2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies

Privacy-Enhanced Group Communication for Vehicular Delay Tolerant Networks

Chibueze P. Anyigor Ogah, Haitham Cruickshank, Zhili Sun,
Philip M. Asuquo, Ganesh Chandrasekaran, Yue Cao, Masoud Al Tawqi
Institute for Communication Systems (ICS)
University of Surrey
Guildford, United Kingdom, GU2 7XH
email: c.anyigorogah@surrey.ac.uk

***Abstract*—Vehicular Delay Tolerant Networking (VDTN) is a special instance of Vehicular Ad hoc Networking (VANET) and in particular Delay Tolerant Networking (DTN) that utilizes infrastructure to enhance connectivity in challenged environments. While VANETs assume end-to-end connectivity, DTNs and VDTNs do not. Such networks are characterized by dynamic topology, partitioning due to lack of end-to-end connectivity, and opportunistic encounters between nodes. Notably, VDTNs enhances the capabilities DTNs to provide support for delay and intermittent connectivity. Hence, they can easily find applicability in the early stages of the deployment of vehicular networks characterized by low infrastructure deployment as is obtainable in rural areas and in military communications. Privacy implementation and evaluation is a major challenge in VDTNs. Group communication has become one of the well discussed means for achieving effective privacy and packet routing in ad hoc networks including VDTNs. However, most existing privacy schemes lack flexibility in terms of the dynamics of group formation and the level of privacy achievable. Again, it is difficult to evaluate privacy for sparse VDTNs for rural area and early stages of deployment. This paper reports on an improved privacy scheme based on group communication scheme in VDTNs. We analyze the performance of our model in terms of trade-off between privacy and performance based on delivery overhead and message delivery ratio using simulations. While this is a work in progress, we report that our scheme offers considerable improvement against other group communication based schemes described in literature.**

***Keywords*—Anonymity, Privacy, Vehicular Delay Tolerant Networks, VDTN, DTN, VANET.**

I. Introduction

Following the emergence of delay tolerant networks (DTNs) as a solution for connectivity in challenged environments such as deep space communication, Vehicular Ad hoc Networks (VANETs), disaster recovery networks, and underwater networks, a new class of ad hoc networks have emerged aptly regarded as Vehicular Delay Tolerant Networks (VDTNs). While conventional ad hoc networks assume end-to-end connectivity from source to destination nodes, VDTNs do not. Hence, packets(also called bundles) are routed using a store-carry-and-forward mechanism otherwise called opportunistic routing. Therefore, packet forwarding is dependent on the probability that contact is made between source and destination nodes. Most often, the nodes in such networks are memory and battery constrained, a node therefore can only carry a packet for as long as it has enough battery life or memory space to queue up the packet, else it drops the packet. Vehicles in ad hoc networks are often referred to as nodes in various literature, therefore we use nodes and vehicles to refer to the same entity in this paper.

Deployment of DTNs with large vehicle density can suffer from abysmal performance especially if there is no adequate infrastructure support to assist in routing packet especially in the early stages of deployment. To alleviate this and ensure a reasonable trade-off between cost and efficiency, road-side units (RSUs) can be introduced to enable Vehicle to Infrastructure (V2I) communication. However, due to high deployment cost, pervasive deployment of RSUs may not be economically feasible. With the incorporation of RSUs, VDTNs optimize the capabilities of VANETs and adapts it to suit classical DTN environments and ensure support for the partitioning in the network. The RSUs offers two main advantages for VDTNs. First, since RSUs are not memory and battery-constrained, they can temporarily store packets until the next forwarding vehicle is in range to carry-and-forward the packets [1]. Secondly, the RSUs facilitate auxiliary security functions as well improve contact opportunity with vehicle in highly dense locations as described in [2].

Each vehicle driven by a human in a VDTN is an instantiation of a mobile node. Similar to classical VANETs, vehicles exchange safety messages in the form of beacons containing location information used to keep each other informed about events such as accidents and traffic conditions. Unfortunately, the regularly exchanged beacons can be utilized by an adversarial vehicles to infer the source (identity of a vehicle) of a message and track its location with some degree of accuracy. Clearly, the closely coupled relationship between drivers and vehicles leads to two privacy issues. First, without proper access control, it opens up a loophole for easy tracking of vehicles by an adversary - *location privacy*. Secondly, since tracking a vehicle is as good as tracking its driver, it leads to *identity privacy* concerns. Of course, tracking a vehicle is as good as tracking its driver - privacy issues.

Security and privacy remains a key factor that will affect customers perception and acceptance of vehicular communication e.g. vehicular communication for intelligent transport systems(ITS). Since the past few years, security and privacy in vehicular communication has received considerable attention from both industry and academia. Sadly, security and privacy schemes tailored for conventional ad hoc networks do not suit VDTN environments [3]. Hence, most traditional security and privacy techniques that are easily applicable in

978-1-4799-8660-6/15 $31.00 © 2015 IEEE
DOI 10.1109/NGMAST.2015.67

traditional networks cannot be directly applied to VDTNs without modification. In its use case for vehicular communication, privacy provisioning in VDTN is compulsory in order to ensure the protection of the privacy of civilian drivers. The nature of the adversary further complicates the design considerations for privacy-enhancing techniques. Due to the closely knit relationship between vehicles acting as nodes and drivers, VDTNs are prone to both global and local attacks i.e. vehicles are driven by humans who may tamper with on-board electronics. In this paper, we propose a novel privacy-aware group communication scheme for sparse VDTNs. While different from other approaches, our scheme makes provision for vehicles to easily swap groups for improved individual privacy. Specifically, our contribution is as follows:

- we identified the requirements for group communication in a disconnected environment. Our RSU-aided packet forwarding scheme ensures a higher delivery rate for a rural deployment of VDTN.
- our group communication ensures redundancy while achieving higher delivery ratio in comparison with our base line scheme.

The rest of this paper is organised as follows. We discuss some related literature in the(SectionII), and describe our scheme and attacker models in Section III. Our enhanced privacy scheme is discussed in Section IV. In Section V, we evaluate the schemes using simulation studies, and finally conclude and present our future work in Section VI.

II. Related Work

The major highlight of this paper, namely privacy by group communication has been proposed in different literature [4]. There is a consensus in literature on privacy protection using frequently changing pseudonyms in VANETs [5]. In pseudonym communication, vehicles are pre-loaded with a set of pseudonyms, *P* by a certificate authority (CA). To send a message *m*, a vehicle chooses a pseudonym p_i from *P* set of pseudonyms to sign *m*. Pseudonymous communication prevents the adversary from linking a vehicle to the messages they exchange to its real identity. The vehicles are equipped with a pool of multiple pseudonyms from which the vehicles can select what pseudonym to use at regular intervals (e.g. every 5 minutes) such that a pseudonym used at time t_n is not the same as that at t_{n+1}. To further ensure a higher level of privacy protection, vehicles can synchronize their pseudonym change with other vehicles willing to change pseudonyms at coordinated positions and time. Several works in literature propose that pseudonym change be done at locations where they are enough vehicles willing to agree to change pseudonyms e.g road intersections and car parks.

The author in [6] describe the concept of mix zones and its variants such as Density Zones and Social spots for effectively changing pseudonyms. An ideal mixed zone can be crowded locations such as social spots [2] and road intersections where vehicles can distract attackers by changing their pseudonyms securely. Sugou et al proposed a specific use of mix zones for location privacy in DTNs [7]. Usually, this requires a group of vehicles that can change pseudonyms at the mix zone - the more the number of vehicles, the higher the anonymity enjoyed by individual vehicles. However, the scheme does suit VDTNs due to their disconnected nature. Again, in resource constrained networks such as VDTNs, some selfish vehicles may not be willing to change pseudonyms [8]. For instance, vehicles with diminishing battery power may decide to sleep and save energy instead of engaging in exchange of signal messages needed to find suitable vehicles willing to change pseudonyms.

Similar to mix zones, techniques based on radio silence include *Silent Periods* and *Silent Cascades* where vehicles can cease beacon transmission by temporarily switching off their radios [9]. Such radio-silence based methods have been criticised to undermine the critical safety objectives of vehicular networks for use in ITS. Tor [10] has been the most popularly implemented anonymity network based on the concept of mixing [5]. Mixed networks send packets along a cascade of proxy nodes otherwise called mixes. Mixes store and forward batches of layer-encrypted packets, both batching and encryption ensures that mix inputs and outputs cannot be correlated. Mixed networks in all its variations are based on source routing, are highly inefficient and cannot be applied in VDTNs since a definite end-to-end path does not exist. Identity Based Encryption (IBE) using a Private Key Generator (PKG) to dynamically generate pseudonyms is used in [11]. Unfortunately, their approach relies on trusted gateways to operate and requires periodic updates from the PKG which are single points of failure. One of the schemes for anonymous communication in DTNs uses Identity-Based Cryptography (IBC). The scheme proposes combining users' identities with location identifiers. To achieve scalability, it recommends the use of a hierarchical identity-based cryptography (HIBC). However, the proposal assumes the presence of trusted gateways with full knowledge of user identities. Similar to the IBE scheme, it is not suitable for a partitioned VDTN as the gateways can easily become single points of failure.

In summary, a variety of anonymity schemes proposed for VDTNs are often borrowed from techniques in traditional VANETs and is not suitable for VDTNs. It is therefore hard to export privacy schemes tailored for DTNs and expect them to work for VDTNs without modification. In particular, most routing protocols tailored for DTNs rely on shared node information to forward bundles and hence identity information is revealed. Although, we have used in built routing protocols, we justify our decision later on.

Our privacy scheme is closely related to the schemes in [12] and [13]. These methods are based on the concept of group communication where a source (.i.e group) chooses the path to the destination prior to sending a packet. Group communication techniques are more suitable for dense networks since redundancy is ensured through multiple communication paths contributed by the numerous number of vehicles in the network. It also ensures eventual packet delivery in case of node failure due to attack. However, it does not suit the sparsely populated VDTN since they may not be enough vehicles to form groups. We describe how we overcome this challenge in our scheme later.

III. Preliminaries

In this section, we present a detailed description of our system, assumptions and the attributes of the adversary against whom we defend the network.

A. Network Model

We consider VDTN deployment in a rural area as described in [14]. Our network can be modelled as a directed multi-graph as follows: $\mathbb{G} = (\mathcal{V},\mathcal{E})$ where $\mathcal{V}$ and $\mathcal{E}$ denote some set of vehicles and contact edges respectively. Our scenario

makes use of road-side units (RSUs) as stationary relay nodes to facilitate efficient packet routing. As described in [15], the authors show that the performance of DTNs can be greatly enhanced by effectively deploying RSUs in vehicular networks. We only deploy RSUs at strategic locations as in [16]. During each contact duration *D*, we assume that the source and destination vehicle can exchange a message *m* characterized by the following set of attributes: (ID_i, *l*, v, t), where ID_i is a pseudonym identity of a vehicle, *l* is the location of the vehicles (a Global Positioning System (GPS) could be used to manage location services), *v* is its speed, while *t* is the time-stamp information.

B. Adversary Model

We consider a global passive adversary in our model. The adversary can monitor all forms of communication and signalling messages traversing the entire network, and is able to partially control a subset(e.g. 10 - 20%) of vehicles in the network. However, the adversary does not possess cryptographic details of the vehicles and so cannot decrypt sensitive messages. We assume that the RSUs are trustworthy and tamper-proof.

Our analysis considers privacy attacks in the form of packet analysis and tracking attacks for location and identity privacy violation. To be able to execute packet analysis attacks, the adversary can delay the message delivery for a considerable amount of time while analysing it to divulge information regarding source and destination vehicles.

IV. System Description

Our scheme addresses cooperative privacy utilizing a group communication framework similar to the schemes in [12] and [13]. Different from the above schemes, we introduce the following improvements to our scheme:

- our scheme leverage RSUs for a more efficient bundle forwarding
- by intelligently assigning nodes to groups, our scheme maximizes privacy by ensuring that group membership is restricted to a threshold for improved privacy.

Our protocol aim to achieve both location and identity privacy. In this regard, anonymity is achieved if an identifiable information such as identity and location of a vehicle cannot be known with certainty by the adversary (i.e. a vehicle is indistinguishable from other in the network). Therefore, vehicle anonymity depends on the number of other indistinguishable vehicles - otherwise called the anonymity set size (ASS) in the network. Mathematically, the privacy enjoyed by a node can be expressed in terms of entropy and degree of anonymity (DoA) using Shanon's equation [17] based on information theory as follows. If *X* is discrete random variable with a probability mass function *P(X=i)* where *i* = 1 to *n* for the different values of *X*, then the entropy *H(X)* can be expressed as in (1).

$$H(X) = -\sum_{i=1}^{N} p_i \log_2 p_i, \tag{1}$$

The DoA [18] assumes that the AS has a number of suspect indistinguishable vehicles with possible link to an action (e.g. sending a message). Assuming the adversary has no priori information about the system, we express the maximum entropy as (H_{max}) in 2

$$H_{max} = log(n) \tag{2}$$

Hence, the adversary can gain H_{max} – H(X) after an attack on the system. The DoA is assessed on a scale of 0 to 1, hence the maximum entropy of a subject is expressed as in 3 below.

$$d = 1 - \frac{H_{max} - H(X)}{H_{max}} = \frac{H(X)}{H_{max}} \tag{3}$$

The privacy as expressed above depends on the number of participants in the network and the level of correctness by the adversary in associating an action to a vehicle. For example, in a network of two vehicles exchanging messages or changing pseudonyms, the probability of the adversary guessing a subject is ($P(1/2)$ = 0.5). The probability is expressed as the ability of the adversary to link a vehicle to the action of say sending a message or changing its pseudonym at a point in time. However, in our scheme, we also measure the performance based on two utility factors, privacy as expressed above in addition to time delay incurred in forwarding a bundle to its destination through rings of groups as expressed in 4. While vehicles are privacy protected through group communication, it takes some time for vehicles to form or join groups to be able to forward messages. Note that we set a threshold for the number of vehicles that can form a group, if the threshold is met, a group is formed to forward packet. Our scheme accounts for this time delay. For each simulation run, we measure the performance utility, $\mathcal{U}_T$ as expressed in 4 and 5 where $\mathcal{U}^{Privacy}$ and $\mathcal{U}^{Delay}$ are privacy and delay functions respectively. We average our values over 30 simulation runs.

$$\mathcal{U}_T = \mathcal{U}^{Privacy} + \mathcal{U}^{Delay} \tag{4}$$

(4) can further be expressed in terms of the normalization co-efficients α and β associated with the network as shown in 5, where α = 1 - β.

$$\mathcal{U}_T = \alpha(\mathcal{U}^{Privacy}) + \beta(\mathcal{U}^{Delay}) \tag{5}$$

The values taken by α and β depends on the level of privacy a user intends to achieve. We assume the default minimum values of of 0.5 (i.e. α = 0.5, β = 0.5). However, the user can adjust the privacy settings to suit need even on initiation. In our evaluation, we vary these values for different simulation runs to arrive at our results.

For simplicity, if we take the privacy to be entropy as expressed in (1) and substitute in (4) thus:

$$\mathcal{U}_T = \alpha(H(X)) + \beta(\mathcal{U}^{Delay}) \tag{6}$$

The anonymity depends on the anonymity set size as well as on the amount of traffic generated by the nodes participating in the network. The amount of traffic generated at any point in time is directly proportional to the number of active vehicles exchanging messages. Hence, traffic analysis attack becomes more challenging for the attacker.

Group Formation: Our network comprises vehicles and RSUs as described in Section III. The RSUs form stationary relay nodes to assist in forwarding packets. Our model assumes the presence of an off-line Trusted Key Manager (TKM) that assigns keys and certificates to network entities. We assume the network has *V* vehicles $V = \{v_0, v_1, v_2, ..., v_L\}$ and predefined groups on initiation $G = \{g_0, g_1, g_2, ..., g_L\}$. Each vehicle

$v_i \in V$ belongs to at least one $g_i \in G$. However, there is a minimum T_{min} and maximum threshold T_{max} for the number of vehicles, n that belongs to a group at a time, $\{T_{min} \leq n \leq T_{max}\}$. Our system assumes that each vehicle v_i possesses a pair of public and private keys $\{P_b^i, P_r^i\}$, a pair of group public and private keys for the group to which they belong, $\{G_b^i, G_r^i\}$ as well as individual and group digital certificates V_c and G_c assigned by an off-line trusted key manager (TKM). Since the number of active nodes in a group or network is proportional to the traffic generated per time, we utilized the threshold as a means of further ensuring privacy since it is difficult for an adversary to correlate multiple simultaneous traffic from multiple sources [13] as efficiently as it can from a single source. Hence, our group communication scheme achieves redundancy and privacy depends on the number of nodes within each group. We summarize the group formation process in Algorithm 1 below.

Algorithm 1 Group Formation

1: **procedure** INPUT(G, V) $\rightarrow G$ is the number of groups, V is the set of vehicles
2: set thresholds (t_{max}, t_{min})
3: *random factor* $r \leftarrow Random()$
4: $GetNodes(v_i) \leftarrow V$
5: *group change formation and change request*:
6: **for** each vehicle $v_i \in V$ **do**
7: add v_i to a random group r($g_i \in G$)
8: **end for**
9: **if** $g_i < T_{min}$ **then** send group and pseudonym change request $m = \{ID_i, l, v, t\}$ (vehicle joins a new group of request is granted)
10: **end if**
11: **end procedure**

Performance Considerations: The discontinuity of connections in VDTNs already impacts performance attributes such as end-to-end delay, latency, and average hop count. With the implementation of security and privacy-enhancing techniques, further performance degradation will be most likely. We analyse the usual metrics for performance evaluation namely delay, latency and hop count as well as the impact of privacy settings on the system.

V. Simulation and Evaluation

In this section, we describe our experiments and conduct performance evaluation of our scheme.

A. Simulation Setup

We implement our scheme using a popular and widely used simulator for delay tolerant networks namely the Opportunistic Networking Environment (ONE) simulator [19]. The ONE simulator has been used to investigate application scenarios for VDTNs as promoted in [3] and used in [1]. Unless otherwise stated, our simulation runs involves 50 – 300 vehicles and 5 stationary relay nodes as RSUs. Table I presents a detailed summary of our simulation parameters. The vehicles are distributed on the map of the City of Helsinki (measuring 5000 x 5000m) extracted in the ONE Simulator while the RSUs are placed at carefully chosen intersections. We partition the entire map into multiple regions, each region represents a starting point for each group as described earlier. In accordance with Finnish traffic regulations, we set an average lower and upper speed bounds for each vehicle as 30 – 60kmh^{-1} (i.e. from 8.30ms^{-1} to 16.70ms^{-1}). The relay nodes plays the dual role of facilitating packet forwarding as well as acting as Roadside Units (RSUs) in a resource-constrained rural or military deployment. Since vehicles usually follow defined routes in the form of roads, our model assumes each vehicle follows a *shortest path map-based movement* mobility model where vehicles are first situated randomly on different spots on road and then allowed to travel along predefined routes to their destination.

Most routing protocols for delay tolerant networks depends on contact information to route packets, we assume that the vehicles exchange using pseudonyms issued by the TKM as described in Section III. We conduct our experiment only on top of First Contact and Direct Delivery routing protocol as they only maintain limited copies of packets in the network [20]. In the former, only a single copy of the message is generated by source node and forwarded to the next available contact until the message reaches its destination, while the later routes packets based on transfer probability. Transfer probability implies that a sender chooses to send a packet or retain a copy based on some probability. In our experiment we refer to a single node and the group to which it belongs as source and destinations. However, other routing protocols can be considered for evaluating our scheme but we leave that to our future work.

TABLE I. Simulation Parameters

Parameter	Description
Duration	12 hrs
Number of vehicles; RSUs	50, 100, 150, 200, 250, 300 vehicle; 5 RSUs
Speed limit	30 kmh^{-1} – 60 kmh^{-1}
Transmission coverage	100 m
Mobility model	Shortest path map based movement
Packet size	500k – 1M
Message generation interval	25 s – 35s

B. Performance Evaluation

In this section, we analyse the performance of our model based on three metrics popularly used for evaluating the performance of delay tolerant networks: the utility ratio (U_T) as described in Section IV, *delivery ratio*, *average delay* and *time to live(TTL)* and in addition to *group hop count* as our performance metrics. The delivery ratio accounts for the fraction of total total generated messages that are successfully delivered to their final destination within a specified time; the average delay reflects time measured between message generation from source to its successful delivery at the destination nodes; the TTL is the time limit within which a message should be delivered to its destination successfully. Our choice of the TTL is particularly crucial as it represents the ability of the group protocol to deliver messages on schedule. The group hop count gives an indication of how many paths a packet is routed through to its destination. The group hop count therefore records each group traversed by a packet carried by a vehicle as it journeys from one path of the map to the other.

1) Utility Ratio: Different from other conventional performance metrics, we utilised the utility ratio as one of our

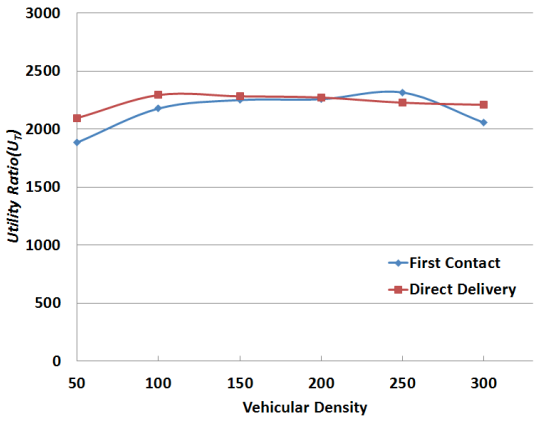

Fig. 1. Variation of utility ratio with vehicle density

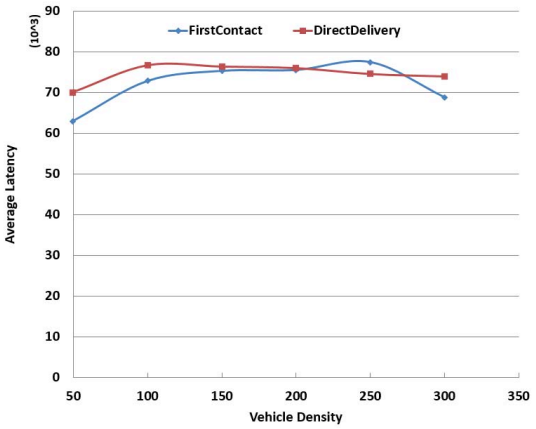

Fig. 3. Average latency variation with vehicle density

performance metrics. We observe that the utility ratio in Figure 1 for both First Contact and Direct Delivery protocols does not show a major difference. As this is only a preliminary work, this behaviour is subject to further experimentation in the future to establish this behaviour even with other routing protocols.

2) Delivery Ratio: Figure 2 shows the variation in delivery ratio with different vehicle densities. As a baseline for comparison, from the figure, we show that our scheme achieved a higher delivery ratio for First Contact and Direct Delivery routing protocols compared to the results in the scheme presented in [12]. As stated earlier, our group communication scheme ensures redundancy, hence eventual packet delivery to its destination. The higher delivery ratio validates the notion of RSU-assisted packet forwarding in our scheme.

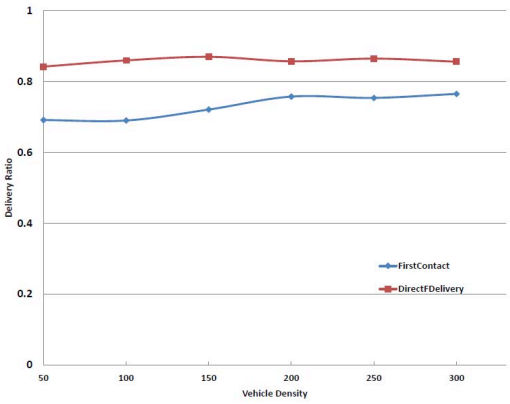

Fig. 2. Variation of overhead ratio with vehicle density

3) Average Latency: In Figure 3, we show the variation in latency for different vehicle densities. We observe that vehicular density or our choice of routing protocol has no significant impact on the latency. However, this scenario could be repeated for other routing protocols such as Epidemic and Spray & Wait routing protocols as part of our future studies.

4) Time to Live(TTL): The delivery ratio for various TTL is as shown in Figures 4 and 5. For this scenario, we varied the TTL from 5 to 30 minutes for vehicles densities ranging from 150 to 250. We compare our results to that scheme in [7]. However, our scheme considers only First Contact and Direct Delivery routing protocols. Similar to [7], there is a gradual increase in delivery ratio as the vehicle density increases from 150 to 250. The lower values achieved in our scheme is due to the routing protocols used. While our baseline scheme assumed multi-copy routing protocols, we used single copy routing protocols.

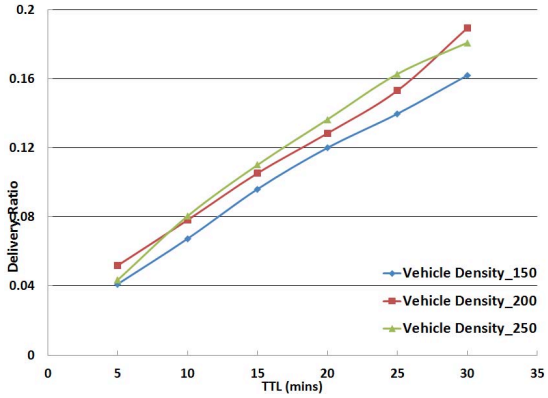

Fig. 4. Delivery ratio for different TTL for first contact routing protocol

5) Group Hop Count: The group hop count is an indication of how many hops a message is routed through from source to destination. We observe that First Contact performs about 45% less that direct contact in routing a single message. This means that for the same vehicle density, first contact will take about 45% increase in the number of hops a packet would go through to reach its destination.

VI. Conclusion and Future Work

In this paper, we have developed a group communication scheme for privacy enhancement in vehicular delay tolerant networks. By adopting different groups, our scheme ensures redundancy and a more efficient packet delivery from source to destination. We introduced RSU-assisted forwarding where each RSU acts as a coordinator for the vehicles within its

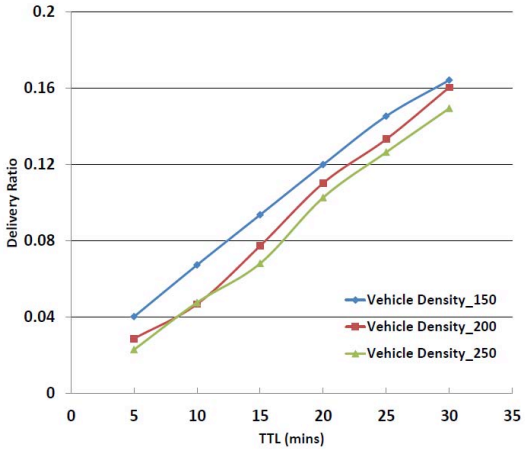

Fig. 5. Delivery ratio for different TTL for direct delivery routing protocol

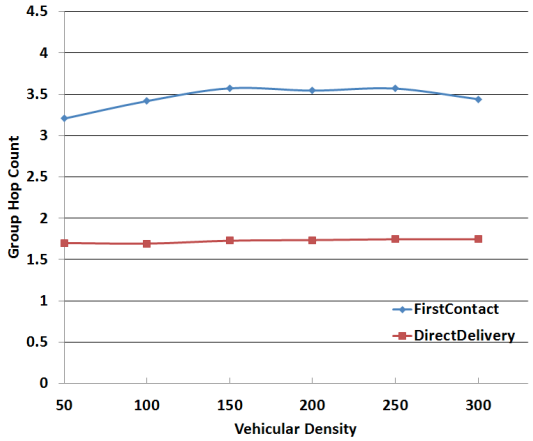

Fig. 6. Group hop count for varying vehicle density

transmission range. Our ongoing future work involves novel group swapping and RSU-assisted pseudonym changing algorithm through the use of mix-zones. We shall investigate the authentication and re-keying mechanisms against malicious nodes and evaluate our scheme against more advanced privacy attacks such timing attacks.

ACKNOWLEDGEMENT

The funding for this work is from the Overseas Scholarship Scheme (OSS) of the Petroleum Technology Development Fund (PTDF) of the Federal of Nigeria Government with support from the Institute of Communication Studies, University of Surrey, United Kingdom.

REFERENCES

[1] R. Lu, X. Lin, and X. Shen, "Spring: A social-based privacy-preserving packet forwarding protocol for vehicular delay tolerant networks," in *INFOCOM, 2010 Proceedings IEEE*, March 2010, pp. 1–9.

[2] R. Lu, X. Li, T. Luan, X. Liang, and X. Shen, "Pseudonym changing at social spots: An effective strategy for location privacy in vanets," *Vehicular Technology, IEEE Transactions on*, vol. 61, no. 1, pp. 86–96, Jan 2012.

[3] P. R. Pereira, A. Casaca, J. J. P. C. Rodrigues, V. N. G. J. Soares, J. Triay, and C. Cervello-Pastor, "From Delay-Tolerant Networks to Vehicular Delay-Tolerant Networks," *Communications Surveys Tutorials, IEEE*, vol. 14, no. 4, pp. 1166–1182, Fourth 2012.

[4] A. Wasef and X. Shen, "Ppgcv: Privacy preserving group communications protocol for vehicular ad hoc networks," in *Communications, 2008. ICC '08. IEEE International Conference on*, May 2008, pp. 1458–1463.

[5] D. Chaum, "Security without identification: Transaction systems to make big brother obsolete," *Commun. ACM*, vol. 28, no. 10, pp. 1030–1044, Oct. 1985. [Online]. Available: http://doi.acm.org/10.1145/4372.4373

[6] A. R. Beresford and F. Stajano, "Mix Zones: User Privacy in Location-aware Services," 2004.

[7] S. Du, H. Zhu, X. Li, K. Ota, and M. Dong, "Mixzone in motion: Achieving dynamically cooperative location privacy protection in delay-tolerant networks," *Vehicular Technology, IEEE Transactions on*, vol. 62, no. 9, pp. 4565–4575, Nov 2013.

[8] R. Lu, X. Lin, H. Zhu, X. Shen, and B. Preiss, "Pi: A practical incentive protocol for delay tolerant networks," *Wireless Communications, IEEE Transactions on*, vol. 9, no. 4, pp. 1483–1493, April 2010.

[9] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, "Enhancing Wireless Location Privacy Using Silent Period," in *Wireless Communications and Networking Conference, 2005 IEEE*, vol. 2, March 2005, pp. 1187–1192 Vol. 2.

[10] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The second-generation onion router," in *Proceedings of the 13th Conference on USENIX Security Symposium - Volume 13*, ser. SSYM'04. Berkeley, CA, USA: USENIX Association, 2004, pp. 21–21. [Online]. Available: http://dl.acm.org/citation.cfm?id=1251375.1251396

[11] L. Huang, H. Yamane, K. Matsuura, and K. Sezaki, "Silent Cascade: Enhancing Location Privacy Without Communication QoS Degradation," in *Proceedings of the Third International Conference on Security in Pervasive Computing*, ser. SPC'06. Berlin, Heidelberg: Springer-Verlag, 2006, pp. 165–180.

[12] R. Jansen and R. Beverly, "Toward Anonymity in Delay Tolerant Networks: Threshold Pivot Scheme," in *MILITARY COMMUNICATIONS CONFERENCE, 2010 - MILCOM 2010*, Oct 2010, pp. 587–592.

[13] C. Shi, X. Luo, P. Traynor, M. H. Ammar, and E. W. Zegura, "ARDEN: Anonymous Networking in Delay Tolerant Networks," *Ad Hoc Networks*, vol. 10, no. 6, pp. 918 – 930, 2012. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1570870511002150

[14] V. Soares, F. Farahmand, and J. Rodrigues, "A Layered Architecture for Vehicular Delay-Tolerant Networks," in *Computers and Communications, 2009. ISCC 2009. IEEE Symposium on*, July 2009, pp. 122–127.

[15] N. Banerjee, M. D. Corner, D. Towsley, and B. N. Levine, "Relays, Base Stations, and Meshes: Enhancing Mobile Networks with Infrastructure," in *Proceedings of the 14th ACM International Conference on Mobile Computing and Networking*, ser. MobiCom '08. New York, NY, USA: ACM, 2008, pp. 81–91. [Online]. Available: http://doi.acm.org/10.1145/1409944.1409955

[16] R. Lu, X. Lin, T. Luan, X. Liang, and X. Shen, "Anonymity analysis on social spot based pseudonym changing for location privacy in vanets," in *Communications (ICC), 2011 IEEE International Conference on*, June 2011, pp. 1–5.

[17] C. E. Shannon, "Communication Theory of Secrecy Systems," *Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.

[18] C. Díaz, S. Seys, J. Claessens, and B. Preneel, "Towards measuring anonymity," in *Proceedings of the 2Nd International Conference on Privacy Enhancing Technologies*, ser. PET'02. Berlin, Heidelberg: Springer-Verlag, 2003, pp. 54–68. [Online]. Available: http://dl.acm.org/citation.cfm?id=1765299.1765304

[19] A. Keränen, J. Ott, and T. Kärkkäinen, "The ONE Simulator for DTN Protocol Evaluation," in *SIMUTools '09: Proceedings of the 2nd International Conference on Simulation Tools and Techniques*. New York, NY, USA: ICST, 2009.

[20] Y. Cao and Z. Sun, "Routing in delay/disruption tolerant networks: A taxonomy, survey and challenges," *Communications Surveys Tutorials, IEEE*, vol. 15, no. 2, pp. 654–677, Second 2013.