynamic networks. The main disadvantage of this routing protocol requires a regular update of its routing tables, which uses up battery power and a small amount of bandwidth even when the network is idle.

2.2. Reactive or On-Demand Routing Protocol

A different approach from table-driven routing is source-initiated (on-demand) routing. This type of routing creates routes only when desired by the source node. When a node requires a route to a destination, it initiates a Route Discovery Process within a network. This process is completed once a route is found or all possible route permutations have been examined. Once a route has been established, Route Maintenance Procedure maintains it until either the destination becomes in accessible along every path from the source or until the route is no longer desired. For example, Ad-Hoc On-demand Distance Vector (AODV), Dynamic Source Routing (DSR).

Ad-hoc On-Demand Distance Vector Routing Protocol: AODV is a very simple, efficient, and effective routing protocol for Mobile Ad-hoc Networks which do not have fixed topology. Being a reactive routing protocol AODV uses traditional routing tables, one entry per destination and sequence numbers are used to determine whether routing information is up-to-date and to prevent routing loops. The maintenance of time-based states is an important feature of AODV which means that a routing entry which is not recently used is expired. The neighbors are notified in case of route breakage. The discovery of the route from source to destination is based on query and reply cycles and intermediate nodes store the route information in the form of route table entries along the route. Main disadvantage is Requirement on broadcast medium, Overhead on the bandwidth. Control messages used for the discovery and breakage of route are as follows: Route Request Message (RREQ), Route Reply Message (RREP), Route Error Message (RERR) and HELLO Messages.

2.3. Hybrid Routing Protocol

The Hybrid Protocols attempt to take advantage of best of both Proactive and reactive schemes. The main idea behind such protocols is to be initiate route-discovery on-demand but at a limited search cost. For example, Zone Routing

Protocol (ZRP)

Zone Routing Protocol: ZRP was the first hybrid routing protocol with both a proactive and reactive routing component. ZRP was proposed to reduce the control overhead of proactive routing protocols and decrease the latency caused by route discovery in reactive routing protocols. A proactive routing protocol, Intra-zone Routing Protocol (IARP), is used inside routing zones, and a reactive routing protocol, Inter-zone Routing Protocol (IERP), is used between routing zones. To reduce the control overhead of proactive routing protocols and decrease the latency caused by route discovery in reactive routing protocols. A proactive routing protocol, Intra-zone Routing Protocol (IARP), is used inside routing zones, and a reactive routing protocol, Inter zone Routing Protocol (IERP), is used between routing zones. A route to a destination within the local zone can be established from the source's proactively cached routing table by IARP. Therefore, if the source and destination of a packet are in the same zone, the packet can be delivered immediately. Most of the existing proactive routing algorithms can be used as the IARP for ZRP. For routes beyond the local zone, route discovery happens reactively. The source node sends a route request to the border nodes of its zone, containing its own address, the destination address and a unique sequence number. Border nodes are nodes which are exactly k hops away from the source. Each border node checks its local zone for the destination. If the destination is not a member of this local zone, the border node adds its own address to the route request packet and forwards the packet to its own border nodes. The source node uses the path saved in the route reply packet to send data packets to the destination. Main advantage is that Single source request can result in multiple route replies, and the source can determine the quality of these multiple routes based on such parameter(s) as hop count or traffic and choose the best routes to be used.

3. System Setup

A network consisting of n nodes, all nodes have the same communication range, and each node can move around within the network. A node can communicate with other nodes within its transmission range, and these nodes are called its neighbors. For nodes outside of one's transmission range, one has to communicate via a multi-hop path. The ad-hoc network is all connected, and each node has at least one neighbor. Nodes do not use physical addresses like MAC addresses in data frames to avoid being identified by others. Instead, they set their network interfaces in the promiscuous mode to receive all the MAC frames that can be detected in the neighborhood. This is important to prevent traffic analysis based on MAC addresses. The ad-hoc network starts up, by the group signature scheme, a key server generates a group public key gpk which is publicly known by everyone, and it also generates a private group signature key gsk_x for each node X . The group signature scheme ensures full

anonymity, and the signature does not reveal the signer's identity but everyone can verify its validity. The main idea of hashing is to distribute the entries across an array of buckets. Given a key, the algorithm computes an index that suggests where the entry can be found: $index = f(key, array_size)$. Advanced hashing can be done in two steps: In this method, the hash is independent of the array size, and it is then reduced to an index using a remainder operation (%). In case the array size is a power of two, the remainder operation is reduced to masking, which improves speed, but can increase problems with a poor hash function. The setup of the ID-based encryption scheme is as follows. Let G_1, G_2 be an elliptic curve group of order q . An admissible bilinear mapping $e: G_1 \times G_1 \rightarrow G_2$. An identity-based encryption scheme is specified by four randomized algorithms. They are Setup, Extract, Encrypt and Decrypt.

Setup: It takes a security parameter k and returns parameters and master key. The system parameters include a description of a finite message space M , and a description of a finite cipher text space C . Intuitively, the system parameters will be publicly known, while the master key will be known only to the private key generator.

Extract: It takes as input parameters, master-key, and an arbitrary ID, and returns a private key d . Here ID is an arbitrary string that will be used as a public key, and d is the corresponding private decryption key. The Extract algorithm extracts a private key from the given public key.

Encrypt: It takes as input parameters, ID, and $M \in M$. It returns a cipher text $C \in C$.

Decrypt: It takes as input parameters, ID, $C \in C$, and a private key d . It returns $M \in M$. These algorithms must satisfy the standard consistency constraint, namely when d is the private key generated by algorithm Extract when it is given ID as the public key, then $M \in M$: Decrypt (params; ID; C ; d) = M .

3.1. Unobservable Secure Routing Scheme

An unobservable secure routing scheme offers complete unlinkability and content unobservability for all type of packets. This method can well protect user privacy against both inside and outside attackers.

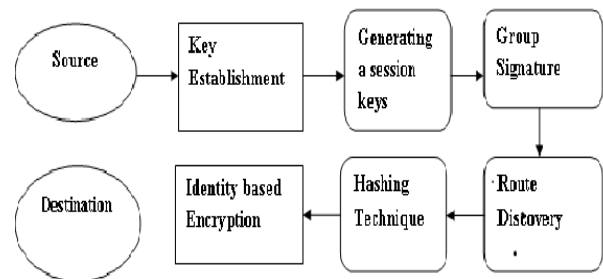


Figure 1. Block Diagram for USHR Model Protocol

Fig-1 shows the block diagram for USHR protocol this method achieves stronger privacy protection over network communication. An efficient Privacy-preserving routing

protocol USHR that achieves content unobservability by employing anonymous key establishment based on group signature. Each node has to obtain a group signature signing key, advanced hashing technique and ID based private key from an offline key server. The unobservable routing scheme comprises of two phases: anonymous key establishment as the first phase and the route discovery process as the second phase. In the first phase of the scheme, each node employs anonymous key establishment to anonymously construct a set of session keys with each of its neighbors. Then under protection of these session keys, the route discovery process can be initiated by the source node to discover a route to the destination node

3.1.1. Anonymous Key Establishment

In this first phase, every node in the network communicates with its direct neighbors within its radio range for anonymous key establishment. Suppose there is a node S with a private signing key gsk_S and a private ID-based key K_S in the ad-hoc network and it is surrounded by a number of neighbors within its power range. The result of this phase, a pairwise session key k_{SX} is constructed anonymously. The two nodes establish this key without knowing who the other party is. Node S establishes a local broadcast key \overline{k}_{S^*} , and transmits it to all its neighbors. It is used for per-hop protection for route discovery.

Steps involved for generating a group signature:

- i. Source node S generates a random number $r_S \in Z_q^*$ and computes $r_S P$, where P is the generator of G_1 . Then computes a signature of $r_S P$ using its private signing key gsk_S to obtain $SIG_{gsk_S}(r_S P)$. Anyone of the node can verify this signature using the group public key gpk . It broadcast within its neighborhood.
- ii. A neighbor node X of source node S receives the message from the source node S and verifies the signature in that message. If the verification is successful, then neighbor node X chooses a random number $r_X \in Z_q^*$ and computes routing path. Intermediate node X also computes a signature using its own signing key gsk_X . Intermediate node X computes the session key and replies to the source node S with message.
- iii. Receiving the reply from neighbor node X , source node S verifies the signature inside the message. If the signature is valid, source node S proceeds to compute the session key between the node X and node S also generates a local broadcast key \overline{k}_{S^*} and sends to its neighbor node X to inform about the established local broadcast key.
- iv. Neighbor node X receives the message from source node S and computes the same session key as $k_{SX} = H_2(r_S r_X P)$. Then it decrypts the message to get the local broadcast key \overline{k}_{S^*} .

3.1.2. Route Discovery

The route request messages flood throughout the whole network, the route reply messages are sent backward to the

source node only. There is a source node intending to find a route to a destination node D , and node S knows the identity of the destination node D . Without loss of generality, we assume three intermediate nodes between source and destination.

Route Request (RREQ)

Source node S chooses a random number r_S , and the identity of destination node to encrypt a trapdoor information that can be opened with node D 's private ID based key, that yields $E_D(S, D, r_S P)$. Then source node S selects a sequence number $seqno$ for this route request, and another random number N_S as the route pseudonym, which is used as the index to a specific route entry. To achieve unobservability, node S chooses a nonce $Nonce_S$ and calculates a pseudonym as each node maintains a temporary entry in his routing table. Any node does not know the real identity of its upstream or downstream node. The entry maintained by source node. Then the node S encrypts using its local broadcast key. Node S broadcast the unobservable route request to its neighbors. On receiving the route request message from the node S , then a node A tries the session keys are shared with all neighbors to calculate hash value $H_3(k_X A | Nonce_S)$ and also to see which one of the node matches the received Nym_S . Then node A finds out \overline{k}_{S^*} and satisfies $Nym_S = H_3(\overline{k}_{S^*} | Nonce_S)$, \overline{k}_{S^*} to decrypt the ciphertext. After finding a route request packet, node A tries to decrypt $E_D(S, D, r_S P)$ using his private ID based key to check the destination node. To avoid RREQ broadcasting storm, A will check if he has received the same request before by looking up in his cache, which includes a list of N_S and $seqno$. Node A is not the destination node this node trial fails, so node A acts as an intermediate node. Node A generates a nonce $Nonce_A$ and a new route pseudonym N_A for this route then it calculates a $Nym_A = H_3(\overline{k}_{A^*} | Nonce_A)$. Also Node A records the route pseudonyms and sequence number in routing table for purpose of routing, and the corresponding table entry is maintained. At the end, node A prepares and broadcast the message to all its neighbors. Finally, the destination node D receives the message from node C . Node D finds out the correct key based on the equation $Nym_C = H_3(\overline{k}_{C^*} | Nonce_C)$. After decrypting the ciphertext using \overline{k}_{C^*} , Node D records route pseudonyms and the sequence number into its route table. Then node D successfully decrypts $E_D(S, D, r_S P)$ to find out the destination node. Node D may receive more than one route request messages that originate from the same source and have the same destination D , but node D replies to the first arrived message and drops the following ones. The route table entry recorded by D is $\langle seqno, N_C, -, C, - \rangle$.

Route Reply (RREP)

After finding the destination node, node D starts to prepare a reply message to the source node. For route reply messages, unicast instead of broadcast is used to save communication cost. Then node D chooses a random number r_D and computes a ciphertext $E_S(D, S, r_S P, r_D P)$ shows the valid destination capable of opening the trapdoor information.

Node A computes the session key for data protection $k_{SD} = H_2(r_{SD}P|S|D)$. Then it generates a new pair wise pseudonym between node C and node D. The pair wise session key k_{CD} , computes and sends the message to node C. When node C receives the above message from destination node D and identifies the sender of the message is by evaluating the equation $Nym_{CD} = H_3(k_{CD}|Nonce_D)$. It uses the right key k_{CD} to decrypts the ciphertext, and also finds out which route this RREP is related to according to the route pseudonym N_C and seqno. Node C searches route table and modifies the temporary entry into $\langle seqno, NB, NC, B, D \rangle$. At the end, node C chooses a new nonce $Nonce_C$, computes $Nym_{BC} = H_3(k_{BC}|Nonce_C)$, and sends the message to node B. The other intermediate nodes perform the same operations as node C. Finally, the route reply is sent back to the source node S by node A. Source node S decrypts the ciphertext using the key k_{SA} and verifies that $E_S(D, S, r_{SP}, r_{DP})$ is faultlessly. Source node S is ensured that destination node D has successfully opened the route request packet, and the route reply is really originated from the destination node D. Source node S computes the same session key between the destination node $k_{SD} = H_2(r_{SD}P|S|D)$ as D node. Then source node S has successfully found a route to the destination node D, and the route discovery process is finished with success. Then node S finds and modifies temporary route table entry $\langle seqno, -, NS, -, - \rangle$ into $\langle seqno, -, NS, -, A \rangle$.

3.1.3. Packet Data Transmission

The source node S successfully finds a route to the destination node D, node S can starts data transmission under the protection of pseudonyms and keys. The data packets from source node S must traverse nodes A, B, and C to reach destination node D. The data packets sent by source node S. Receiving the message from source node S, node A knows that this message according to the pseudonym Nym_{SA} . After decryption key, node A knows this message is a data packet should be forwarded to node B according to route pseudonym N_S . Hence node S composes and forwards the packet to node B. Data packet is forwarded by other intermediate nodes until it reaches the destination node D.

3.1.4. Properties of USHR

USHR aims to offer the following privacy properties

- i. Anonymity: The senders, receivers, and intermediate nodes are not identifiable within the whole network.
- ii. Unlinkability: There is no link between any two or more item of interest from the senders, the receivers, the intermediate nodes, and the messages are protected from outsiders.
- iii. Unobservability: Any meaningful packet in the routing scheme is indistinguishable from other packets to an outside attacker.

4. Performance Evaluation

In this section, the performance of USHR protocol and

USOR protocol in terms of detection confidence index value and packet delivery ratio is evaluated. Further, average throughput of USHR, and USOR protocol in terms of network delay and network capacity values obtained in trace file is demonstrated. To calculate the packet losses for both USHR and USOR protocol, performance of USHR protocol and USOR protocols were evaluated. From critical evaluation it is concluded that USOR routing protocols add a lot of overhead and cause degradation of power efficiency. Thus, such protocols are not well suited for an ad-hoc mobile environment. On the other hand, the USHR protocols require lesser battery power and reduce the routing overhead. The USHR protocols have been proven to operate more efficiently as compared to USOR and AODV protocols. The difference between USHR and USOR on packet delivery ratio is less than 20%.The performance drop of both protocols when node speed goes up due to more frequent route disruption at higher speeds. Route disruption leads to packet drop and retransmission, and a new route has to be constructed before remaining packets can be sent out. Lower packet delivery ratio of USHR is due to the following reasons: 1) In USHR only trusted neighbors will forward route packets for each other, otherwise packets are simply dropped, 2) Local key update and node mobility leads to trust lost between one and its neighbors. Before neighboring nodes establish shared local keys, no traffic can be passed between them, which results in transmission delay in USHR; 3) Route repair in USOR is complex task in the protocol for the sake of privacy protection, as route repair requires identity information about the destination;4) In USHR, intermediate nodes can reply to a route request if they know a route to the requested destination, USHR cannot do this as any intermediate node is not supposed to know either the source node or the destination node;5) In USHR, achieves low delay compared with USOR protocol; and 6) In USHR, maximizes the network capacity compared with USOR protocol.

5. Simulation Results

Computation cost of USHR was analyzed and compared with USOR schemes. USHR protocol was implemented and its performance is evaluated by comparing with USOR protocol. The parameters required to execute the code is provided in table-1.

Table 1. Parameter Specifications

PARAMETER	SPECIFICATION
1024-bit ID-based Encryption/ Decryption	20ms
Group Signature Generation/ verification	22ms
Scenario Dimension	650 m X 650 m
Number of Mobile Nodes	100 nodes
Routing Protocol	USHR

The implementation and the performance evaluation of the protocol USHR require a group signature generation and two point multiplications in the first process. In the route discovery process, each node except the source node and destination node needs one ID-based encryption/decryption, while the source node and destination node have two ID-based encryption/decryption. The simulation results and comparisons of the proposed system were executed and analyzed using Network Simulator version 2.34. In the simulation, 100 nodes are randomly distributed within a network field of size 650m x 650m as such a rectangle field can make the number of hops between two nodes larger. Mobile nodes are moving in the field according to the random way point model, and the speed ranges from 0 to 20m/s. packet losses for USHR and USOR protocol. Packet loss occurs when one or more packets of data travelling across a network fail to reach their destination. Dropping packets when the queue is full is a poor solution for any connection that requires real-time throughput. In cases where quality of service is rate limiting a connection, packets may be intentionally dropped in order to slow down specific services to ensure available bandwidth for other services marked with higher importance. For this reason, packet loss is not necessarily an indication of poor connection reliability or a bottleneck. According to the simulation results presented in Fig-2, by taking x-axis as number of packets and y-axis as path length.

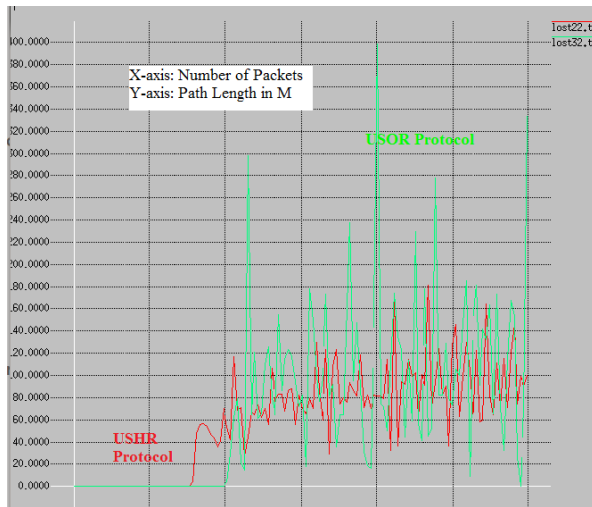


Figure 2. Packet losses for USHR and USOR protocol

Network capacity is the maximum capacity of a link or network path to convey data from one location in the network to another. Network capacity is the measurement of the number of links or paths that can be occupied to transfer the data from one node to another node in the large network. Network capacity is one of the scarce resources which has been used in efficient ways to occupy a large number of paths or links which has to provide outstanding throughput. Throughput increases in both protocols with increasing pause time, even though it is increased more dramatically in USOR protocol. In USOR, capacity shows a big growth from

40kbits/sec at pause time 0 sec to 91kbits/sec at pause time 110 sec. In contrast, throughput in USOR is 81 Kbit/sec at pause time 0 sec and increases by approximately 20 Kbit/sec at pause time 110 sec. At low pause time, the network topology will change frequently, more broken links will occur and the discovery process will be needed more. As a consequence, there will be a greater routing overhead and packets will be dropped resulting in less delay and more capacity. In USHR, throughput shows a big growth from 40kbits/sec at pause time 0 sec to 95kbits/sec at pause time 110 sec. By taking X-axis as Number of Packets and Y-axis as Bandwidth Utilization in mbps value obtained from the trace file. Fig.3 illustrates the Network capacity for USHR, USOR and AODV Protocol. The better performance is shown by USHR. The performance values are specified in table-2.

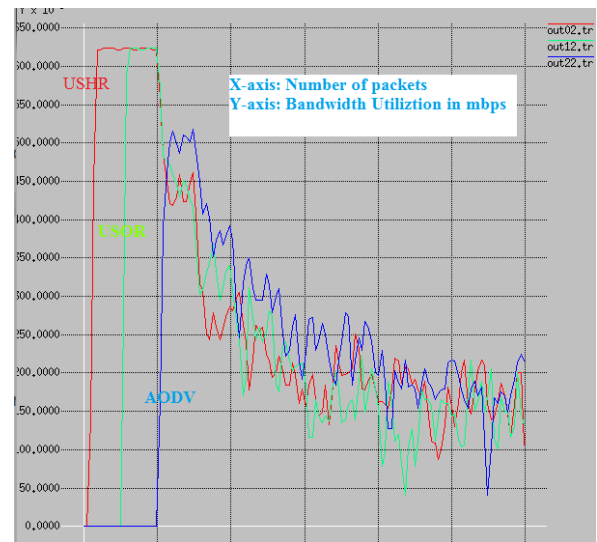


Figure 3. Network capacity for USHR, USOR and AODV routing protocol

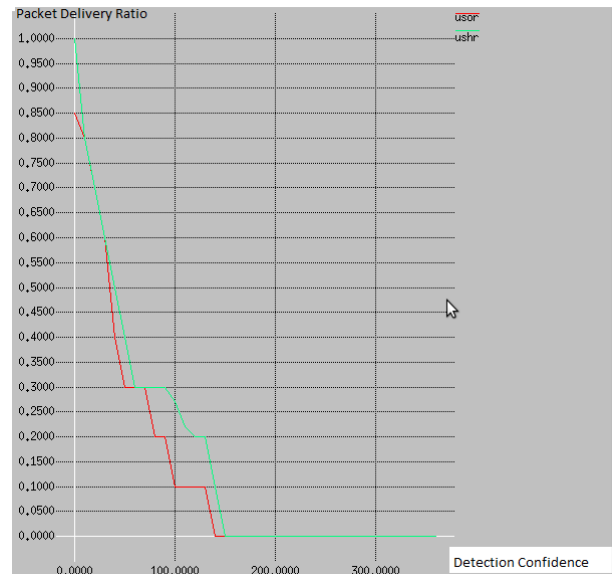


Figure 4. Performance comparison for USHR and USOR Protocol

Table 2. Performance Comparison for USHR and USOR protocol

ROUTING PROTOCOL	USHR	USOR
PERFORMANCE	1	0.85

Packet delivery ratio is calculated by dividing the number of packets received by the destination through the number of packets originated by the application layer of the source (i.e. Constant Bit Rate (CBR)). It specifies the packet loss rate, which limits the Maximum throughput of the network. Fig.4 illustrates the performance comparison for USHR and USOR Protocol. By taking x-axis as detection confidence index value and y-axis as packet delivery ratio.

6. Conclusion

In this paper a secure hybrid routing protocol based on unobservable identity in MANET was presented. The proposed scheme is featured as an effective security that can effectively minimize the delay, maximize the network coverage, and computational complexity and greatly improves the performance compared with the USHR protocol based advanced hashing technique scheme. The proposed secure hybrid routing protocol based on unobservable identity in MANET scheme completely offers privacy preserving routing the other USHR protocol with lower packet loss and enhanced network performance. The simulation results and comparisons of the proposed system were executed and analyzed using NS2. It was observed that the performance of the USHR protocol is increased and the network delay, network capacity and also the packet losses in the networks are calculated. Privacy preserving routing was implemented using USHR protocol based advanced hashing technique. To further enhance the performance, USHR protocol can be implemented in wireless sensor networks with a motive to enhance life of the network with reduced

power consumption.

REFERENCES

- [1] S. Capkun, L. Buttyan, and J. Hubaux, Self-Organized Public-Key Management for Mobile Ad-hoc Networks, *IEEE Transaction Mobile Computing*, Vol. 2, No. 1, 52-64 ,2003.
- [2] A. Boukerche, K. El-Khatib, L. Xu, and L. Korba, SDAR: A Secure Distributed Anonymous Routing protocol for wireless and mobile ad-hoc networks, *IEEE Local Computer Networks*, pp. 618-624, 2004.
- [3] Y. Zhang, W. Liu, and W. Lou, Anonymous Communications in Mobile Ad-hoc Networks, *IEEE Informatics And Communication*, pp. 125-138, 2005.
- [4] L. Song, L. Korba, and G. Yee, AnonDSR: Efficient Anonymous Dynamic Source Routing for mobile ad-hoc networks', *Proceeding ACM Workshop on Security of Ad-hoc and Sensor Networks*, Vol.3, No.10, 32-42, 2005
- [5] S. Seys and B. Preneel, ARM: Anonymous Routing Protocol for Mobile Ad-hoc Networks', *IEEE International Conference on Advanced Information Networking and Applications*, pp.1-11, 2006
- [6] D. Sy, R. Chen, and L. Bao, ODAR: On-Demand Anonymous Routing in Ad-hoc Networks, *IEEE Conference on Mobile Ad-hoc and Sensor Systems*, Vol. 4, 721-730, 2006
- [7] Karim El Defrawy, and Gene Tsudik, Privacy-Preserving Location-Based On-Demand Routing in MANETs, *IEEE Journal. Selected. Areas in Communication*, Vol. 29, No. 10, 1926-1934, 2011.
- [8] K. E. Defrawy and G. Tsudik, 'ALARM: Anonymous Location-Aided Routing in suspicious MANETs, *IEEE Transaction in Mobile Computing.*, Vol. 10, No. 9, 1345-1358, 2011.