IPHV7I10025X
International Journal Of Advanced Research and Innovation -Vol.7, Issue .I
ISSN Online: 2319 – 9253
Print: 2319 – 9245

USAGE OF ROAD SIDE ACCESS POINTS TO COOPERATIVE DOWNLOAD IN VEHICULAR ENVIRONMENTS

[1] Mupparaju Vatsalya, [2] V. Saipriya

Department of Computer Science and Engineering,
Vignan's Nirula Institute of Technology and Science for Women.Guntur, A.P,India

Abstract: **-** To download the contents from users aboard vehicles, we use the SPAWN protocol for the retrieval and sharing of contents vehicular environments. SPAWN is designed for unidirectional traffic over a highway, and is built on the assumption that all on-road vehicles are active downloader's of a same content. We consider a complex (i.e., non-linear) road scenario where users aboard vehicles equipped with communication interfaces are interested in downloading large files from road-side Access Points (APs). We investigate the possibility of exploiting opportunistic encounters among mobile nodes so to augment the transfer rate experienced by vehicular downloader's. To that end, we devise solutions for the selection of carriers and data chunks at the APs, and evaluate them in real-world road topologies, under different AP deployment strategies. Through extensive simulations, we show that carry & forward transfers can significantly increase the download rate of vehicular users in urban/suburban environments, and that such a result holds throughout diverse mobility scenarios, AP placements and network loads.

Keywords:- *Sybil attack, SPAWN Protocol, traffic control, urban vehicular networks, location-hidden trajectory.*

I.INTRODUCTION

Vehicles traveling within cities and along highways are regarded as most probable candidates for a complete integration into mobile networks of the next generation. Vehicle-to infrastructure and vehicle-to-vehicle communication could indeed foster a number of new applications of notable interest and critical importance, ranging from danger warning to traffic congestion avoidance. It is however easy to foresee that the availability of onboard communication capabilities will also determine a significant increase in the number of mobile users regularly employing business and infotainment applications during their displacements. As a matter of fact, equipping vehicles with WiMAX/LTE and/or WiFi capabilities would represent a clear invitation for passengers on cars or buses to behave exactly as home-based network users. The phenomenon would thus affect not only lightweight services such as web browsing or e-mailing, but also resource-intensive ones such as streaming or file sharing. In this paper, we focus on one of the latter tasks, namely the download of large-sized files from the Internet. More precisely, we consider a urban scenario, where users aboard cars can exploit roadside Access Points (APs) to access the servers that host the desired contents. We consider that the coverage provided by the roadside APs is intermittent: this is often the case, since, in presence of large urban, suburban and rural areas, a pervasive deployment of APs dedicated to vehicular access is often impractical, for economic and technical reasons. We also assume that not all on-board users download large files all the time: indeed, one can expect a behavior similar to that observed in wired networks, where the portion of queries for large contents is small . As a result, only a minor percentage of APs is simultaneously involved in direct data transfers to downloader cars in their respective coverage area, and the majority of APs is instead idle.

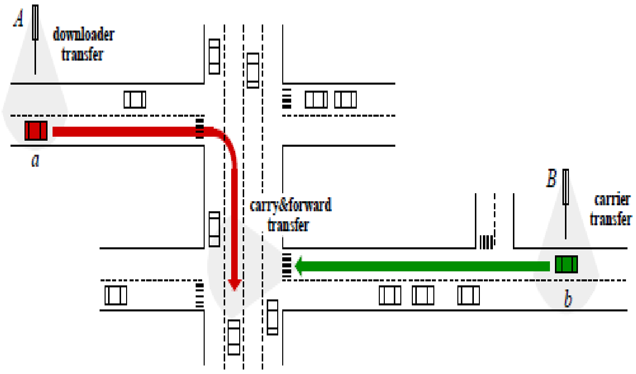

Fig. 1. Vehicle a downloads part of some content from AP A. The idle AP B delegates another portion of the same content to a vehicle b. When b encounters a, vehicle-to-vehicle communication is employed to transfer to a the data carried by b

Within such a context, we study how opportunistic vehicle-tovehicle communication can complement the infrastructure-based connectivity, so to speed up the download process. We exploit the APs inactivity periods to transmit, to cars within range of idle APs, pieces of the data being currently downloaded by other vehicles. Cars that obtain information chunks this way can then transport the data in a *carry&forward* fashion , and deliver it to the destination vehicle, exploiting opportunistic contacts with it, as in Fig. 1. We remark that the concept of cooperative download in vehicular networks has been already proposed for highway environments: however, unlike what happens over unidimensional highways, urban/suburban road topologies present multiple route choices that make it hard to predict if vehicles will meet;moreover, the presence of traffic lights, stop and yield signs renders cars contact timings very variable. These key aspects make highway-tailored solutions impracticable in complex nonlinear road scenarios, for which we are, to the best of our knowledge, the first to identify challenges and propose solutions.

Detecting Sybil attacks in urban vehicular networks, however, is very challenging. First, vehicles are anonymous. There are no chains of trust linking claimed identities to real vehicles. Second, location privacy of vehicles is of great concern. Location information of vehicles can be very confidential. For example, it can be inferred that the driver of a vehicle may be sick from knowing the vehicle is parking at a hospital. It is inhibitive to enforce a one-to-one correspondence between claimed identities to real vehicles by verifying the physical presence of a vehicle at a particular place and time. Third, conversations between vehicles are very short. Due to high mobility of vehicles, a moving vehicle can have only several seconds [4] to communicate with another occasionally encountered vehi-cle. It is difficult to establish certain trustworthiness among communicating vehicles in such a short time. This makes it easy for a malicious vehicle to generate a hostile identity but very hard for others to validate. Furthermore, short conversations among vehicles call for online Sybil attack detection. The detection scheme fails if a Sybil attack is detected after the attack has terminated.

II. RELATED WORK

While it was first described and formalized by Douceur [3], the Sybil attack has been a severe and pervasive problem in many forms. In a Sybil attack, an attacker can launch a Sybil attack by forging multiple identifies, gaining a dispropor-tionately large influence. In the literature, there have been many different approaches proposed to detect or mitigate the attack.

Many studies have followed Douceur’s approach, focus-ing on how to establish trust between participating entities based on trusted public key cryptographies or certificates in distributed systems, for example, P2P systems [3], [5], sensor networks [6], [7] and mobile ad hoc networks [8]. Although deploying trusted certificates is the only approach that has the potential to completely eliminate Sybil attacks, it also violates both anonymity and location privacy of entities. In addition, most of these schemes rely on a centralized authority that must ensure each entity is assigned exactly one identity. Moreover, it is possible for an attacker to violate the assumption, getting more than one identities. This mechanism also has the problem of key revocation which is challenging, particularly in wireless mobile networks.

Another category of Sybil attack detection schemes is based on resource testing [9], [10], [11]. The goal of resource testing is to determine if a number of identities possess fewer resources than would be expected if they were independent. The resources being tested can be computing ability, storage ability, and network bandwidth, as well as IP addresses. These schemes assume that entities have homogeneous hardware configurations. In vehicular networks, this assumption cannot hold since malicious vehicles can easily have more powerful resources than the normal vehicles.

SybilGuard [12] is an interesting scheme studying the social network among entities. In this scheme, human-established real-world trust relationship among users is used for detecting Sybil attacks. Since even the attacker can generate as many as Sybil identities, building relationship between honest users and Sybil identities is much harder. Thus, there exists a small “cut” on the graph of trust relationship between the forged identities and the real ones. However, this scheme cannot be used in vehicular net-works, since it is very challenging to establish such trust relationship among vehicles. This is because vehicles are highly mobile. Communications often happen among temporarily met and unfamiliar vehicles.

To exploit the fact that one single vehicle cannot present at multiple locations at the same time, Bouassida et al. [13] have proposed a detection mechanism utilizing localization technique based on Received Signal Strength Indication (RSSI). In this scheme, by successively measuring the RSSI variations, the relative locations among vehicles in vicinity can be estimated. Identities with the same estimated locations are considered as Sybil vehicles. In practice, the complicated outdoor environments can dramatically affect the wireless signal propagation so that RSSI measurements are highly time variant even measured at the same location. Xiao et al. [14] have proposed a Sybil attack detection scheme where the location of a particular vehicle can be determined by the RSSI measurements taken at other participating vehicles. In addition to the inaccuracy of RSSI measurements, this scheme also needs all neighboring vehicles to collaborate which may suffer a Sybil attack against the detection scheme itself. Zhou et al. [15] have proposed a privacy-preserving Sybil attack detection scheme using pseudonyms. In the scheme, the trust authority distributes a number of pseudonyms for each vehicle. Abused pseudonyms can be detected by RSUs. Since RSUs are heavily involved in the detection process, this scheme requires the full coverage of RSUs in the field. It is infeasible in practice due to the prohibitive cost. Furthermore, in such a scheme, vehicles should managed by a centralized trusted center. Each time RSU detects suspicious pseudonyms, it should send all the pseudonyms to the trust center for further decision, which makes the trust center be the bottleneck of the detection.

III. IMPLEMENTATION

System Model and Assumptions

In vehicular networks, a moving vehicle can communicate with other neighboring vehicles or RSUs via intervehicle communications and roadside-to-vehicle communications. Fig. 1 illustrates the architecture of the system model, which consists of three interactive components:

. RSUs: can be deployed at intersections or any area of interest (e.g., bus stations and parking lot entrances). A typical RSU also functions as a wireless AP (e.g., IEEE 802.11x) which provides wireless access to users within its coverage. RSUs are interconnected (e.g., by a dedicated network or through the Internet via cheap ADSL connections) forming a RSU backbone network.

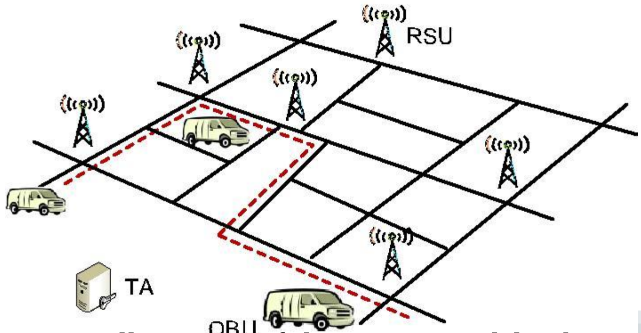

Fig. 1. An illustration of the system model, where the dash line indicates the travel route of a vehicle. As the vehicle traverses the area, it will encounter multiple RSUs, typically deployed at intersections.

. On-board units (OBUs): are installed on vehicles. A typical OBU can equip with a cheap GPS receiver and a short-range wireless communication module (e.g., DSRC IEEE 802.11p [20]). A vehicle equipped with an OBU can communicate with an RSU or with other vehicles in vicinity via wireless connections. For simplicity, we simply refer to a vehicle as a vehicle equipped with an OBU in the rest of this paper. A vehicle can be malicious if it is an attacker or compromised by an attacker.

. Trust authority: is responsible for the system initialization and RSU management. The TA is also connected to the RSU backbone network. Note that the TA does not serve vehicles for any certification purpose in Footprint. A vehicle can claim as many arbitrary identities as it needs.

Trajectory-Encoded Message

Intuitively, an authorized message issued from an RSU can be used to identify a vehicle. However, it is often the case that two or more authorized messages may have the same link tag. In this case, it is hard to tell whether these messages belong to different vehicles.

With the independent mobility assumption, as two vehicles move along, the probability for the pair of vehicles having exactly the same trajectories is slim. Therefore, it is feasible to use trajectories to exclusively represent corre-sponding vehicles as long as those trajectories are suffi-ciently long. With authorized messages, a straightforward method for a vehicle to present its trajectory is to sort all its authorized messages into a sequence according to time. Thus, in future conversations, the vehicle can use this sequence of authorized messages to identify itself. This method is simple but inefficient because each time when the vehicle needs to be identified in a conversation, all messages in the sequence should be sent to the conversation holder for verification. This will cost tremendous wireless bandwidth and computational resources. Furthermore, a malicious vehicle can easily forge a huge number of fake trajectories by arbitrarily picking a subset of authorized messages as long as these messages are in the right order of time. Since authorized messages are location hidden, the conversation holder cannot tell whether a provided trajectory is an actual one or a forged one.

In Footprint, we embed the trajectory of a vehicle into an authorized message. Specifically, upon the starting of a new event, besides computing the new event id and link tag for the new event, an RSU also informs all its neighboring RSUs with the new generated link tag. During the new event, when a vehicle first meets an RSU R_k, it requests an authorized message M k S_{Rk} ðMÞ from R_k using temporary key pair ðKv^{pub};j; Kv^{pri};jÞ following the procedure as described in i i

As this vehicle moves on and encounters another RSU R_l, it first chooses a new temporary key pair
pub $_K$pri $_K$pub S
$^{ðK}v_i$;jþ ^{Rk}
1 $^{;}$ $_{pri}v_i$;jþ$1^{Þ. Then, it}$ signs on v_i;jþ$1^{k M k}$ ðMÞ,
using . After that, it requests R_l for a new
K trajectory-
$^{vi\ þj}$ authorized message by sending
K^{pub}
embeddedPub v_i;jþ$1^{k M k}$
$^{S}R_k$ ðMÞ k $^{SK}{}_{vi;jþ1}$$^{;}$ M$^{;}$ ðMÞÞ to R_l. Upon request, R_l
$^{S}R_k$ first
verifies the authorized message following the procedure described in the above section. If the verification succeeds, R_l further checks whether the link tag in S_{Rk} ðMÞ belongs to one of its neighbors. If yes, R_l constitutes a new message

with the new temporary public key of the vehicle Kv^{pub};jþ1,I current time stamp, all (link tag, time stamp) pairs contained in M if any. Then, R_l signs on the new message and sends the trajectory-embedded authorized message back to the vehicle. If the link tag contained in S_{Rk} ðMÞ does not belong to any neighboring RSU of R_l, R_l will treat itself as the first RSU in the trajectory of the vehicle and sign accordingly. This procedure repeats as the vehicle moves. As a result, a trajectory is embedded within a single authorized message (see Appendix F, available in the online supplemental material, for an example of trajectory generation).

Within an event, a vehicle can actively choose to terminate the current trajectory and start a new trajectory at any time by sending only a new temporary public key to an RSU. When an event expires, all RSUs will simulta-neously change their link tags. In this case, the system forces all vehicles to start new trajectories.

With trajectory-encoded messages, each time when a vehicle needs to be identified, the vehicle only needs to send a single authorized message to a verifier which extremely reduces the number of verifications from OðlÞ to Oð1Þ, l is the length of the trajectory (i.e., the number of involved RSUs). Moreover, the trajectory encoded in an authorized message is verified and constructed by neighboring RSUs, which largely limits the ability of a malicious vehicle to arbitrarily forge fake trajectories.

IV.SYBIL ATTACK DETECTION

During a conversation, upon request from the conversation holder, all participating vehicles provide their trajectory-embedded authorized messages issued within specified event for identification. With submitted messages, the conversation holder verifies each trajectory and refuses those vehicles that fail the message verification. After that, the conversation holder conducts online Sybil attack detection before further proceeding with the conversation.

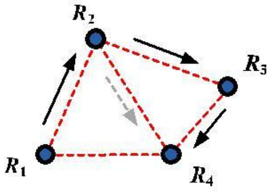

Fig. 2. RSU neighboring relationship and the freedom of trajectory generation can facilitate Sybil trajectory generation. In the above figure, neighboring RSUs (denoted by dots) are connected with dash line. The solid arrows indicate the actual sequence of RSUs a malicious meet and the dash arrow presents a possible forged trajectory.

Recall that, in Footprint, vehicles have wide freedom to create their trajectories. For example, a vehicle is allowed to request multiple authorized messages from an RSU using different temporary key pairs. Thus, a vehicle can use different authorized messages for different conversations. This capability, however, can be leveraged by a malicious vehicle that tries to launch a Sybil attack by using multiple different messages in a single conversation. We define the Sybil attack detection problem as: Given a set of trajectory-embedded authorized messages within an event, how can the conversation holder recognize real vehicles and Sybil ones?

The online Sybil attack problem is hard due to three following factors:

First, authorized messages generated for different vehi-cles are asynchronous. The rationale of using trajectories to represent vehicles is based on the fact that a vehicle cannot present itself at different locations at the same time. The asynchrony of messages makes the judgment directly based on this fact impractical.

Second, authorized messages are temporarily linkable, which means there is no invariable mapping between an RSU signature and the real RSU who signed this signature. Thus, no distance information is available between two RSUs enclosed in any two signatures. This makes the problem even harder since one cannot utilize the time difference between two authorized messages and the distance between the pair of corresponding RSUs to infer whether two messages belong to two distinct vehicles.

Last, a malicious vehicle can abuse the freedom of trajectory generation and the neighbor relationship among RSUs to generate elaborately designed trajectories. For example, in Fig. 2, an attacker can legally generate multiple trajectories which appear different from each other even under a very simple RSU topology. Assume the real path of the attacker is fR_1; R_2; R_3; R_4g (indicated by solid arrows). It can start a new trajectory at any RSU by using a different temporary key pair. Therefore, besides the trajectory fR_1; R_2; R_3; R_4g, trajectories like fR_1; R_2; R_3g, fR_2; R_3; R_4g, fR_1; R_2g; fR_2; R_3g, fR_3; R_4g, fR_1g, fR_2 g, fR_3g and fR_4g are all legitimate. In addition, knowing the neighboring relation-ship of R_2 and R_4, the attacker can generate forged trajectories like fR_1; R_2; R_4g, fR_1; R_4g, and fR_2; R_4g (indicated by the dash arrow). Note that the attacker cannot generate a trajectory like fR_1; R_3g because R_1 is not a neighbor of R_3. In the case of this example, R_3 only expects signatures signed by R_2 and R_4.

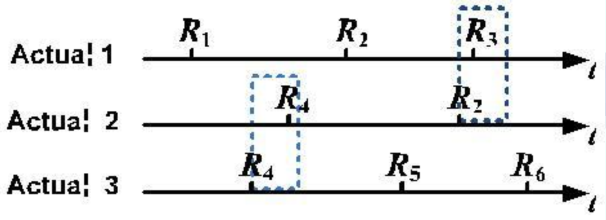

Fig. 3. Checking for distinct trajectories by using a check window (denoted as the box of dotted line) and counting the total number of different RSUs contained in a pair of trajectories.

In the following sections, we present the social relation-ship between two trajectories according to our definition of similarity. Then, we introduce how to find and remove Sybil trajectories.

V.CONCLUSION

We presented a complete study of cooperative download in urban vehicular environments. We identified and proposed solutions to the problems of carriers selection and chunk scheduling, and extensively evaluated them. The main contribution of this work lies in the demonstration that vehicular cooperative download in urban environments can bring significant download rate improvements to users traveling on trafficked roads in particular. we have developed a Sybil attack detection scheme Footprint for urban vehicular networks. Consecu-tive authorized messages obtained by an anonymous vehicle from RSUs form a trajectory to identify the corresponding vehicle. Location privacy of vehicles is preserved by realizing a location-hidden signature scheme. Utilizing social relationship among trajectories, Footprint can find and eliminate Sybil trajectories.

REFERENCES

[1]. Footprint: Detecting Sybil Attacks in Urban Vehicular Networks, Shan Chang, Yong Qi, Member, IEEE, Hongzi Zhu, Member, IEEE, Jizhong Zhao, Member, IEEE, and Xuemin (Sherman) Shen, Fellow, IEEE,2012.

[2]. Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, "An Efficient Pseudonymous Authentication Scheme with Strong Privacy Preservation for Vehicular Communications," IEEE Trans. Vehi-cular Technology, vol. 59, no. 7, pp. 3589-3603, Sept. 2010.

[3]. R. Lu, X. Lin, H. Zhu, and X. Shen, "An Intelligent Secure and Privacy-Preserving Parking Scheme through Vehicular Commu-nications," IEEE Trans. Vehicular Technology, vol. 59, no. 6, pp. 2772-2785, July 2010.

[4]. J.R. Douceur, "The Sybil Attack," Proc. First Int'l Workshop Peer-to-Peer Systems (IPTPS '02), pp. 251-260, Mar. 2002.

[5]. M. Castro, P. Druschel, A. Ganesh, A. Rowstron, and D.S. Wallach, "Secure Routing for Structured Peer-to-Peer Overlay Networks," Proc. Symp. Operating Systems Design and Implementa-tion (OSDI '02), pp. 299-314, Dec. 2002.

[6]. B. Dutertre, S. Cheung, and J. Levy, "Lightweight Key Manage-ment in Wireless Sensor Networks by Leveraging Initial Trust,"

Technical Report SRI-SDL-04-02, SRI Int'l, Apr. 2002.

[7]. J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil Attack in Sensor Networks: Analysis & Defenses," Proc. Int'l Symp. Information Processing in Sensor Networks (IPSN '04), pp. 259-268, Apr. 2004.

[8]. S. Capkun, L. Buttyan,_ and J. Hubaux, "Self-Organized Public Key Management for Mobile Ad Hoc Networks," IEEE Trans. Mobile Computing, vol. 2, no. 1, pp. 52-64, Jan.-Mar. 2003.

[9]. C. Piro, C. Shields, and B.N. Levine, "Detecting the Sybil Attack in Mobile Ad Hoc Networks," Proc. Securecomm and Workshop, pp. 1-11, Aug. 2006.

[10]. N. Borisov, "Computational Puzzles as Sybil Defenses," Proc. Sixth IEEE Int'l Conf. Peer-to-Peer Computing (P2P '06), pp. 171-176, Oct. 2006.

[11]. P. Maniatis, D.S.H. Rosenthal, M. Roussopoulos, M. Baker, T. Giuli, and Y. Muliadi, "Preserving Peer Replicas by Rate-Limited Sampled Voting," Proc. 19th ACM Symp. Operating Systems Principles (SOSP '03), pp. 44-59, Oct. 2003.

[12]. H. Yu, M. Kaminsky, P.B. Gibbons, and A. Flaxman, "Sybilguard: Defending against Sybil Attacks via Social Networks," Proc. SIGCOMM, pp. 267-278, Sept. 2006.

[13]. M.S. Bouassida, G. Guette, M. Shawky, and B. Ducourthial, "Sybil Nodes Detection Based on Received Signal Strength Variations within Vanet," Int'l J. Network Security, vol. 9, no. 1, pp. 22-32, 2009.

[14]. B. Xiao, B. Yu, and C. Gao, "Detection and Localization of Sybil Nodes in Vanets," Proc. Workshop Dependability Issues in Wireless Ad Hoc Networks and Sensor Networks (DIWANS '06), pp. 1-8, Sept. 2006.

[15]. T. Zhou, R.R. Choudhury, P. Ning, and K. Chakrabarty, "Privacy-Preserving Detection of Sybil Attacks in Vehicular Ad Hoc Networks," Proc. Fourth Ann. Int'l Conf. Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous '07), pp. 1-8, Aug. 2007.

[16]. Q. Wu, J. Domingo-Ferrer, and U. Gonzalez_-Nicola´s, "Balanced Trustworthiness, Safety and Privacy in Vehicle-to-vehicle Com-munications," IEEE Trans. Vehicular Technology, vol. 59, no. 2, 559-573, Feb. 2010.

[17]. L. Chen, S.-L. Ng, and G. Wang, "Threshold Anonymous Announcement in VANETs," IEEE J. Selected Areas in Comm., vol. 29, no. 3, pp. 1-11, Mar. 2011.

[18]. C. Chen, X. Wang, W. Han, and B. Zang, "A Robust Detection of the Sybil Attack in Urban Vanets," Proc. IEEE Int'l Conf. Distributed Computing Systems Workshops (ICDCSW '09), pp. 270-276, June 2009.

[19]. S. Park, B. Aslam, D. Turgut, and C.C. Zou, "Defense against Sybil Attack in Vehicular Ad Hoc Network Based on Roadside Unit Support," Proc. 28th IEEE Conf. Military Comm. (MILCOM '09), 1-7, Oct. 2009.

[20]. IEEE Vehicular Technology Soc.: 5.9 GHz Dedicated Short Range Comm. (DSRC) - Overview. http://grouper.ieee.org.groups/ scc32/dsrc/, 2011.

Author's Profile:

1. MUPPARAJU. VATSALYA M.Tech (CSE) Department of Computer Science & Engineering at Vignan's Nirula Institute Of Technology & Science for Women, Guntur.

2. V. SAIPRIYA received B.Tech (CSIT) from JNTUH, M.Tech(C.S.E) from JNTUK she is currently working as an Assistant Professor, department of Computer Science & Engineering at Vignan's Nirula Institute Of Technology Science for Women, Guntur. She guided many projects in the area of image processing. Her area of interest is leaf Image Processing.