Performance Analysis of Location Privacy Preserving Scheme for MANETs

Bhawani Shanker Bhati and Pallapa Venkataram
(Corresponding author: Pallapa Venkataram)

Protocol Engineering and Technology Unit, Department of ECE, Indian Institute of Science
Bangalore 560012, India
(Email: pallapa@ece.iisc.ernet.in)

(Received June 24, 2014; revised and accepted Jan. 16 & June 13, 2015)

Abstract

We consider the problem of preserving node's location privacy which is essential for minimizing the attacks during multi-hop routing in MANETs. As by intercepting and analyzing the transmitted packets, intermediate nodes (conventionally, assumed to be trustworthy) can track sender and receiver nodes, and can also trace the route between them. Earlier approaches attempts to preserve the location privacy by changing node-IDs or masking the location information, but results in high cost and degradation of service quality. To overcome these drawbacks, this paper presents: 1) a novel rough set based Location Privacy Preserving (LPP) scheme during route establishment; and 2) an efficient Data Transfer scheme for Location Privacy Preserving based Routes (DTLPPR) during data transfer. Analysis of trustworthiness of neighbor nodes using Discrete Time Markov Chain, and proposed scheme in terms of *location privacy* and *route untraceability* is presented. Analytical work is validated using simulations.

Keywords: Location privacy, mobile ad hoc networks, rough set, route untraceability, trust attributes

1 Introduction

The self-organizing, decentralized and infra-structureless features of MANETs provide a promising solution for several real world applications [4]. The nodes functions as both a router and a host, and communicate with other nodes which are not in its transmission range through intermediate nodes by establishing a route and then transferring the data packets. Though nodes are considered to be trustworthy, but a few nodes might be malicious and launch attacks: 1) by using the information such as sender/receiver identity, locations, neighborhood, etc.; and 2) by overhearing and analyzing the data packets over wireless links. Thus, malicious nodes can track the location of a mobile node, and can also trace the route [10]. Location of the nodes is utilized to reduce overhead and achieve high throughput with low delay [7]. However, if the user's mobility or location is not safeguarded, malicious node can build user mobility profile and link the information to user identities or addresses.

1.1 Location Privacy

The unsought for leak of location and analysis of overheard data packets, results in location breach, thereby launching attacks which can disrupt MANET. Thus, location privacy preserving scheme is a critical requirement for minimizing the attacks, and also for the successful operation of MANET. Location privacy prevents sender and receiver from being revealed to any untrusted nodes, and also provides an untraceable route. Most of the earlier works, rely on: (1) Changing the node identity (node-ID); or (2) Masking of the location information by adding noise. However, they result in high cost and degradation of service quality. In addition, limited resource is one of the major problems. As a result, earlier works are unsuitable for resource constraint MANET. This necessitates the development of a low cost scheme to preserve location privacy without affecting the services.

1.2 Proposed Location Privacy Preserving Scheme

In order to preserve the location privacy, we propose a novel rough set based Location Privacy Preserving (LPP) scheme, and an efficient Data Transfer scheme for Location Privacy Preserving based Routes (DTLPPR). LPP scheme, establishes an untraceable route through trusted nodes (acts as temporary sender for their next hop), where trust value is determined by the trust attributes (defined using Rough set theory). In DTLPPR scheme, sender (or temporary sender) node randomly generates a challenge in *challenge generation period.* For every challenge received, trusted neighbor node sends back a response message to its sender. We mention that, sender (or temporary sender) node selects two trusted neighbor nodes, one extra node for backup to overcome data loss due to route failures. The proposed schemes can be used for any ad hoc network by adapting the nature of communications and security challenges of that network, however, in this work we consider MANET. We theoretically analyze the trustworthiness, location privacy and route untraceability. The performance of proposed scheme is evaluated by performing simulations, and also comparing with earlier works. The contributions of this paper are: (1) *Location Privacy* - Preserving location privacy of sender and receiver nodes, by not revealing who are the originator and receiver of data packets to any node, except the designated trusted intermediate nodes; (2) *Route Untraceability* - Route established is not revealed, i.e., malicious nodes cannot identify the trusted intermediate nodes; (3) *Trustworthiness of neighborhood* - A Discrete Time Markov Model is proposed to evaluate the trustworthiness; and (4) *Data Transfer scheme* - Strengthening the location privacy, by ensuring that data is received by designated trusted node.

1.3 Organization of The Paper

The rest of the paper is organized as follows. In Sections 2 and 3, some of the earlier works and definitions used are given, respectively. Section 4, explains proposed location privacy scheme. Section 5, discusses the performance of proposed scheme against some of the attacks. We theoretically analyze the proposed scheme in Section 6, and provide simulation results in Section 7. Finally, we conclude in Section 8.

2 Related Works

Earlier works on preserving location privacy, rely on changing the node-IDs [2, 9, 20, 26, 31] or masking of the location information by adding noise [11, 21, 27, 28]. In the former approach, a node uses pseudonyms instead of real node-ID. Further, to strengthen the location privacy, nodes change their pseudonyms time-to-time [2], which makes it difficult for an attacker node to link the data packets for longer time period. In [19], authors discuss the impact on the performance due to frequently changing node-IDs for the Vehicular Adhoc Network (VANET). The major challenges faced are: when to change the pseudonyms, and how to conceal the relevance between old and new pseudonyms. For example, density of neighbor vehicles is used as a threshold value for pseudonym change [20]. In [26], the receiver node's location is exposed for route discovery, and then pseudo identifiers of communicating nodes are used for data delivery. MASK [31] enables both network-layer and MAC-layer communications without disclosing real identities. ANODR [9], assigns a random route pseudonym to each hop on the route to provide an untraceable and intrusion tolerant routing. However, MASK and ANODR introduces high overheads due to changing pseudonyms. In the later approach, location information is safeguarded by adding noise to original location information. A geographical mask [11], is used to add deterministic or stochastic noise to original location of a point. A similar approach is presented in [21], where the location information is perturbed by different levels for different groups, thus allowing obfuscation of a mobile node's exact location. As location information is perturbed, there is degradation in service quality. An approach to achieve receiver anonymity is presented in [27] that uses fuzzy receiver positions, and the data packets for a receiver node are delivered to nodes within a geographical area called anonymity zone. [28] preserves node's location information by defining a safety level. If a region has high safety level, then it is less likely for an attacker to determine the nodes within that region. In [32], the location privacy is preserved by dissociating node's location information and identity. In [3] presents, two schemes SECLOUD to conceal the true sender/receiver nodes, i.e., the attacker cannot identify the true sender/receiver; and ANONYRING to hide the sender/receiver nodes within a group of nodes forming a ring. The techniques given in [5] focuses on passive routing attacks, and addresses venue anonymity, privacy of network topology and privacy of node's motion pattern. In [24], by combining signature and Weil Pairing, an anonymous and authenticated communication scheme in VANET, namely ATCS, is presented. [1] prevent driver's (node in VANET) privacy by using a security scheme, where authentication and driver's privacy trade-offs are discussed. However, [3, 32, 24] and [1], does not consider route untraceability. Earlier works on preserving location privacy, mainly focus on the route establishment stage, and do not pay much attention to data transfer stage. [30] address issues on anonymous authentication, and proposes an efficient communication protocol for VANET based on conditionally anonymous ring signature. [13] points out security pitfalls of important secure routing protocols. and also propose a secure routing protocol against active attackers using digital signatures. [30] and [13] do not consider the passive attackers.

3 Definitions

3.1 Rough Sets

Rough set theory introduced in early 1980's [15] is used extensively in various fields [23], mainly for reasoning about knowledge and classification. The data is represented using an information table, denoted as $I = < U, A, V, f >$, where U is a non-empty finite set of objects called universe, A is a non-empty finite set of attributes, $V = V_{a_1} \cup V_{a_2} \cup ...V_{a_K}$ (V_{a_i} is the value of the attribute 'a_i') and 'f' is an information function which appoints the attribute value to every object in U. Table 1 represents set of all neighbor nodes as universe and their trust attributes as set of attributes. Trust attributes considered are Node History (NodeHist), Node Reliability

Table 1: Rough set concepts for trust in MANET

Symbol	**Definition**
$U = \{n_1, n_2, ..., n_M\}$	Non - empty finite set of 1-hop neighbor nodes
$A = \{a_1, a_2, ..., a_K\}$	Non - empty finite set of attributes: Node History, Resource Availability and Node Reliability
V_{a_i}	Value of the attribute 'a_i'

Table 2: Node history (NodeHist) attribute values

Packets Forwarded(%)	**Packets Dropped(%)**	**NodeHist Value**
[0,51)	[51,100]	1 (= suspicious)
[0,51)	[0,51)	2 (= normal)
[51,100]	[0,51)	3 (= good)

Table 3: Node reliability (NodeRel) attribute values

Link Stability	**NNTT**	**NodeRel Value**
Low	Medium	1
Low	High	
Medium	High	
Low	Low	2
Medium	Medium	
High	High	
Medium	Low	3
High	Low	
High	Medium	

Table 4: Resource availability (RscAvl) attribute values

Bandwidth	**Battery Power**	**RscAvl Value**
Low	Low	1 (= Low)
Low	Medium	
Medium	Low	
Medium	Medium	2 (= Medium)
High	Low	
Low	high	
Medium	High	3 (= High)
High	Medium	
High	High	

(NodeRel) and Resource Availability (RscAvl). Rough set concepts, classify the nodes into three separate regions: positive region (PosR), negative region (NegR) and boundary region (BndR), based on their trust attributes. Considering, $T \subseteq A$ and $Y \subseteq U$, then the approximation of Y is determined based on the information in T, by finding *T-lower* ($T_l(Y) = \{e \in U | [e]_T \subseteq Y\}$) and *T-upper* ($T_u(Y) = \{e \in U | [e]_T \cap Y \neq \phi\}$) approximations of Y. $[e]_T$ is the equivalence classes of *T-indiscernibility* relation. The nodes in $T_l(Y)$ can be certainly the elements of Y and the nodes in $T_u(Y)$ can be possible elements of Y, based on the trust attributes in T. Using the $T_l(Y)$ and $T_u(Y)$, universe U is divided into three disjoint regions: (1) *Positive region*, PosR(Y) = $T_l(Y)$; (2) *Negative region*, NegR(Y) = U - $T_u(Y)$; and (3) *Boundary region*: BndR(Y) = $T_u(Y)$ - $T_l(Y)$. In this paper, we define trusted neighbor nodes as PosR, non-trusted neighbor nodes as NegR and medium trusted neighbor nodes as BndR. However, we mainly focus on positive region for determining the trustworthiness, which is explained in Section 6.1.

3.2 Trust Attributes

The trustworthiness is determined based on trust attributes (see Table 1). Now, we briefly describe each one of these trust attributes: (1) **Node History** reflects the behavior of a node, and it depends on percentage of packets forwarded (ratio of number of packets forwarded to number of packets received) and percentage of packets dropped (ratio of number of packets dropped due to malicious behavior to number of packets received), where no feedback about the packet drop indicates a malicious behavior and the packet drop count (due to malicious behavior) is incremented; (2) **Node Reliability** indicates node's ability to provide higher delivery rates and to minimize the number of route failures, and it depends on Neighbor Node's Traversal Time (NNTT) and link stability between nodes. The NNTT is defined as the time taken by a node on average to process a packet. For simplicity, we consider that the NNTT and link stability parameters can be low, medium or high based on predefined threshold values, and Table 3 shows the values that can be taken by node reliability attribute. The link stability can be measured based on signal strength, where 'low' indicates that link between nodes will expire soon and 'high' indicates that link between nodes will sustain for longer time; (3) **Resource Availability** indicates the nodes richness in terms of availability of resources to support applications, and depends on bandwidth and battery power. We consider that the bandwidth and battery power resource values can be low, medium or high based on application dependent threshold values. Table 4 shows the values that can be taken by resource availability attribute. We mention that the node reliability attribute parameters can be assigned finer values, for example: very low, low, medium, high and very high values. Similarly, we can assign finer values to node history attribute parameters and resource availability attribute parameters. However, for simplicity we have assigned the parameter values as shown in Tables 2, 3 and 4.

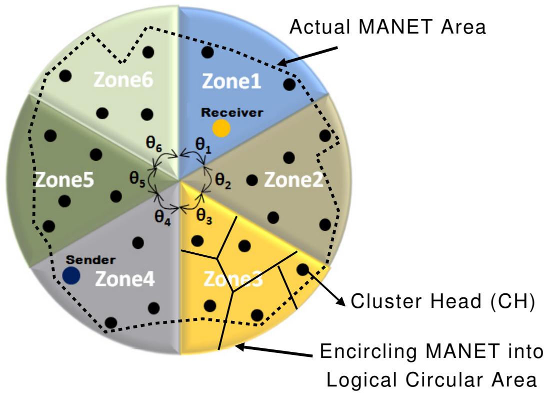


Figure 1: MANET division into 6 zones

4 Proposed Location Privacy Scheme

In this Section, we discuss our proposed rough set based location privacy scheme. First, we describe the network and attack models, and then details on tracing of trust attributes, construction of information tables and selection of trusted neighbor node is provided. Finally, we present our proposed schemes LPP and DTLPPR in detail.

4.1 MANET Model

We assume that a MANET is built with bidirectional wireless links. As earlier works [27, 32], we assume that every node have the knowledge of their positions (e.g., through GPS, WiFi-based positioning system), and a node can get the position information of other nodes using any secure positioning service [12, 25]. We assume that MANET is logically divided into 'N' number of zones (see [8]). However, we assume that area of MANET is circular in nature and it is divide into six zones, as shown in Figure 1. The MANET is divide into zones of equal angles ($\theta_1 = \theta_2 = \theta_3 = \theta_4 = \theta_5 = \theta_6 = \theta = 60°$) with respect to the center of MANET. In the case, when MANET is not circular, we encircle the MANET into a logical circular area to enable zone formation. The zones are further divided into clusters by considering a node as a cluster head (node with high resources) having set of nodes at most 2-hops away, and maintaining trust attribute values for the nodes within its cluster.

4.2 Attack Model

Threats in MANET may come from within as well as from outside. The attackers from outside (or external attackers), are able to passively receive data packets within their hearing range, and then determine the location and identity of node sending the data packets. On the other hand, attackers from within (or internal attackers) are the active nodes pretending to be legitimate node and sending packets to gain knowledge about other nodes location and identity. Earlier works have focused on active attacks which are done through viruses or Trojans. In this work, we focus on the passive attacks, where we consider that the attackers have following goals: (1) Obtain information such as sender and receiver nodes of the data packets; and (2) Trace the route taken by the data packets. By analyzing the traffic, an attacker can obtain these information. We mention some of the attacks [17] due to traffic analysis: (1) *Packet Tracing Attack* - By overhearing transmission of data packets as they traverse from sender to receiver, an attacker may determine the communicating nodes and also trace the route; and (2) *Timing Analysis Attack* - An attacker can monitor the packet departure and packet arrival times, and use this information to determine the sender and receiver. The attackers can overhear the transmission of data packets within their hearing range. However, their computing resources are limited, i.e., encrypted data cannot be decrypted easily, and the attacker cannot locate the nodes using secure position service.

4.3 Tracing Trust Attributes

To provide confidentiality during zone-based tracing of trust attributes, nodes use t-degree polynomial functions [22] to privately send information to their neighbor nodes and cluster head. A node-n (in zone Z_1) should be aware of the functions $h_{1,l}(x)$, where $l = 1, 2, ..., 6$ (six zones). The first index and second index in function $h_{k,l}(x)$ represents destination zone-id (k) and source zone-id (l) of the information packets, respectively. When node-n in Z_1 sends its information to node in Z_2, it sends out an encrypted packet (encrypting using key determined from t-degree polynomial) $E_{h_{2,1}(n)}$(node-n, *information*, *timestamp*). The "*information*" field consists parameter values of trust attributes (eg., battery power status, NNTT, etc.) and "*timestamp*" field indicates freshness of the information. When neighbor nodes of node-n receive this information, they make an entry in their Neighbor Node Information Table (NNIT). Similarly, nodes within a cluster send information to their cluster head, and the cluster head makes an entry in its Cluster Node Information Table (CNIT). However, in this case, nodes use cluster-id instead of destination zone-id, and its own node-id instead of source zone-id.

4.4 Information Table

The nodes and cluster heads represent the received information in the form of NNIT and CNIT, respectively. The row of NNIT represents the neighbor nodes and each column represents their trust attributes. Table 5 shows an example of NNIT at node-S, with A, B, C, D, E, F and G as neighbor nodes (for Figure 2). Here, we consider node history (*TA-1*), node reliability (*TA-2*) and resource availability (*TA-3*) as trust attributes for neighbor nodes. The CNIT is similar to NNIT, except that it has information on all the nodes within cluster. The

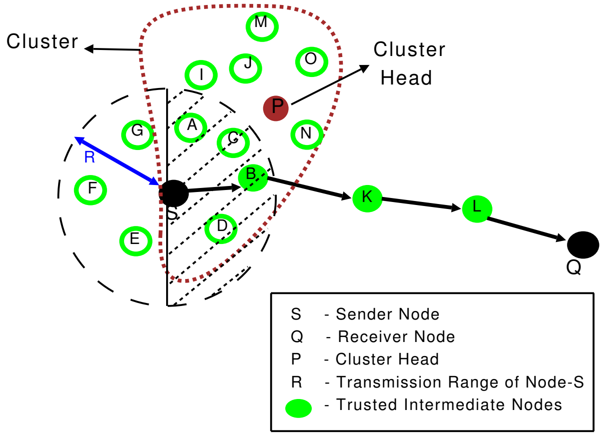


Figure 2: Node-S with its neighborhood and cluster head node-P

Table 5: Rough set based NNIT at node-S

Node-S	*TA-1*	*TA-2*	*TA-3*
A	2	1	2
B	3	3	2
C	2	1	2
D	1	1	2
E	3	2	3
F	1	1	2
G	3	1	2

Table 6: Rough set based CNIT at cluster head-P

Cluster Head-P	*TA-1*	*TA-2*	*TA-3*
A	1	3	1
B	2	3	2
C	1	2	3
D	3	1	2
I	1	1	1
J	3	1	1
M	1	1	3
N	3	1	2
O	3	2	1
S	1	2	3

row in CNIT represents cluster members and each column represents their trust attributes, as shown in Table 6 (for Figure 2).

4.5 Trusted 1-hop Neighbor Node Selection

The selection of trusted node is to: (1) Save node's power by avoiding unnecessary transmission. (2) Effectively utilize the bandwidth. (3) Increase the packet delivery rate. (4) Provide location privacy. The sender (or temporary sender) selects a trusted node among its neighbor nodes with the highest trust value. The trust value of a node-k, calculated by node-i (denoted as TV_k^i) is given by, $TV_k^i = \beta * TV_k^i + (1-\beta) * TV_k^{CH}$. β is the self-weightage factor, first term $(TV_k^i = \sum_j (W_j^k * V_j^k(nnit)))$ is direct trust calculated by the sender (or temporary sender) and second term $(TV_k^{CH} = \sum_j (W_j^k * V_j^k(cnit)))$ is indirect trust calculated based on the feedback from node-k's cluster head. W_j^k is the weight assigned to trust attribute-j for node-k, $j \in \{$NodeRel, NodeHist, RscAvl$\}$, $V_j^k(nnit)$ and $V_j^k(cnit)$ are the values of trust attribute-j for node-k from NNIT and CNIT, respectively. As, sender node has knowledge of the receiver's position (using secure position service), trust value is calculated only for neighbor nodes towards receiver node, i.e., neighbor nodes within shaded region of Figure 2. For example, in Figure 2, node-B and node-C are selected for data transmission and backup, respectively (by assigning equal weights to trust attributes and $\beta = 0.6$).

4.6 Location Privacy Preserving (LPP) Scheme

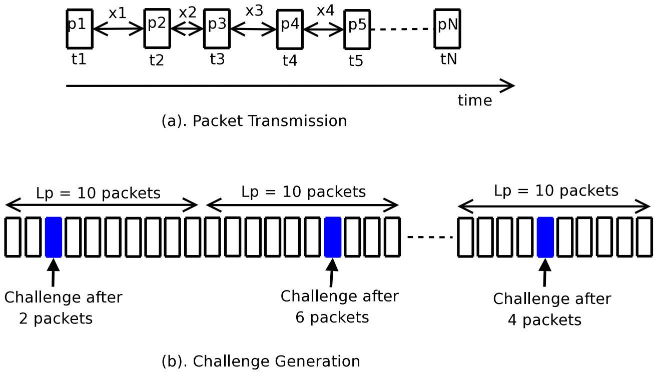
LPP scheme establishes an untraceable route, while preserving location privacy. First, nodes privately send information to their neighbor nodes and also to cluster head (see Section 4.3). Second, each node maintains a NNIT, and cluster head maintains a CNIT (see Section 4.4). Third, NNIT and CNIT are used to determine the trusted neighbor nodes (see Section 4.5). Finally, an untraceable route is established.

4.6.1 Route Establishment With Trusted Neighbor Nodes

When a sender has data for a receiver, and if there is no trusted neighbor node (towards receiver) in sender's routing table, then route establishment stage (hop-by-hop basis) is initiated, as explained here. Sender selects a trusted neighbor node (with highest trust value), and then establishes connection with it, using route request (rreq) and route reply (rrep) messages, and finally transmits the data packets to selected trusted neighbor node. Since, rreq and rrep messages are sent only to selected trusted neighbor node, there is a decrease in message overhead compared to broadcasting of rreq message in some of the earlier works. Now, selected trusted neighbor node acts as a temporary sender and establishes connection with its trusted neighbor node (towards receiver), and this process is continued till the receiver. The format of rreq message is: $<$ *type, rreq-id, trusted neighbor node's address, originator's address* $>$, where *type* indicates rreq message, *rreq-id* is rreq id number and *originator's address* is sender (or temporary sender) node's address; and the format of rrep message is: $<$ *type, rreq-id, trusted neighbor node's address, originator's address* $>$, where *type* is rrep message. Since, receiver's address is not used in rreq and rrep messages, attacker cannot obtain the information regarding receiver. Here, we assume that a sender (or temporary sender) knows trusted neighbor node's public key. As, data packet has to be sent only to trusted neighbor node, sender (or temporary sender) sets TTL $= 1$. The data packet format is $< Trapdoor, data >$, where Trapdoor (TD) information is obtained by encrypting the concatenated information using selected trusted neighbor node's public key. The TD information is given by, $TD = E_{PuK\_k}(S\_Ad||k\_Ad||D\_Ad||Dp)$, where, S_Ad is sender (or temporary sender) node's address, k_Ad is selected trusted neighbor node-k's address, D_Ad is receiver node's address, Dp is receiver node's position and $||$ represents concatenation operation. The data part corresponds to different layer protocols and original data to be sent. The trusted neighbor node decrypts the TD using his private key, whereas other neighbor nodes can only overhear transmission, but cannot decrypt it. The trusted neighbor node compares D_Ad with its own address and realizes that it is not the receiver, and then it acts as a temporary sender and transmits the data packets. In the case, when receiver is 1-hop away, TD information contains concatenation of only node-k's address and receiver node's address. In literature, source routing [6] and sequence numbers [16] are used to avoid loops in a route, but they can disclose communicating nodes location, and thus cannot be used in location privacy scheme. In LPP scheme, data packets are forwarded to only trusted neighbor node, which reduces the distance to receiver in each routing step, and it leads to a loop-free routing. Since, trusted neighbor nodes has knowledge of only previous hop (acting as temporary sender), the original sender node's location privacy is preserved, and we see that the identity of original sender is also preserved. The other neighbor nodes, which cannot decrypt the data packets, are unable to determine receiver, and thus location privacy of receiver is preserved. In the case of receiver, its information is disclosed only to trusted intermediate nodes. To preserve the location privacy, control messages (rreq, rrep etc.) are encrypted, so that they cannot be differentiated from other data packets. We mention that the routing table at each node maintains information on trusted neighbor node towards receiver with their timeout values and rreq-id.

4.6.2 Established Route Is Untraceable

An attacker can overhear the data packets transmitted over wireless links by a node, and identify it as a sender, but cannot determine whether it is the original sender or an trusted intermediate node. The neighbors of a sender which cannot decrypt the TD, confuse the attacker by sending data packets to all their neighbors with an invalid TTL (indicating receiving nodes to discard data packets). Thus, an attacker cannot differentiate between the original sender and other neighbors. Similarly, trusted intermediate nodes and their neighbor nodes confuse the attacker, until receiver node is reached. The neighbor nodes of trusted intermediate nodes are called as participating (or supporting) nodes, because they participate (or support) in providing an untraceable route. When receiver node receives the data packet, it again transmits the data packet with an invalid TTL to its neighbor nodes, i.e., the receiver acts as a temporary sender, and the neighbor nodes of receiver confuse the attacker by sending data packets to their neighbor nodes with an invalid TTL. Thus, it becomes difficult for an attacker to trace the route.



(a). Packet Transmission

(b). Challenge Generation

Figure 3: Data transfer scheme for location privacy preserving based routes (DTLPPR)

4.7 Data Transfer Scheme For Location Privacy Preserving Based Routes (DTLPPR)

To ensure that the data packets has reached designated trusted neighbor node, DTLPPR scheme is proposed, where a sender (or temporary sender) randomly generates a challenge for every 'L_p' number of data packets sent to next hop, and in reply, a response is generated by the next hop. Also, to strengthen LPP scheme, time between transmission of each data packet is varied at every hop during data transfer stage, i.e., if packet 'p1' is sent at time 't1', then packet 'p2' is sent at time 't2' (t2 = t1 + x1) and so on. The values of x1, x2, ..., are different (generated randomly), so that it becomes difficult for an attacker to identify sender and receiver based on their packet departure and arrival times, respectively. The Figure 3(a) shows packet transmission in DTLPPR scheme.

4.7.1 Challenge Generation Period

The challenge generation period indicates the number of data packets (L_p) for which, a sender (or temporary sender) node randomly generates a challenge, and it is determined using challenge attribute. By using rough set theory, challenge attribute (denoted as ch) takes value as shown in the Table 7, which is dependent on parameters: 1)*sensitivity of the data packets* (*or data sensitivity*), and 2) *trustworthiness* of selected trusted neighbor node. The *data sensitivity* and *trustworthiness* value is divided into levels - low and high. Original sender node decides *data sensitivity*, and *trustworthiness* is determined

Table 7: Challenge attribute (ch) Values

Data Sensitivity	**Trustworthiness**	**Value**
[0, 0.5]	[2, 3]	Low = 1
[0, 0.5]	[1, 2)	Medium = 2
(0.5, 1]	[2, 3]	
(0.5, 1]	[1,2)	High = 3

as described in Section 4.5. The *data sensitivity* value is sent to trusted neighbor node acting as temporary sender (during data transmission). If *data sensitivity* is low and *trustworthiness* of selected trusted neighbor node is high, then challenge attribute takes lowest value (indicating low challenge generation period or L_p). As *data sensitivity* increases and/or *trustworthiness* of selected neighbor node decreases, challenge generation period is increased. We mention that, for simplicity, values of challenge attribute are low (=1), medium (=2) and high (=3). The challenge generation period is determined using, $L_p = L_d * 2^{ch}$, where, L_d is a design parameter, indicating initial number of data packets decided by a sender (or temporary sender) node for generating a challenge at the start of data transfer. Later, sender (or temporary sender) node randomly generates a challenge within 'L_p'. For example, Figure 3(b) shows random generation of a challenge within L_p (= 10), where $L_d = 5$ and $ch = 1$.

4.7.2 Challenge - Response Messages

Sender (or temporary sender) ensures that the data packets has reached designated trusted neighbor node by randomly generating a challenge, and it is given by: $Challenge = [Op_i||n_i||k_i||fr_{flag}]$, where, n_i and k_i are two nonces generated by sender (or temporary sender) for packet-i, Op_i is operation to be done on two nonces for packet-i by the next hop and fr_{flag} is forwarding-rate flag. If fr_{flag} is set to 1, then forwarding-rate of next hop is required in response message, otherwise not required. A sender (or temporary sender) maintains forwarding-rate of next hop, and the counter is incremented for every packet forwarded by next hop. The next hop performs operation (Op_i) on two nonces n_i and k_i, and sends this result back to sender (or temporary sender) along with its forwarding-rate and number of packets received from sender (or temporary sender). The response generated by next hop is given by: $Response = [n_i(Op_i)k_i||fr_{tn}||N_{rx}]$, where, fr_{tn} is forwarding-rate of next hop and N_{rx} is number of packets received from sender (or temporary sender) at the time of response. If the values of 'n_i (Op_i) k_i' and fr_{tn} matches with the values calculated by sender (or temporary sender), then data transfer is continued. Otherwise, it terminates the data transfer and selects another trusted neighbor node or the backup node as next hop. The number of packets received N_{rx} is used by sender (or temporary sender) as a timestamp to obtain forwarding-rate of next hop, i.e, counter value at N_{rx}. We mention that, challenge and response messages are encrypted using next hop's and sender's (or temporary sender's) public key, respectively.

5 Location Privacy Protection Against Attacks

The performance of our proposed scheme against some of the attacks is discussed.

5.1 Timing Analysis Attack

Timing analysis attack [17], considers transmission of the data packets to be observable, and an attacker can locate sender and receiver using packet departure (at sender) and arrival (at receiver) times, respectively. In LPP scheme, neighbor nodes of a sender and receiver sends the data packets (with an invalid TTL) to their neighbors to provide covering feature to original data packets, and thus the attacker finds it difficult to locate the original sender and receiver. The location privacy of communicating nodes can be improved by considering two (or more) hops neighbor nodes, but it may result in high communication overheads. Also, we notice that the location privacy of nodes is strengthen by sending the data packets at different time intervals during data transfer stage (in DTLPPR scheme).

5.2 Packet Tracing Attack

Packet tracing attack [17] leads to a traceable route, i.e., intermediate nodes can be located by the attacker. In the proposed LPP scheme, participating nodes provide an untraceable route by sending data packets (with an invalid TTL) to their neighbor nodes. Notice that, there is an increase in number of participating nodes with increase in number of trusted intermediate nodes, which in turn increases the untraceability of route. The route untraceability is also improved in DTLPPR scheme, where trusted intermediate nodes send data packets at different time interval.

6 Analysis

In this section, we theoretically analyze our proposed schemes. First, we use rough set theory to determine the trusted neighbor node towards receiver. Second, we build a mathematical model for evaluating their trustworthiness. Later, we analyze the achieved location privacy in terms of *sender/receiver location privacy* and *route untraceability.*

6.1 Trusted 1-hop Neighbor Nodes

As explained in Section 3.1, neighbor nodes (from NNIT) or cluster members (from CNIT) in the positive regions are trusted node(s). First, we consider NNIT (Table 5), with $U_{nnit} = \{A, B, C, D, E, F, G\}$ be a set of neighbor nodes, $X_{nnit} = \{A, B, C, D\}$ to be set of neighbor nodes (towards receiver) and $T = \{TA-1, TA-2, TA-3\}$ to be subset of trust attributes. The lower and upper approximations of X_{nnit} are $T_l(X_{nnit}) = \{A, B, C\}$ and $T_u(X_{nnit}) = \{A, B, C, D, F\}$, respectively. So, from NNIT we obtain positive region as PosR$_{nnit} = \{A, B, C\}$. Second, we consider CNIT (Table 6), with $U_{cnit} = \{A, B, C, D, I, J, M, N, O, S\}$ is set of nodes within a cluster, $X_{cnit} = \{A, B, C, D\}$ to be set of cluster members (towards receiver) which are 1-hop away from sender (or temporary sender). We mention that, sets X_{nnit} and X_{cnit} have the same elements. From CNIT, we obtain positive region as PosR$_{cnit} = \{A, B\}$. Now, we take intersection of both the positive regions, i.e., *Required Positive Region* = PosR$_{nnit}$ $\bigcap$ PosR$_{cnit}$ $= \{A, B\}$. The trustworthiness of nodes A and B is determined, and node with highest trust value is selected for data transmission, whereas the other node as backup node. When there is only one node in the *Required Positive Region*, then we select that node for data transmission and backup node is selected from PosR$_{nnit}$ or PosR$_{cnit}$, however higher priority is given to PosR$_{nnit}$ (due to high self-weightage factor). If there are no nodes in *Required Positive Region*, then nodes are selected from PosR$_{nnit}$ or/and PosR$_{cnit}$, with higher priority given to PosR$_{nnit}$.

6.2 Trustworthiness Of Neighborhood Nodes

Trustworthiness depends on parameter values of trust attributes, and it may increase or decrease due to change in these parameter values. The change in trustworthiness is modelled as Discrete Time Markov Chain (DTMC) with M states, where state-*1* represents the lowest trustworthiness and state-M represents the highest trustworthiness (see Figure 4). Consider, a random variable $(Y_t)_{t \geq 0}$ representing the current trustworthiness corresponding to a given state of node. Trustworthiness takes value within $[TV_{low}, TV_{high}]$, where TV_{low} and TV_{high} represents low and high, i.e., state-*1* and state-M (in our scheme $TV_{low} = 1$ and $TV_{high} = 3$), respectively. The trustworthiness range $[TV_{low}, TV_{high}]$ is divide into M states with a step of δ ($\delta = \frac{1}{|A|}$), where $|A|$ is the cardinality of trust attribute set. The probability of transition from state-i to state-j, i.e., 1-step transition probability is: $P_{i,j}(t) = P(Y_t = j | Y_{t-1} = i); 1 \leq i, j \leq M$.

6.2.1 1-step Forward/Backward Transition Probability

The 1-step transition probabilities are dependent on change in trustworthiness, which in turn depends on change in its parameter values of trust attributes. If the current state is 'i' at time 't', and their is an improvement in parameter values, then trustworthiness transits to the state (*i+1*); otherwise if parameter values declines, then trustworthiness transits to the state (*i-1*). The trustworthiness can remain in the same state, if there is no change in parameter values. In our model, increase in trustworthiness is related to improvement in any one of the trust attribute parameter values. Assuming that at each instant of time, one of the parameter value is changed, then the forward transition probability (p) and backward transition probability (q) are, $p = p_{i,i+1} = \frac{1}{3}(p_I^{nr} + p_I^{nh} + p_I^{ra})$ and $q = p_{i,i-1} = \frac{1}{3}(p_D^{nr} + p_D^{nh} + p_D^{ra})$, respectively. p_I^{nr}, p_I^{nh} and p_I^{ra} are the probabilities of increase in node reliability, node history (positive behavior) and resource availability, respectively. Similarly, p_D^{nr}, p_D^{nh} and p_D^{ra} are the probabilities of decrease in node reliability, node history (negative behavior) and resource availability, respectively.

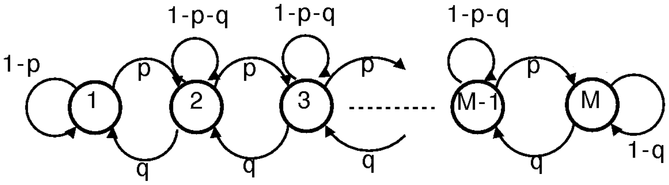


Figure 4: State transition diagram

Node Reliability

We assume that NNTT parameter values lies within a range $[NNTT^l_{min}, NNTT^k_{max}]$, where $NNTT^k_{max}$ and $NNTT^l_{min}$ are the maximum NNTT value taken by node-k and minimum NNTT value taken by node-l, respectively. The probability (p_{nt}) with which trustworthiness of node-n (with node traversal time = $NNTT_n$) increases due to NNTT parameter is, $p_{nt} = \frac{NNTT^k_{max} - NNTT_n}{NNTT^k_{max} - NNTT^l_{min}}$. The link stability parameter can be determined using distance between nodes. Assuming that all the nodes have same speed, then the link stability will be high for a neighbor node near to the sender or temporary sender node (as the link will be active for more duration). The probability (p_{ls}) with which trustworthiness of node-n (at a distance D_n from the sender/temporary sender node) increases is, $p_{ls} = 1 - \frac{D_n}{R}$, where R is the transmission range of node. Thus, probabilities with which the trustworthiness increases and decreases (due to node reliability trust attribute) are, $p_I^{nr} = p_{nt} * p_{ls}$ and $p_D^{nr} = (1 - p_{nt}) * (1 - p_{ls})$, respectively.

Node History

We represent parameters of node history trust attribute as forwarding rate (for percentage of packets forwarded) and dropping rate (for percentage of packets dropped). The forwarding rate (f_r) and dropping rate (d_r) is given by $f_r = \dfrac{N_{pf}}{N_{rx}}$ and $d_r = \dfrac{N_{pd}}{N_{rx}}$, respectively. N_{pf} is the number of packets forwarded, N_{pd} is the number of packets dropped and N_{rx} is the number of packets received. Thus, probabilities with which the trustworthiness increases and decreases (due to node history trust attribute) are, $p_I^{nh} = f_r*(1-d_r)$ and $p_D^{nh} = (1-f_r)*d_r$, respectively.

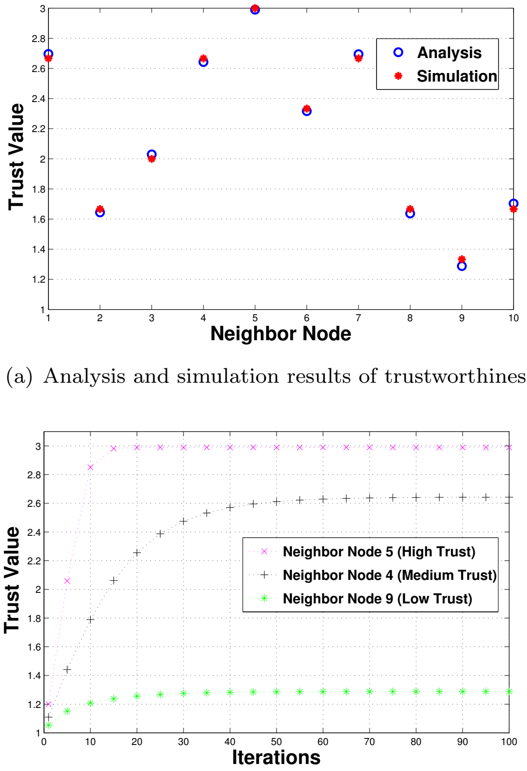
Resource Availability

We assume that, bandwidth availability lies within $[BW^u_{min}, BW^v_{max}]$, where BW^u_{min} is the minimum value at node-u and BW^v_{max} is the maximum value at node-v. Battery power availability lies within $[BP^f_{min}, BP^g_{max}]$, where BP^f_{min} is the minimum value at node-f and BP^g_{max} is the maximum value at node-g, respectively. The probability with which the trustworthiness increases and decreases (due to resource availability) are $p_I^{ra} = p_{bw} * p_{bp}$ and $p_D^{ra} = (1 - p_{bw}) * (1 - p_{bp})$, respectively. $p_{bw} = 1 - (\frac{BW^v_{max}-BW_n}{BW^v_{max}-BW^u_{min}})$ and $p_{bp} = 1 - (\frac{BP^g_{max}-BP_n}{BP^g_{max}-BP^f_{min}})$ are the probabilities that the trustworthiness increases due to bandwidth and battery power availability, respectively. BW_n and BP_n are bandwidth and battery power availability at node-n, respectively.

From the transition matrix T_m, we compute steady-state probabilities π_j, $j\in${1,2,...,M}. To validate, we consider a Markov chain as represented in Figure 4 with 7 states, where events are considered to arrive with Poisson process at arrival rate λ to simulate change in parameter values. The analysis and simulation parameters are given in Table 8. T_{bw} and T_{bp} are the total bandwidth and battery power, respectively, and T_{nntt} represents the highest NNTT. Finally, we compare the analytical results with simulation results. First, we evaluate the average trustworthiness, and Figure 5(a), shows the analysis and simulated trustworthiness of 10 neighbor nodes. The average trust values obtained by analysis are very close to simulated results. However, there are some slight differences due to the fact that, during simulations, trust values are calculated using the discretized values. Second, we investigate the speed of convergence (number of iterations) of trust value. We mention that, trust values are recalculated, when any one of the parameter values change. Figure 5(b), shows the number of iteration required for convergence of trust value for low, medium and high trust values. The speed of convergence depends on the state transition probabilities.

Table 8: Analysis and simulation parameters

Parameters	Value(s)
Transmission Range (R)	200m
Number of Neighbor Nodes	10
Mobility Model	Random Way Point
δ	0.33
λ	5 - 10
$[BW_{min}, BW_{max}]$	[30%, 90%] of T_{bw}
$[BP_{min}, BP_{max}]$	[30%, 90%] of T_{bp}
$[NNTT_{min}, NNTT_{max}]$	[30%, 90%] of T_{nntt}



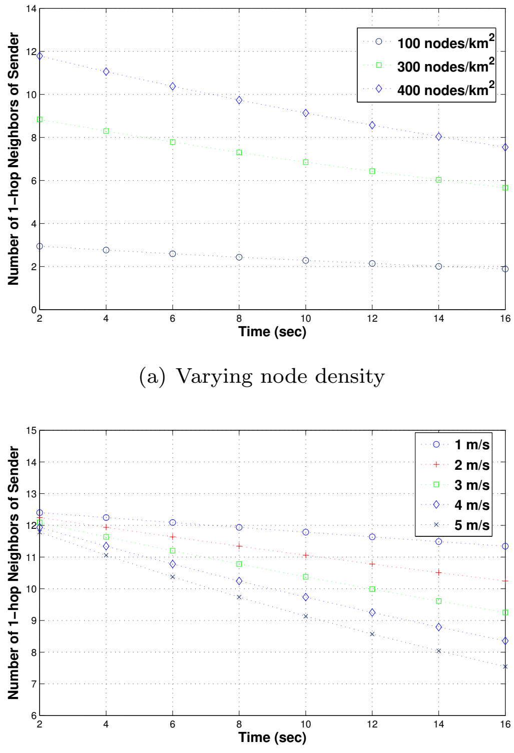
(a) Analysis and simulation results of trustworthiness

(b) Convergence of analysis trustworthiness

Figure 5: Trustworthiness of neighbor nodes

6.3 Sender/Receiver Location Privacy

The neighbor nodes of a sender and receiver confuse the attacker by providing covering feature to original sender's data packets, and also, receiver acts as a temporary sender. The location privacy of a sender or a receiver depends on number of neighbor nodes. From [27], probability ($p_s(t)$) that a node with mobility speed 'm' stays in the region after time 't', is exponentially distributed, $p_s(t) = e^{\frac{-t}{T_s}}$, where $T_s = \frac{\pi*A_r}{L_l*m}$ (A_r and L_l are the area and perimeter, respectively). For circular region with radius R, $T_s = \frac{\pi*R}{2*m}$. We calculate the number of nodes remaining in sender node's transmission range using node density (n_d) and mobility speed (m). The process of node mobility in sender node's transmission range is assumed to follow exponential distribution [27]. The duration of data transfer indicates elapsed time of nodes communication. The number of nodes remaining ($N_{rem}(t)$) in transmission range of a sender node after a time period 't' is, $N_{rem}(t) = p_s(t) * \pi * R^2 * n_d$. By considering the transmission range to be equal, receiver and sender have same location privacy. Figure 6(a) shows the remaining number of neighbor nodes at mobility speed of 5 m/s for varying node densities with time. We see that, as the node density decreases, the number of neighbor nodes remaining in transmission range drops and hence the location privacy decreases. We also see that, the remaining neighbor nodes decrease over time. Figure 6(b) shows the number of neighbor nodes remaining at node density 300 nodes/km^2 with varying node mobility speed with time. We see that, the number of neighbor nodes remaining within the transmission range decreases when the node mobility speed increases, so the location privacy decreases. Thus, location privacy is dependent on the node mobility, node density and also on transmission range.



(a) Varying node density

(b) Varying node speed

Figure 6: Estimated sender location privacy

6.4 Route Untraceability

The number of participating nodes determines the strength of untraceability, which is dependent on the number of trusted intermediate nodes (determined using number of hops). From [29], number of hops depends on: (i) The distance (d) between sender and receiver, and (ii) The remaining distance (Z) to the receiver.

To compute the expected number of hops, we assume that a node selects a trusted neighbor node within the link stability *'ls'* ($ls < R$) (see Figure 7). For using [29], circular MANET with radius R_m is approximated by square MANET with side length L_m, where the L_m is equal to ($\sqrt{\pi} * R_m$). Then, expected distance (r) between sender and trusted neighbor node is, $r = (\frac{2n_{des}}{2n_{des}+1} * ls)$. n_{des} is the number of neighbor nodes distributed over the shaded circle (see Figure 7). For simplicity, we consider that the neighbor nodes are uniformly distributed. Therefore, $n_{des} = \frac{N_{ls}}{2}$, where N_{ls} is all the neighbor nodes within range ls, and N_{ls} depends on node density (n_d) and ls. We consider that the selected trusted neighbor node may be anywhere on the boundary of semi-circle with radius r. From [29], expected remaining distance (Z) is given by,

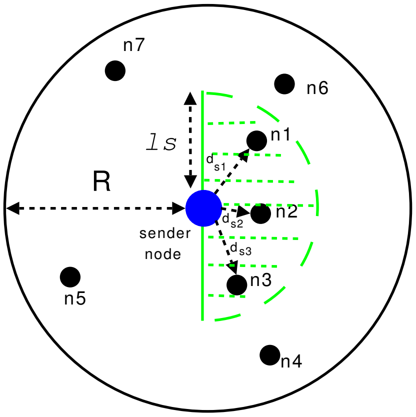


Figure 7: The distances between sender and its neighbor nodes within ls

$$Z = \int_{d-r}^{\sqrt{d^2+r^2}} Z f_Z(Z) dZ \qquad (1)$$

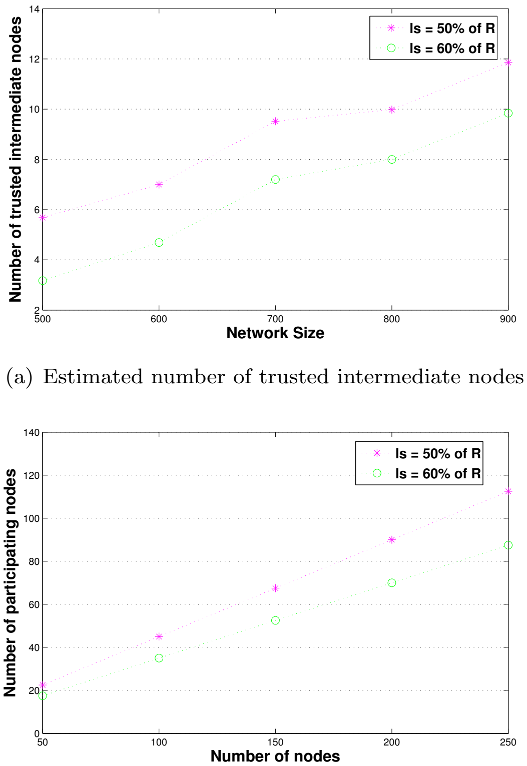
where, $f_Z(Z)$ is the pdf of Z, $f_Z(Z) = \frac{2Z}{\pi dr\sqrt{1-(\frac{d^2+r^2-Z^2}{2dr})^2}}$.

After determining Z for the first hop, *'d'* in the next hop is changed to Z (from Equation (1)). Then, by repeating the process and counting the hops until Z falls below ls, the number of trusted intermediate nodes can be determined. The *hop count* is dependent on ls, thus the ls should be chosen such that it minimizes the transmission cost (or hop count). In order to determine the number of participating nodes, number of neighbor nodes of trusted intermediate nodes is calculated. Considering the transmission range of nodes in MANETs to be the same and n_d to be node density, then the number of neighbor nodes (N_{1-hop}) for a node is, $N_{1-hop} = (\pi * R^2) * n_d$. In MANETs, trusted intermediate nodes can have overlapping transmission range and common neighbor nodes. We need to count these common neighbor nodes only once during calculation of participating nodes. The transmission range of two nodes intersect if the distance between them is less than (R). From geometry, area of intersection (A_{ij}) between node-i and node-j is, $A_{ij} = 2R^2 cos^{-1}(\frac{d_{ij}}{2R}) - \frac{1}{2} d_{ij}\sqrt{4R^2 - (d_{ij})^2}$. d_{ij} is distance between the two nodes i and j. Then, number of participating nodes (denoted as NP_{1-hop}) are,

$$NP_{1-hop} = (N_{TN} * N_{1-hop}) - \sum_{i,j,i \neq j} (n_d * A_{ij}) \qquad (2)$$

where N_{TN} is the number of trusted intermediate nodes, and i, j = 1,2,....,N_{TN}. The expected distance (r) is used as the distance d_{ij} between two nodes on the same link. Figures 8(a) and 8(b) shows the number of trusted intermediate nodes and number of participating nodes for varying ls (ls = 50% and 60% of R), respectively. The

R of the nodes is assumed to be 200m and the network size (circular MANET with radius, R_m) is varied. We see that, with the increase in network size, there is an increase in the number of trusted intermediate nodes. The number of trusted intermediate nodes decrease with increase in *ls*. The Figure 8(a) confirms that transmission cost is determined by the *ls*. The network size is kept constant at 700m and number of nodes is varied. In Figure 8(b), number of participating nodes increases for lower value of *ls*, i.e., route untraceability increases. However, it results in an increase in number of trusted intermediate nodes. The number of participating nodes increases with number of nodes.



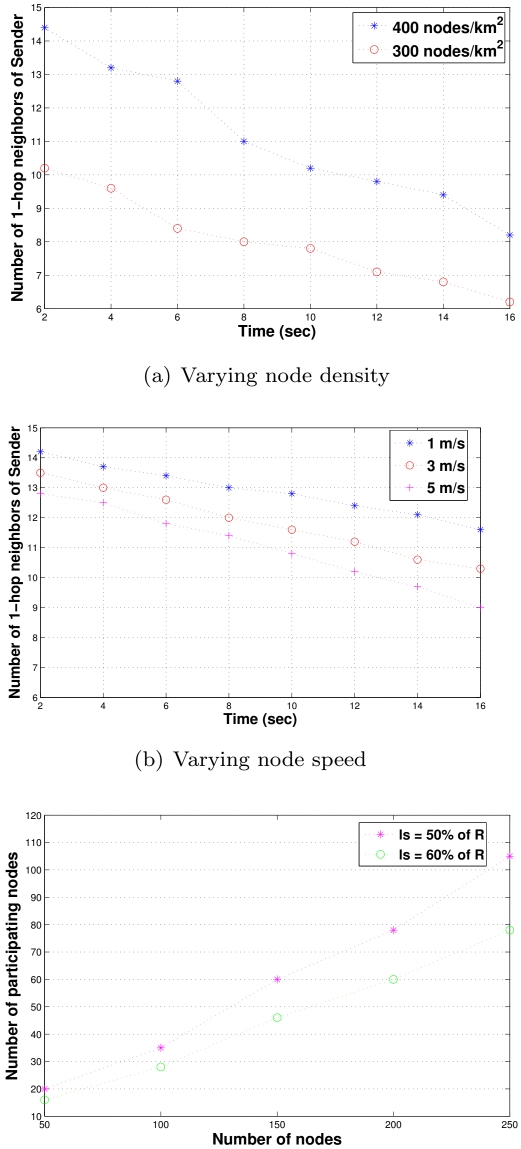
(a) Estimated number of trusted intermediate nodes

(b) Estimated number of participating nodes

Figure 8: Route untraceability

7 Simulation and Results

We provide the performance of proposed scheme using simulations (network simulator NS - 2.34 [14]). We consider bidirectional wireless links with 2Mbps capacity. The number of sender and receiver pairs are kept constant (10 pairs), whereas node mobility, node density and total number of nodes are varied. Each simulation duration was set to be 200s, and the final results were average of 20 simulations. Rough sets are used over the values of trust attributes to maintain NNIT/CNIT. Each node send the parameters values to their neighbor nodes, whenever the parameter values goes below or above the threshold level. Also, each node keeps track of the neighboring node, and whenever the change in received signal strength equals pre-defined value, it updates the NNIT and CNIT. Whenever the change in position is such that the distance between current and previously recorded position is greater than pre-defined value, the node sends the current position to its neighbor nodes. The threshold values of each parameters are varied for each simulation. The following metrics are used to evaluate the performance of proposed scheme in terms of location privacy: (1) *Actual sender location privacy* is the number of neighbor nodes of a sender; and (2) *Actual route untraceability* is the number of participating nodes. Figure 9(a) shows the actual sender location privacy for 300 nodes/km^2 and 400 nodes/km^2 node density. We see that, as the number of neighbors of a sender node move out of its transmission range over time, sender location privacy decreases. Figure 9(b) shows the actual sender location privacy for 1 m/s, 3 m/s and 5m/s node speed. We see that the sender location privacy decreases with increase in node speed over time. In Figure 9(c), average number of participating nodes increases with increasing number of nodes. We compare our proposed scheme with MASK [31] and AODV [16]. The reason behind choosing reactive protocols is that, they are on-demand protocols, so they establish route whenever it is required, and have low processing and computational overhead at node. Reactive routing protocols also provide quick adaptation to dynamic link conditions [16]. For encryption, we use RC6 [18] algorithm. The following metrics are used to evaluate the performance of proposed scheme, in terms of routing efficiency: (1) *Number of hops* is the average number of hop counts; (2) *Delivary rate* is the portion of data packets which are delivered successfully to a receiver; (3) *Latency* is the average time taken by a data packet from a sender to a receiver; and (4) *Normalized control bytes* is the normalized control overhead for sending a single data byte to a receiver. The *ls* is set to be 50% of R (R = 200m) for the proposed scheme, and for others we set *ls* to be equal to R. We see that, LPP has slightly high number of hop counts compared to AODV and MASK (see Figure 10(a)), and the hop count is not much affected when we incorporate DTLPPR scheme. It is expected, as the distance to trusted neighbor selection is dependent on *ls*. We see that, LPP has similar delivery rate as AODV under low mobility (2m/s), but at high mobility the LPP has lower delivery rate compared to AODV (see Figure 10(b)). Also, there is a slight reduction in the delivery rate when DTLPPR scheme is incorporated, however it provides better delivery rates when compared to MASK. The latency in LPP is higher than the AODV, but lower than MASK. This is due to the fact that, in LPP packets are routed through the trusted intermediate nodes only, and also requires time in encryption/decryption. In MASK, node-IDs (pseudonyms) are changed, resulting in high latency and low delivery rates compared to LPP. Figure 10(d) shows that LPP has higher control overhead when compared to AODV, which is expected due to encryption/decryption of data packets and trapdoor; but lower control overhead compared to MASK, because in LPP, control messages are sent only to trusted neighbor node. Also, the control packet sizes are less compared to MASK. However, we see that there is a slight increase in control overhead when DTLPPR is incorporated.



(a) Varying node density

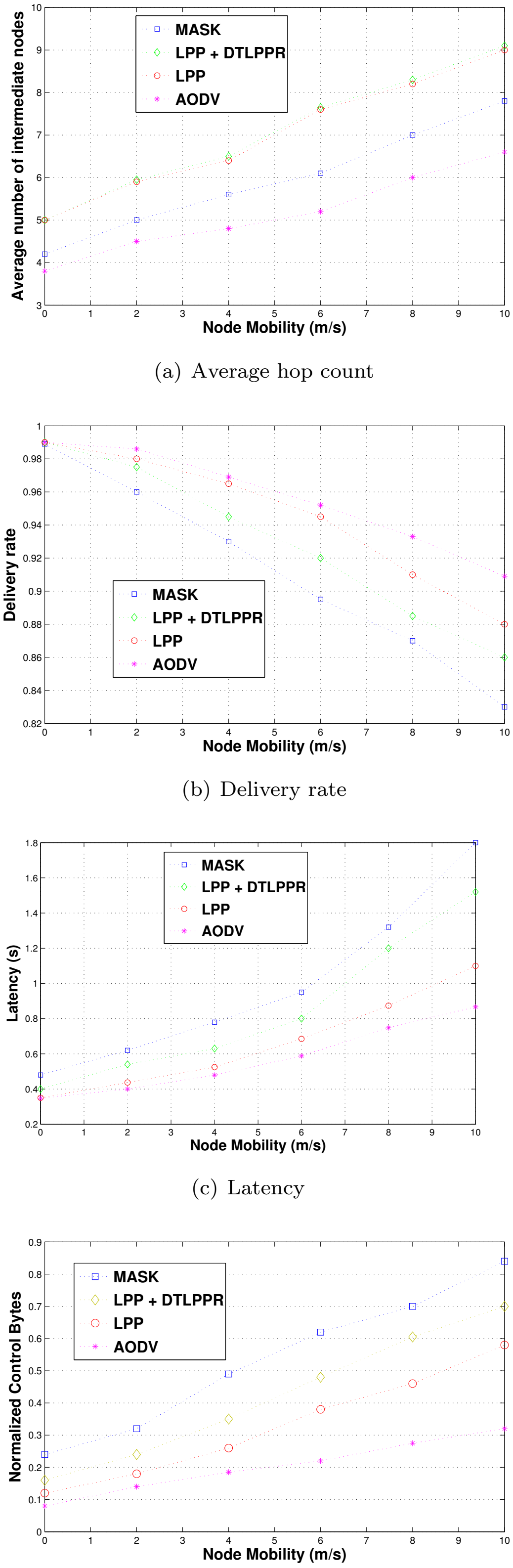
(b) Varying node speed

(c) Average number of participating nodes

Figure 9: Sender location privacy and route untraceability

8 Conclusions

To overcome the drawbacks of the earlier approaches, and to preserve location privacy along with route untraceability, a novel LPP and an efficient DTLPPR schemes are proposed in this paper. The scheme uses trusted nodes for routing, which are determined using rough set theory. The analysis of scheme is discussed in terms of *trustworthiness of neighborhood*, *location privacy* and *route untraceability*. The proposed scheme performs better, and the effectiveness is shown through results. Future work, aims at reinforcing the proposed scheme in an attempt to



(a) Average hop count

(b) Delivery rate

(c) Latency

(d) Normalized Control Bytes

Figure 10: Comparison of proposed scheme with MASK and AODV

withstand stronger active attacks.

References

[1] M. S. Bouassida, "Authentication vs. privacy within vehicular adhoc networks," *International Journal of Network Security*, vol. 13, no. 3, pp. 121–134, 2011.

[2] F. Dotzer, "Privacy issues in vehicular ad hoc networks," in *5th International Workshop on PET*, pp. 197–209, 2005.

[3] T. Hayajneh, R. Doomun, P. Krishnamurthy, and D. Tipper, "Source - destination obfuscation in wireless ad hoc networks," *Security and Communication Networks*, vol. 4, no. 8, pp. 888–901, 2011.

[4] J. Hoebeke, I. Moerman, B. Dhoedt, and P. Demeester, "An overview of mobile ad hoc networks: applications and challenges," *Journal of the Communications Network*, vol. 3, no. 3, pp. 60–66, 2004.

[5] X. Hong, J. Kong, and M. Gerla, "Mobility changes anonymity: new passive threats in mobile ad hoc networks," *Wireless Communication and Mobile Computing*, vol. 6, no. 3, pp. 281–293, 2006.

[6] D. Johnson, Y. Hu, and D. Maltz, *The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4*, RFC 4728, 2007.

[7] B. Karp and H. T. Kung, "GPSR: Greedy perimeter stateless routing for wireless networks," in *International Conference on Mobile Computing and Networking*, pp. 243–254, 2000.

[8] T. D. S. Keerthi and P. Venkataram, "Locating the attacker of wormhole attack by using the honeypot," in *2012 IEEE 11th International Conference on TrustCom*, pp. 1175–1180, 2012.

[9] J. Kong and X. Hong, "Anodr: Anonymous on demand routing with untraceable routes for mobile adhoc networks," in *Mobile Ad Hoc Networking and Computing*, pp. 291–302, 2003.

[10] J. Kong, X. Hong, and M. Gerla, "A new set of passive routing attacks in mobile ad hoc networks," in *IEEE Military Communications Conference (MILCOM'03)*, pp. 796–801, 2003.

[11] M. Po Kwan, I. Casas and B. C. Schmitz, "Protection of geoprivacy and accuracy of spatial information: How effective are geographical masks?," vol. 39, no. 2, pp. 15–28, 2004.

[12] J. Lim, S. Kim and H. Oh, "A secure location service for ad hoc position-based routing using self-signed locations," in *Proceedings of 6th International Conference on CANS*, pp. 121–132, 2007.

[13] R. Matam and S. Tripathy, "Provably secure routing protocol for wireless mesh networks," *International Journal of Network Security*, vol. 16, no. 3, pp. 182–192, 2014.

[14] Network Simulator, *The Network Simulator ns-2.34*, 2015. (`http://www.isi.edu/nsnam/ns/`)

[15] Z. Pawlak, "Rough sets," *International Journal of Computer and Information Sciences*, vol. 11, no. 5, pp. 341–356, 1982.

[16] C. Perkins, E. Belding-Royer, and S. Das, *Ad Hoc on-demand Distance Vector (AODV) Routing*, RFC 3561, 2003.

[17] J. F. Raymond, "Traffic analysis: Protocols, attacks, design issues, and open problems," in *International Workshop on Design Issues in Anonymity and Unobservability*, pp. 10–29, 2000.

[18] R. L. Rivest, M. J. B. Robshaw, R. Sidney, Y. L. Yin, "The RC6 block cipher," in *First Advanced Encryption Standard (AES) Conference*, Aug. 1998.

[19] E. Schoch, F. Kargl, T. Leinmuller, S. Schlott, and P. Papadimitratos, "Impact of pseudonym changes on geographic routing in vanets," in *Proceedings of ESAS*, pp. 43–57, 2006.

[20] J. H. Song, V. W. S. Wong, and V. C. M. Leung, "Wireless location privacy protection in vehicular adhoc networks," *Mobile Networks and Applications*, vol. 15, no. 1, pp. 160–171, 2010.

[21] W. Wang and C. Cui, "Achieving configurable location privacy in location based routing for manet," in *Military Communications Conference*, pp. 1–7, 2008.

[22] W. Wang and T. Stransky, "Stateless key distribution for secure intra and inter-group multicast in mobile wireless network," *Computer Networks*, vol. 51, no. 15, pp. 4303–4321, 2007.

[23] C. Wu, Y. Yue, M. Li, and O. Adjei, "The rough set theory and applications," *Engineering Computations*, vol. 21, no. 5, pp. 488–511, 2004.

[24] W. Hu, K. Xue, P. Hong and C. Wu, "Atcs: A novel anonymous and traceable communication scheme for vehicular adhoc networks," *International Journal of Network Security*, vol. 13, no. 2, pp. 71–78, 2010.

[25] X. Wu, "Disposer: distributed secure position service in mobile ad hoc networks," *Wireless Communications and Mobile Computing*, vol. 6, no. 3, pp. 357–373, 2006.

[26] X. Wu and B. Bhargava, "AO2P: Ad hoc on-demand position-based private routing protocol," *IEEE Transactions on Mobile Computing*, vol. 4, no. 4, pp. 335–348, 2005.

[27] X. Wu, J. Liu, X. Hong, and E. Bertino, "Anonymous geo-forwarding in manets through location cloaking," *IEEE Transactions on Parallel and Distributed Database Systems*, vol. 19, no. 10, pp. 1297–1309, 2008.

[28] T. Xu and Y. Cai, "Location safety protection in ad hoc networks," *Ad Hoc Networks*, vol. 7, no. 8, pp. 1551–1562, 2009.

[29] O. Younes and N. Thomas, "Analysis of the expected number of hops in mobile adhoc network with random waypoint mobility," *Electronic Notes in Theoretical Computer Science (ENTCS)*, vol. 275, pp. 143–158, 2011.

[30] S. Zeng, Y. Huang, and Xingwei Liu, "Privacy-preserving communication for vanets with conditionally anonymous ring signature," *International Journal of Network Security*, vol. 17, no. 2, pp. 135–141, 2015.

[31] Y. Zhang, W. Liu, W. Lou and Y. Fang, "MASK: Anonymous on-demand routing in mobile ad hoc networks," *IEEE Transaction on Wireless Communication*, vol. 5, no. 9, pp. 2376–2385, 2006.

[32] Z. Zhi and Y. K. Choong, "Anonymizing geographic ad hoc routing for preserving location privacy," in *Distributed Computing Systems Workshops*, pp. 646–651, 2005.

Bhawani Shanker Bhati received his B.E. degree from the CMRIT, Bangalore, India in 2009 and M.E. degree from the IISc, Bangalore, India in 2012. He is currently pursuing his Ph.D in the Department of ECE, IISc, Bangalore, India. His research interest are in the areas of Ad hoc Networks, Communication Protocols, Ubiquitous Computing, Security and Privacy in Wireless Networks.

Pallapa Venkataram received his Ph.D. Degree in Information Sciences from the University of Sheffield, England, in 1986. He is currently the chairman for center for continuing education, and also a Professor in the Department of ECE, IISc, Bangalore, India. Dr. Pallapa's research interests are in the areas of Wireless Ubiquitous Networks, Communication Protocols, Computation Intelligence applications in Communication Networks and Multimedia Systems. Dr. Pallapa is the holder of a Distinguished Visitor Diploma from the Orrego University, Trujillo, PERU. He has published over 200 papers in International/national Journals/conferences. He has received best paper awards at GLOBECOM'93 and INM'95 and also CDIL (Communication Devices India Ltd) for a paper published in IETE Journal. He is a Fellow of IEE (England), Fellow of IETE(India) and a Senior member of IEEE Computer Society.