IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 8, Aug 2015.
www.ijiset.com
ISSN 2348 – 7968

Efficient Data Dissemination and Privacy Preservation using Trajectory Prediction in VANETs

Suneetha Eluri[1] and N.Dipti[2]

[1] – Assistant Professor, Department of Computer Science & Engineering,
University College of Engineering, JNTU-K,
Kakinada, Andhra Pradesh, India.

[2] – M.Tech, Department of Computer Science & Engineering,
University College of Engineering, JNTU-K,
Kakinada, Andhra Pradesh, India.

Abstract

A Vehicular Ad-Hoc Network or VANET is an emerging and significant class of Mobile Ad-Hoc Network or MANET which make available contact connecting vehicles and connecting vehicles and road-side base stations. But efficient data dissemination and vehicle user privacy are challenging due to network disruption, topological change and regular changes of mobility patterns. Also the vehicle user's secrecy and validation must be taken in account in creation of secure Vehicular Network. To address these difficulties, numerous routing approaches have been proposed in past, that does not formulate any judgment or prediction on vehicular traces. They acquire benefit of navigation systems in which vehicular trajectory is priori known. To conquer the restraints of existing algorithms, an incorporated approach is proposed in this paper, to achieve efficient data dissemination through location trajectory prediction & distributed routing, as well as authentication and privacy in Vehicular ad-hoc networks.

Keywords- *Vehicular Ad-hoc Network (VANET), Vehicle Trajectory, Routing, Prediction, Privacy, Authentication*

1. Introduction

With the rapid advance in wireless technologies, Cars that are equipped with wireless communication equipments and wayside base stations can constitutes a huge self-organised communication network recognized as vehicular ad-hoc network (VANET). A Vehicular Ad-Hoc Network (VANET) is a subset of Mobile Ad-Hoc Network or MANET which provides communication between motor vehicles by means of small wireless communications. However, VANET is different from other kind of Ad-Hoc networks by means of their cross network architectures, high pace vehicular movement characteristics and wide range of new possible applications. In Vehicular networks, each and every contributing vehicle is converted into a wireless router or node, allow vehicles about 100 to 300 meters far from each other join and form a network. Vehicles can therefore, communicate with each other either directly when they encounter each other or through multi hop transmissions. Every vehicle in network is considered to be an intellectual mobile node competent of commune with its neighbours and other cars in network. In VANET, vehicular nodes are endowed with communication devices known as on-board units (OBUs), which are used to set up communications with other cars or roadside units (RSUs) for example traffic lights or traffic signs; based on the purpose.

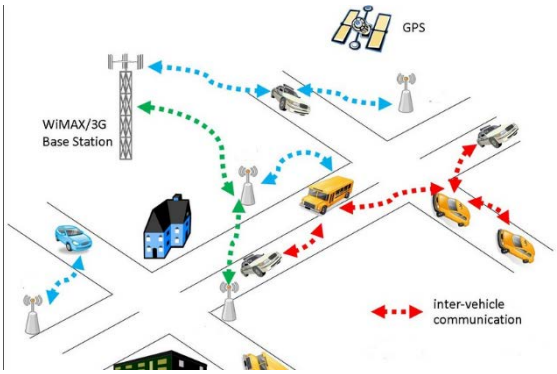


Fig 1: Communication in Vehicular Ad-Hoc Network

Vehicular networks have many appealing applications, such as driving precautions; lessen traffic congestion, infrastructure monitoring and urban supervision, calamity rescue preparation [3], and traffic management. It is a significant facet of safety applications for example Intelligent Transportation Systems (ITSs) and advanced cooperative collision

ISSN 2348 – 7968

warning system. Interactive steering can thwart vital accidents from happening, thus ensuring traffic safety and efficiency. On the other side, convenience application contains applications like driver aid, supportive driving, involuntary parking, driverless vehicle, Map position, etc. Vehicular network also offers location based services (LBS) to its user [2]. For instance, via the location based services a user can access information like weather conditions predict, news broadcast next-door restaurants, etc throughout entire journey. GPS and other navigation systems might integrate with traffic reports to providing the best route to vocation. A vehicular network also offers infotainment services such as in-car activity make cellular phone calls and use Internet-enable information such as traffic environment, games and climate forecasts.

Compared with traditional wired or other wireless or mobile ad-hoc networks, VANETs are extremely dynamic, and their communications are unstable. Hence, data delivery in vehicular networks faces a set of new dreadful challenges [1]. First, vehicular networks are subjected to frequent disruptions. It is difficult to find a connected path between a pair of source and destination in vehicular networks. This is due to high mobility and rough distribution of vehicles over the network. Second, vehicles habitually travel at an elevated speed. Two vehicles can communicate once they are inside the contact range. Recent works have revealed that the contact duration in case of a vehicle and a static access point is as short as 10 seconds on average.

More importantly, there is a great deal of uncertainty associated with vehicle mobility. Vehicles travel at their individual wills. It is hard, if not unfeasible, to get the complete knowledge about the vehicle outline of future movement. For routing in a vehicular network, a transmit node must choose how long a packet should be held in reserve and which node a given packet should be forward to. Thus, the information of future vehicle movement plays a key role for optimal data dissemination. Existing study shows that it is likely to determine an optimal routing path when the data of future node traces is on hand; this is NP-hard though. However, it is not viable to have prior knowledge about future traces of nodes. Hence, a number of algorithms have been designed for data delivery in vehicular networks. Existing routing algorithms heavily rely on predictions of vehicle mobility. However, they have adopted only easy mobile patterns such as the spatial distribution and inter-meeting time distribution, which support coarse-grained calculations of vehicle movements.

Furthermore, without security, a Vehicular Ad Hoc Network (VANET) system is susceptible to a number of attacks such as propagation of false warning messages as well as suppression of authentic warning messages, thereby rooting accidents. In VANET, it is constantly assume that the malicious attacker can collect messages sent by other vehicles and observe the vehicle's movement as well. It also enables to speculate the data and devise the vehicle's real identity, journey routes and position. This makes security assurance and privacy preservation primary concern in building such networks. Therefore, VANET protocols should protect the privacy of the vehicles as far as possible and messages from being tampered with by attackers [9]. However, anonymous authentication is facing a problem in VANETs.

2. Related Work

Ever since the advance of vehicular networks, data deliverance in vehicular networks has been premeditated and a number of algorithms have been proposed which can be loosely divided into two categories. The first group of routing algorithms simply assumes the availability of future movement, that is, the traces of nodes are fixed and can be known beforehand. This illustration works fine in traditional Delay Tolerant Networks, such as satellite networks, whose nodes have simple and stable mobility traces. They take help of navigation systems, in which drivers must let, know the navigation system the destinations prior to journey and vehicular traces are priori known.

The second group of routing algorithms makes evaluations about routing metrics, since there is no assisting information about node potential traces. It has been revealed that the inter-meeting time is exponentially distributed based only on the historical meetings but doesn't use current position information.

In short, present algorithms either suppose the availability of future traces of nodes or make coarse-grained prediction based on simple mobile patterns. Also these algorithms don't take into account sparse features and security prerequisites of VANETs.

3. Literature Review

This section addresses the different techniques those are presented to solve the data delivery and security problems of VANET.

ISSN 2348 – 7968

An algorithm, Flooding [4], well-known as epidemic routing, is a simple one in which each node forwards all the packets it carries to any node it meets. It introduces very high cost, which is the major drawback. In Delegate Forwarding [5], Erramilli expresses that forwarding with a metric of good quality can reduce network cost. This is done by the strategy of only forwarding packets to those nodes which lead the packet to the highest quality.

In GeOpps [7], Leontiadis et.al. assumes that the trace of a node can be obtained through the navigation system equipped onboard in the car. Such algorithms are restricted by the presence of navigation systems and the tendency of drivers. In TDB [6], Jaehoon Jeong et al. put forward a data forwarding scheme utilizing the vehicles' trajectory information for light- traffic highway networks where the carry delay is the leading factor for the end-to-end delivery delay. However, TBD tends to perform poor under high vehicular traffic density.

In [8], Hubaux et al. identify the specific issues of security and privacy confronts in Vehicular networks, and indicates that a Public Key Infrastructure-PKI should be well deployed to protect transited messages and to mutually authenticate entities of network. In [10], Raya et al. use a classical PKI to provide secure and privacy preserving interactions to Vehicular networks. In this, each vehicle requires to pre-load an enormous group of secret certificates. The amount of the laden certificate in each car must be large enough to offer security and privacy preservation for a extensive period. Each car can revise its certificate from the central authority during the annual examination of the car. In this advance, revoking one vehicle implies for revoking the huge number of certificates loaded in it. This implies the vehicle is not able to send messages to neighbouring vehicles.

4. Proposed System

4.1 Problem Definition

The main job of data deliverance is to move the packets from their sources to respective targets.

Well-managed inter-vehicle data dissemination is of innermost significance to vehicular networks and consequences of such has been acknowledged by many existing studies. Inter-vehicle data delivery may bring in delivery latency due to recurrent topology disruption of a vehicular network. Thus, we have to consider inter-vehicular communications only for that application which can endure certain delivery latency. For instance, in the situation of urban sensing, cars continuously assemble data of use, for instance road traffic conditions and road closures. A vehicle may send a message request for a particular sort of data and the individual that has the information should act in answer to the indecision node with the data. Such interaction has necessitated multi-hop data delivery in vehicular networks. Only some illustration, like the spatial distribution and inter- meeting time distribution, support coarse predictions of vehicle trace. But none of these algorithms pays no attention to the fact that links in a vehicular network is unstable and venerable to various attacks.

4.2 System Architecture

To prevail over the limitations of existing algorithms, this paper suggests an approach to develop the hidden mobility steadiness of vehicles to foresee future trajectories. Moreover, the results based on entropy analysis demonstrate that the future trajectory of a vehicle is closely related to its preceding trajectory. Thus, we incorporate multiple order Markov chains for calculate future trajectories of vehicles. With the accessible future trajectories of vehicles, we recommend an analytic model and tentatively obtain the delivery probability of a packet. It develops a global algorithm for work out routing paths when predicted possible trajectories are on hand. This paper proposes a distributed algorithm with which knowledge of vehicles' position and its mobility pattern made available in localized and distributive manner. It also proposes a mean for identity verification of sender and receiver to thwart network from assault.

VAN Router: The graphically depicted VAN network consisting of 'n' nodes (A, B, C, D, E, F, ..., n) which works as both end users as well as intermediate routers to relay messages to end users, hence, providing a secure and reliable communication. The VAN Router will receive the data file from the sender and select a less cost node and send to the particular destination. The end user can seize data file from the data sender via VAN router and deliver file to selected destination without altering the File Contents. Users may be given particular data files inside the router only.

If any attacker will initiate in a van network, in such case the VAN Router will pick alternate less cost node and send to particular end user. In a VAN network

ISSN 2348 – 7968

we can assign city cost, view city details and view attackers. If we want to assign city cost, then select city name and enter new cost and accept, then it will be store in a database of VAN network.

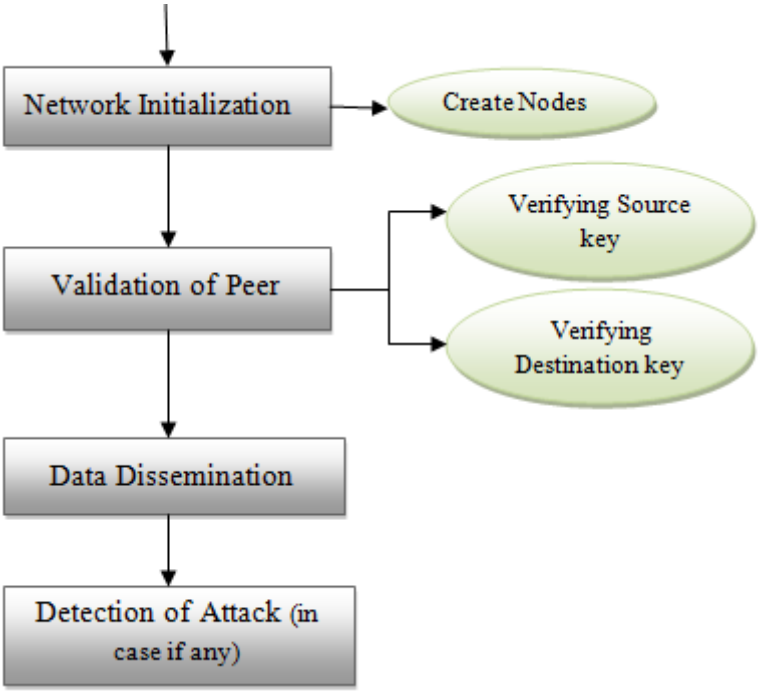


Fig 2: Proposed System Architecture

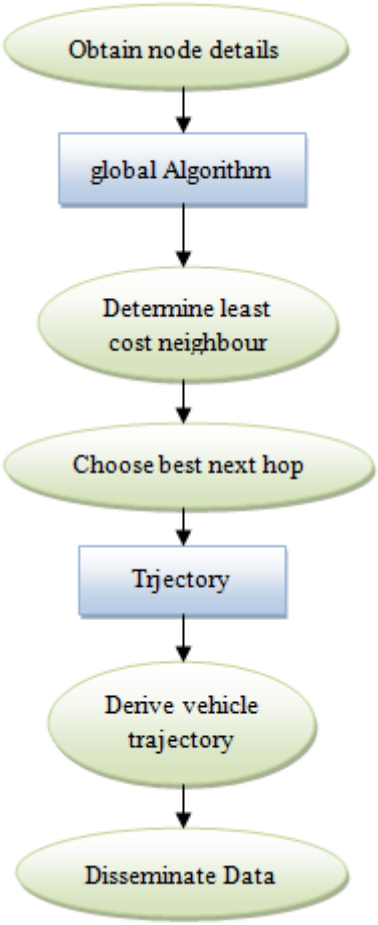


Fig 3: Dissemination of Data

Data Dissemination: In this module, the data sender will browse the data file and initialize the nodes, then select a node & send to the particular end user. Data Sender will send their data file into VAN network through which message is dispatch to the desired goal. After subsequent delivery to destination, the data sender will get response from the vanet network.

View Vehicle Trajectory: This component enable user to view vehicle trajectory and view attack destination. If click on view vehicle trajectory, then all data about vehicle with their tags such as node name, metadata, time & date can be viewed. In GPS one can also view an attacker details with their tags such as attacker name, node name, Mac address, time and date of attack.

Attacker: Attacker is one who is rerouting the trajectory node. The assailant will choose the node and insert fake key to the exacting node. Following aggressive victorious the attacker details will store in GPS and VAN router with their tags such as attacker name, city name, IP address, time & date.

5. Algorithm

5.1 System Model

The vehicular network is modelled as a collection of nodes, N = {0, 1, 2, 3....., |N|-1}. When two nodes, i and j are in the communication range (denoted by D), i.e. there is a link between the two nodes and they can communicate with each other while the link exists. The position of node n at time τ is denoting by $p_n(\tau)$. The time is divided into many slots.

Therefore, the trajectory of node n is a sequence of vehicle's location at given instances of time, represented as

$$T_n = \langle p_n(0), p_n(1), \ldots p_n(\tau) \rangle \quad (1)$$

ISSN 2348 – 7968

The set of all possible Links is denoted by L (τ)

$$L(\tau) = \{l_{i,j} \mid d_{i,j}(\tau) \le D; \forall i, j \in N\} \quad (2)$$

Minimization of delay and minimization of total cost can be represented as

$$\min \sum_{p\in\Phi} \mathbb{E}[\sigma_p], \text{ and } \min \sum_{p\in\Phi} \mathbb{E}[\varsigma_p] \quad (3)$$

Probability of packet is defined as

$$\rho_p^1 = \varepsilon_{\lambda(p),\psi(p)} \quad (4)$$

Total delivery probability is given by ρ_p

$$\rho_p = 1 - \prod_{0<h<H} \left(1 - \rho_p^h\right) \quad (5)$$

5.2 Distributed Algorithm with Session Key

Input: N, NI, M, SK, CR

START

Step1: Node updates session keys and neighbour list and exchange metadata.

Step2: First vehicle entered into communication range

Step3: Verification of session keys

Step4: if ver=success then

Step5: $\Lambda_n = \Lambda_n \cup \{n'\}$,

Step6: Node exchange metadata with another node $n' : n \leftarrow \mathcal{M}_{n'}, \quad n' \leftarrow \mathcal{M}_n$

Step7: Calculation of metric $\Delta\Phi_{n'} = \Phi_n - \Phi_{n'}$ from $\mathcal{M}_n, \mathcal{M}_{n'}$

Step8: Recalculate metric for every packet $\Delta\Theta_{p,N,t}(n') = \rho_p(n') - \rho_p(n)$

Step9: Sort the packets based on new metric in decreasing order

Step10: Transmit the packet.

Step11: updation of packet set when vehicle receives packet from neighbour.

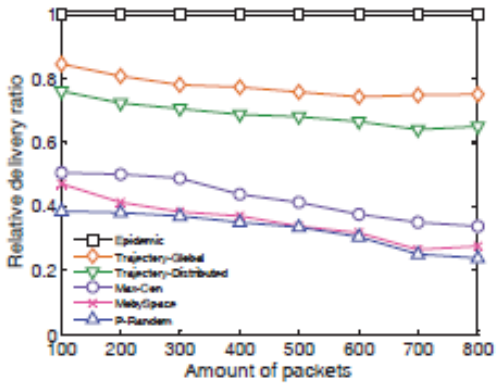
Else

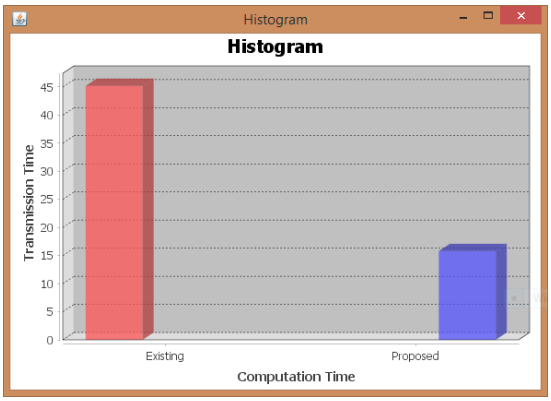
Repeat Step1.

END

Create session keys values for each vehicle in network which are pre-loaded to every registered car. Depending upon the public identity and the session key value, a vehicle can authenticate sender and receiver and broadcast messages making secure communication with other vehicles. The other vehicles in the network can also make the message authentication and identity verification through these session keys.

6. Experimental Results





The outcome of performance evaluation in terms of relative delivery ratio of proposed algorithm against other algorithms is depicted above. We are able to examine the comparable trend as shown that the proposed algorithm outperforms the current distributed algorithms and apprehend enhanced delivery ratio performance than the rest. Moreover, proposed algorithm considerably decreases transmission time of data packet. This performance gain of our algorithms is mainly due to the fact that improved routing paths with large delivery probabilities usually lead to shorter delays.

7. Conclusion

ISSN 2348 – 7968

Vehicular Ad-hoc networks have received significant consideration recently. Although data delivery of vehicular networks has been premeditated, only a few existing algorithms effectively make use of trajectories of vehicles. In this paper, an integrated approach is proposed for better data dissemination and maintaining privacy in VANETs. The proposed algorithm takes full benefits of vehicle traces. Performance results verify that our algorithm outperforms former algorithms. This reveals that forecasted vehicular traces do help information dissemination as well as in privacy preservation in vehicular networks.

8. References

[1] H. Hartenstein and K. Laberteaux, ‘‘A Tutorial Survey on Vehicular Ad Hoc Networks,’’ IEEE Commun. Mag., vol. 46, no. 6, pp. 164-171, June 2008.

[2] R.Parker and S.Valaee, “Vehicle Localization in Vehicular Networks”, Vehicular Technology Conference, 2006. VTC-2006 fall. IEEE 64th, pp. 1–5.

[3] Jinyuan Sun, Xiaoyan Zhu, Chi Zhang, and Yuguang Fang “Rescue Me: Location-Based Secure and Dependable VANETs for Disaster Rescue” , March,2011

[4] D R. Ramanthan, R. Hansen, P. Basu, R. Rosales-Hain, and R. Krishnan, "Prioritized epidemic routing for opportunistic networks," Proc. ACM MobiSys workshop on Mobile Opportunistic Networks (MobiOpp), 2007, p. 66.

[5] V. Erramilli, M. Crovella, A. Chaintreau, and C. Diot, "Delegation forwarding," Proc. ACM MobiHoc, 2008, pp. 251-260

[6] Jaehoon Jeong, Shuo Guo, Yu Gu, Tian He and David Du Department of Computer Science & Engineering, University of Minnesota, “TBD: Trajectory-Based Data Forwarding for Light-Traffic Vehicular Networks”

[7] I. Leontiadis and C. Mascolo, "Geopps: Geographical opportunistic routing for vehicular networks," Proc. IEEE WoWMoM, 2007, pp. 1-6.

[8] M. Raya and J.-P. Hubaux, “Securing vehicular ad hoc networks,” J. Computer Security, vol. 15, no. 1, pp. 39–68, Jan. 2007.

[9] Tadiparthi Priyanka,T. P. Sharma,National Institute of Technology Hamirpur (NIT-H) “Privacy in Vehicular Ad Hoc Networks: A Review”, 07th IRF International Conference, 22nd June-2014

[10] M. Raya, and J.P. Hubaux, "Securing Vehicular Ad Hoc Networks", Journal of Computer Security, Special Issue on Security of Ad Hoc and Sensor Networks, Vol. 15, no. 1, pp. 39- 68, 2007.