Secure and Privacy Preserving Smartphone Based Traffic Information System

KALLURI ANIL KUMAR
Student M.Tech
Department of ECE
SR Engineering College, Warangal, India

K.DIVYA
Assistant Professor
Department of ECE
SR Engineering College, Warangal, India

Abstract:- **The main reason for such systems would be to alleviate traffic congestion that is available in each and every major city. This project is for solving the problem by collecting traffic data, producing traffic estimates, and providing drivers with location-specific information. The Present methods designed for getting the present location through GPS. But no possibility of route map to other place from present place. Moving to desired place has become difficulty to the driver and also the traffic density in that route. The proposed method using the smart phone based traffic information system. Here TIS information is collected based on the IR Sensors that are connected with each other based on the distance which make us to know the information that number of vehicles moving on road with that information we can change the direction of route based on the number vehicles moving. This task that can't be accomplished only by depending around the security from the mobile-to-cellular infrastructure communication. But also as TISs require fine-grained location information, the privacy from the adding participants must be protected. We have to ensure their security and privacy as well as their effectiveness (e.g., precision).**

This paper used the condition of the available facilities like Road maps, path ways and available telecommunication infrastructure. Growing smart phone transmission combined with the wide coverage of cellular infrastructures, renders smart phone based traffic human resources (TISs) this is an extensive solution for smart phone-based traffic estimation that is known as secure and privacy protecting. We provide a complete-blown implementation on actual smart phones, along with a comprehensive assessment of their precision and efficiency. Our results make sure smart phone-based TISs can provide accurate traffic condition estimation while being secure and privacy protecting.

Keywords:- **Privacy; Security; Traffic Information Systems; WIFI.**

I. INTRODUCTION

TRAFFIC congestion deteriorates the quality of life of citizens and contributes significantly to environmental pollution and economic loss. Traffic information systems (TISs) aim at solving this problem by collecting traffic data, producing traffic estimates, and providing drivers with location-specific information. The increasing Smartphone penetration, along with the wide coverage of cellular networks, defines an unprecedented large-scale network of sensors, with extensive spatial and temporal coverage, able to serve as traffic probes for TISs. To reap the benefits of Smartphone-based TISs, users must participate in large numbers. Ideally, anyone possessing a Smartphone should contribute to the TIS. Nevertheless, this very openness of such systems renders them vulnerable to adversaries and malicious users. It is thus necessary to secure the collection of data and render the contributing users (smart-phones) accountable. This is a task that cannot be achieved only by relying on the security of the mobile-to-cellular infrastructure communication. It's thus essential to secure the assortment of data and render the adding customers (smart phones) accountable. This can be a task that can't be accomplished only by depending around the security from the mobile-to-cellular infrastructure communication. Simultaneously, as TISs require fine-grained location information, the privacy from the adding participants must be protected. Traffic congestion deteriorates the caliber of existence of citizens and contributes considerably to environmental pollution and economic loss [1]. Traffic human resources (TISs) goal at fixing this issue by collecting traffic data, producing traffic estimations, and supplying motorists with location-specific information. The growing Smartphone transmission, along with the wide coverage of cellular systems, defines an unprecedented large-scale network of sensors, with extensive spatial and temporal coverage, in a position to function as traffic probes for TISs. To make use of Smartphone-based TISs, customers must participate in large figures. Ideally, anybody having Smartphone should lead towards the Inc. This requirement for privacy is intensified within the context of Smartphone-based TISs. Smart phones already reveal a great deal of, possibly sensitive, information towards the cellular operators. Balancing security, privacy, effectiveness and efficiency is not straightforward. We present a Smartphone-based Inc. and assess its accuracy through GPS (GPS navigation) traces within the presence of traffic estimation errors as well as for different values of location reporting rates and accumulation frames. In addition, by leveraging cellular providers, existing telecommunication standards and condition-of-the-art cryptographic schemes, we propose comprehensive privacy and security-protecting architecture, resilient against problem customers and TISs organizations. We formally assess the privacy and security qualities from the system and demonstrate its efficiency through extensive evaluations [2].

A. TISs: Condition-of-the-practice traffic data collection depends on roadside sensors, e.g., inductive loop sensors (ILDs), to collect information about traffic flow at fixed points on the highway network [5]. Although broadly recognized, using fixed sensors comes having a high deployment cost. Furthermore, Road side sensors are deficient in estimating the rate of vehicles passing over a road link because they appraise the speed in the place of deployment. The literature also indicates using devoted automobiles, i.e., probe automobiles (PVs), as floating traffic probes [4]. Pare outfitted with Gps navigation receivers and devoted communication links. A lot of such devoted automobiles render accurate traffic status estimations achievable. Nonetheless, the cost of getting devoted communication links between your in vehicle equipment and also the traffic management center is still restricting factor [3]. Smartphone-based road status estimation eliminates considerable installation and maintenance costs, in terms of vehicle equipment and Road side infrastructure. Previous works employed network-based probe techniques that leverage network signaling information, e.g., handoff information or time/position (difference) of arrivals. Nonetheless, a few of them were handset based (i.e., using Gps navigation-enabled phones).The communications cost and the slow update of Gps navigation-enabled phones. Nevertheless, these obstacles happen to be bypassed through the growing capacity of modern cellular systems and also the current Smartphone share of the market.

B. Privacy and security Issues: Developing TISs that collect location samples from products, transported by people within their everyday lives, poses serious privacy implications. Simultaneously, the exchanged data must be reliable because the feedback supplied by the Inc. affects the actual traffic conditions. TISs require strong guarantees with respect towards the security from the communications and the privacy from the people adding towards the Inc. For this finish, authentication, access control, and confidentiality mechanisms must maintain place. Furthermore, attacks individuals location privacy from the taking part customers ought to be reduced. Even When location samples are collected within an anonymous manner (thus not revealing the actual identity of customers), breaching user privacy continues to be possible. More particularly, successive anonymous location updates from smart phones still reveal spatial and temporal correlations you can use as indirect identifiers. Such correlations could be used by monitoring techniques [2], to rebuild a vehicle’s location and, thus, infer frequently visited places, e.g., home or place of work. In such cases, user deanonymization might be easy. To beat these threats, path cloaking and privacy-protecting sampling techniques happen to be suggested. Within this paper, we all do not consider risks against data teams of location samples rather, we attempt to deal with the issue of acquiring communications and interactions inside the system while getting rid of any direct link between a tool and it is location. The identity from the devices encoded having a symmetric key recognized to the ID proxy. Similarly, the place details are encoded using the public key from the traffic server thus, it's accessible only because of it. These keys are in place and placed on the mobile client during its initialization. The plan accomplishes privacy underneath the assumption that the traffic and also the ID proxy servers don't collude and it takes a 3rd party for that identity management. This point introduces an additional burden for deployment and requires 3rd party that establishes trust relations using the clients participating within the TISs. Vehicular ad-hoc systems (VANETs) are based on TISs. They might even link interactions of a mobile using the Inc., or other service, by means of unique identifiers like the Worldwide Mobile Subscriber Identity (IMSI) and also the Worldwide Mobile Station Equipment Identity (IMEI). A whole lot worse, just in case cellular providers collude with the Inc. server, that customers submit their traffic reviews, it’s trivial to recognize customers and completely rebuild their whereabouts. Finally, Smartphone-based TISs could be seen as an instantiation of participatory sensing (PS) systems, which raise similar privacy and security challenges.

II. SECURE AND PRIVACY-PRESERVING TISS

An introduction to our smart phone-based TIS. The machine comprises smart phone clients, outfitted with A-GPS navigation receivers, along with a traffic estimation server because the back-end infrastructure. A credit card application is a component of each smart phone to report periodically the position of the device towards the traffic information server in order to query the server for traffic conditions in its closeness. The traffic estimation server processes the client-posted data and reacts to queries with predefined values representing the typical speed on every road link in the area from the querying Smartphone. We simulate urban road systems and traffic conditions by generating “actual” location tracks for every vehicle/mobile. The generated location samples are preprocessed and degraded to emulate “realistic” dimensions. This preprocessing defines the number of automobiles which are outfitted having a-Gaps navigation mobile phones (based on a transmission rate) and introduces statistical errors towards the location updates. Then, the place data are post processed with a two-step filtering process. A simple data screening plan is utilized to remove unexpected position and speed estimations. This filtering process assigns speed estimations to any or all road links which are later aggregated at predefined time times. According to specified thresholds, the estimated link speeds has sorted out into several traffic condition levels, highlighted as colored road segments around the Smartphone displays.

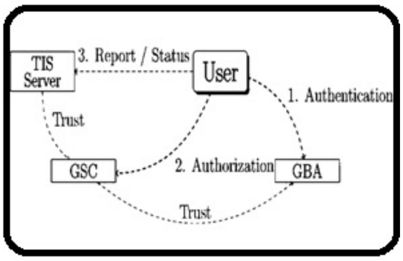
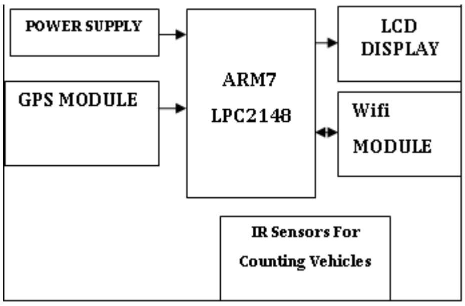


Fig.1. Proposed System Overview



Hardware Architecture

III. CONCLUSION

This paper has proven a comprehensive analysis around the feasibility of implementing Smartphone-based TISs. We presented a localization algorithm, appropriate for Gaps navigation location samples, and evaluated it through realistic simulations. In addition, leveraging state-of-the-art cryptographic and telecommunication schemes, we presented an extensive privacy and security-preserving architecture for Smartphone-based Ienc. Our results confirm it's achievable to construct accurate and trustworthy Smartphone-based Inc. Nonetheless, you will find still challenges ahead: Privacy and security cannot, alone, incentivize uses to sign up in large figures. Toward this, it’s interesting to supply fair and privacy-protecting incentive mechanisms.

IV. REFERENCES

[1] M. A. Ferman, D. E. Blumenfeld, and X. Dai, “An analytical evaluationof a real-time traffic information system using probe vehicles,” *J. Intell.Transp.Syst.*, vol. 9, no. 1, pp. 23–34, 2005.

[2] M. Fontaine, B. Smith, A. Hendricks, and W. Scherer, “Wireless locationtechnology-based traffic monitoring: preliminary recommendationsto transportation agencies based on synthesis of experience and simulationresults,” *Transp. Res. Rec., J. Transp. Res. Board*, vol. 1993, pp. 51–58,2007.

[3] B. Hoh, M. Gruteser, H. Xiong, and A. Alrabady, “Preserving privacyin GPS traces via uncertainty-aware path cloaking,” in *Proc. 14thACM Conf. Comput.Commun.Secur.*, Alexandria, VA, USA, 2007,pp. 161–171.

[4] N. Alexiou, M. Lagana, S. Gisdakis, M. Khodaei, and P. Papadimitratos,“VeSPA: Vehicular security and privacypreserving architecture,” in *Proc.ACMHotWiSec, colocated with ACM WiSec*, Budapest, Hungary, 2013,pp. 19–24.

[5] T. Moore *et al.*, “Fast exclusion of errant devices from vehicular networks,”in *Proc. 5th IEEE-CS Conf. SECON*, San Francisco, CA, USA,2008, pp. 135–143.