On Location Security Solutions in Vehicular Ad Hoc Networks

Rasheed Hussain*, Junggab Son, and Heekuck Oh*
*Dept. of Computer Science and Engineering, Hanyang University
e-mail : {rasheed, hkoh}@hanyang.ac.kr

Abstract

Location information is considered to be of prime importance in Vehicular Ad Hoc NETworks (VANETs) because important decisions are made based on accurate and sound location information. Vehicles exchange their whereabouts in the form of scheduled beacon messages with their neighbors. These messages contain location, speed, time, and lane information etc. In this paper we aim at the location security in VANET and emphasize on the confidentiality and integrity of location information in case of Nonline-of-Sight (NLoS). For location confidentiality we propose a geolock-based mechanism whereas for location integrity we leverage cooperation among neighbors. In case of NLoS, the verifier vehicle asks its one-hop neighbors in an efficient way to verify the claimed location of the node on his behalf. On the basis of trust values and weightage assigned to neighbors, it is decided whether the verification is sound.

1. Introduction

Since the recent past, car manufacturing companies backed up by academia and research institutions, have been gearing up to equip cars with computation and communication resources. The aim is crystal clear, to allow drivers and passengers to communicate with each other as well as with the static infrastructure alongside the road. Such system known as Vehicular Ad Hoc NETwork (VANET) is expected to revolutionize the driving experience by making it safe and comfortable. VANET employs two communication paradigms also known as zero-infrastructure (Vehicle-to-Vehicle communication) and infrastructure-based (Vehicle-to-Roadside communication) [1,2]. By exploiting aforementioned communication paradigms, VANET offers variety of application ranging from traffic information and safety to infotainment on the road [3-5]. Nevertheless, the catastrophic repercussions of several security attacks and privacy concerns in VANET are still being worked out by research community [6, 7].

To enable location-aware services in VANET, vehicles need to exchange their whereabouts with the neighbors. The information includes location, speed, heading etc. and is collectively called beacon messages. The frequency with which beacon messages must be broadcasted, is still controversial although Dedicate Short Range Communication (DSRC) defined a static frequency range from 100ms to 300ms [8].

Location information along with other information in beacon is prone to serious attacks and will have devastating consequences. For instance false position information will drastically change the network topology and affect the routing functionality [9]. It is worth noting that the forwarding decisions are made based on the beacon information in hand. If the position information in beacon or other messages happens to be wrong, then it can greatly affect the routing efficiency. For example a node could simply lie about its position so that it could become the next forwarding node. Such scenarios are most likely in greedy forwarding where the farthest node is selected to be the next forwarder. In such cases, location verification becomes essential. Nevertheless keeping the beacons frequency in mind, it may not be ideal to verify the location in every beacon.

In this paper we address two parameters from location security: location confidentiality and location integrity. VANET attackers are divided into two major classes namely insiders and outsiders [10]. With injecting bogus information capability in hand, outsiders could have devastating consequences on VANET application. Therefore we put forth a geolock-based scheme in order to preserve the confidentiality of location in message exchange. We believe that the messages which are meant for VANET application, it

* This research was supported by the MKE (The Ministry of Knowledge Economy), Korea, under the ITRC (Information Technology Research Center) support program (NIPA-2012-H0301-12-4004) supervised by the NIPA (National IT Industry Promotion Agency).

* This work was supported in part by the National Research Foundation of Korea (NRF) grant funded by the Ministry of Education, Science and Technology (No. 2012-R1A2A2A01046986).

might not be necessary to keep the contents of the messages confidential from insiders. But we could limit the scope effect of the messages. For instance beacon messages are normally meant for one-hop neighbors. Multi-hop beaconing is still controversial in the literature [11]. The advantage of geolock-based mechanism is threefold; it keeps the outsiders from injecting bogus information to the network, it does not allow stale messages to linger around in the network, and the messages are meant for a portion of specific geographic location (for instance beacon messages are meant for only one-hop neighbors). For location integrity we put forth a cooperative based approach to handle Nonline-of-Sight (NLoS) issues in VANET and prove the soundness of the claimed location in messages. The rest of the paper is organized as follows.

Section 2 gives a brief overview of the related work and in section 3; we outline our proposed scheme followed by concluding remarks in section 4.

2. Related Work

An ample amount of research has been carried out to secure the location information in VANET. Leinmuller et al. [12] outlined position verification approaches in VANET. Their proposed mechanisms are capable of recognizing nodes that cheat about their location in beacon messages. They employ verification sensors in their proposed scheme. Xiao et al. [13] proposed an RSS (Received Signal Strength) based Sybil attack detection scheme in VANET. Their proposed scheme is distributed in nature and the vehicles on road perform '*Sybil node detection*' by verifying the claimed positions of the neighbor vehicular nodes. This verification is based on the strength of the received signal from the claimer. Nevertheless, smart malicious nodes with much more resources than benign nodes, could manually configure the signal strength to create a powerful illusion. Moreover perfect line of sight is necessary for such scheme to work. Another such scheme is proposed by Yan et al. [14] to prove the announced position of the vehicle by employing in-vehicle radars. The limitations of their scheme are the same as Xiao et al.'s scheme.

Recently Osama et al. [15] proposed a location verification mechanism which is a remedy for NLoS scenarios in VANET. They proposed a cooperative mechanism where in case of NLoS the verifier queries its neighbors to verify the claimed position on verifier's behalf. The verifier has no direct line of sight to the claimer, so it verifies the claimed position indirectly with the help of other neighbors. The neighbors who are in direct line of sight with the claimer, cross-check RSS-based calculated distance from the claimer with the radar-based calculated distance. It is worth noting that in their scheme, colluding attack might be possible if the neighbors of the claimer are malicious too and are in the form of a Caravan. Besides, RSS-based approach might be dodged by intelligent malicious attackers.

Yan et al. discussed location information security mechanisms briefly in [16]. The main theme of their research is location integrity, location availability, and location confidentiality. They propose a location-based encryption mechanism by constructing a geolock key which is used to encrypt the outgoing messages. The encrypted messages can be decrypted only in a certain geographic region where the messages are meant for. Nonetheless GPS information is publically available which means that everybody who has access to GPS information can construct geolock key.

We cover two aspects of location security in this work, location confidentiality and location integrity. We eliminate the problems in Yan et al.'s geolock-based mechanism and take another road towards geolock-based approach in VANET. For location integrity we propose a pure cooperative mechanism where neighbors are given weighted based on their trust values.

3. Proposed Scheme

Localization is essential in VANETs. Most of VANET applications, for instance traffic information system, security warning alert etc. depend upon the comprehensive location information. We split our proposed system into two parts namely location confidentiality and location integrity.

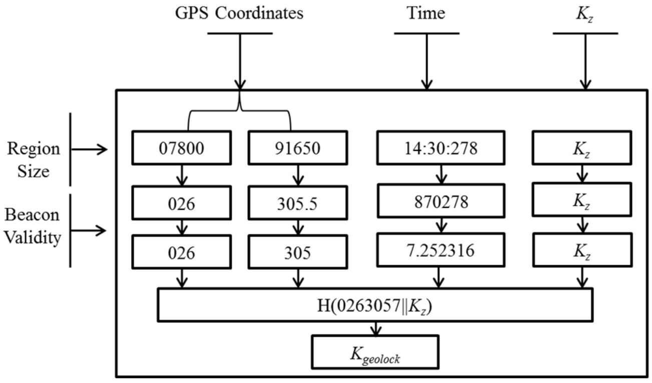

Fig. 1. Geolock key calculation

3.1. Location Confidentiality

VANET exploits the scheduled beacon messages to feed the neighbors' whereabouts information to application and important decisions are made upon that information. Beacon messages contain location, speed, heading, and other information that is essential for VANET application. Usually beacon information is sent in plaintext along with security parameters. Outsiders can misuse the location information in many ways, for instance they can create illusions to launch Sybil attack. In order to prevent outsiders from doing so, location-based encryption scheme was proposed by Yan et al. [16]. Since GPS information is publicly available to everybody provided that a simple GPS device is at disposal, Yan et al. scheme might not work under such realistic assumption. We proposed a geolock-based mechanism where we construct the geolock key ($k_{geolock}$) as shown in Fig. 1 and then encrypt beacon messages with $k_{geolock}$. It is worth noting that we cannot make location information total confidential, but instead we can tweak it in order to keep outsiders from misusing it. Geolock key construction module takes as input, the effective region size, message lifetime and zone key (k_z) and then multiplexes these values altogether in order to calculate hash value from the multiplexed content.

$K_{geolock}= H(location||lifetime||k_z)$

After constructing geolock, outgoing beacon messages are encrypted with $k_{geolock}$. In other words, only one-hop neighbors are able to construct $k_{geolock}$ and decrypt the message. Including message lifetime factor in the geolock will enable stale messages to be non-valid since $k_{geolock}$ cannot be constructed once the valid time is over.

$M = \quad E.K_{geolock}(content)$

Where M is the outgoing message and E denotes encryption function. It is worth noting that the physical boundaries where k_z is effective, must be specified in advance and the scope of these keys must be tradeoff between security and key management.

3.2. Location Verification in Nonline-of-Sight

Since VANET leverages wireless communications among vehicles and other infrastructure, a clear line of sight is essential for successful communication. Many previous schemes leveraged on-board radars in vehicles which were used for object detection and location verification. One of the potential issues with radar is the line of sight. Any obstacle in between source and target would keep the two entities to exchange messages due to the nature of wireless communication. NLoS can be divided into two classes, static NLoS and mobile NLoS. Static NLoS refers to the static obstacle along the road, for instance trees and buildings. Since these objects are known beforehand, certain countermeasures can be taken to remedy NLoS. On the other hand mobile NLoS refers to huge vehicles, for instance trucks and containers moving on the road which blocks the signals from vehicles ahead or behind depending upon the traffic flow. Mobile NLoS can be intentional or un-intentional. We deal with both the cases.

We propose a cooperative mechanism among the vehicles to verify the position of a vehicle who claims to be at certain location. Every vehicle maintains three neighbor tables namely *f-table* (forward table) which contains the neighbors ahead of reference node in one-hop, *b-table* (behind table) which contains the neighbors behind the reference node, and *o-table* (opposite table) which contains the neighbors in the opposite direction. It is worth noting that maintaining neighbor tables has a great conflict of interest with privacy because it is not desired to maintain table with the physical credentials of the vehicles. We propose a privacy-preserved neighbor list mechanism where each neighbor is indexed by $H.K_{V_i}(ELP)$ where K_{V_i} is individual secret key and ELP is unique electronic license plate number. Note that the privacy of neighbors is preserved since K_{V_i} is only known to the vehicle itself and the revocation authority and it is revocable.

3.3. How to check Nonline-of-Sight

In order to check for NLoS, *f-table* should be monitored continuously to check for any inconsistency in the data. For instance an abrupt change in the location, time, or speed would trigger the NLoS function. It is worth noting that a straight highway is easy to handle in case of NLoS because most of the times, with a considerable amount of traffic, the topology does not change rapidly. Hence NLoS can be detected easily. On the other hand, in case of urban scenarios, before triggering NLoS function, the physical road and the lane information of the claimed vehicle must be checked for intersections or splitting roads. A vehicle might not be in the neighborhood anymore since that vehicle changed the road at an intersection. So we believe that the lane information would give us a clear idea of whether NLoS happened or not.

We include the information about NLoS in the beacon message with a bunch of bytes called CCB (Communication Control Bytes). CCB contains the information about NLoS and the claimed vehicle. Since beacons are received by one-hop neighbors and opposite side vehicles, another neighbor who is in direct line of sight of the claimed vehicle will confirm the location of the claimed vehicle. We assign trust values to the neighbors of the NLoS raising node. Trust is directly proportional to the time spend in the neighborhood. The longer the node is in the neighborhood, the larger is the trust value. Trust values ranges from -1 to 1 where -1 means no trust, 0~1 means trustworthy and 0 means neutral. Then this trust values contribute to the weightage. We give more weightage to the opposite side vehicles than the neighbors in the same direction. The main reason is to eliminate the possibility of colluding attacks. We argue that the opposite side vehicles might not be in contact for so long to launch an attack. At the same time, they could verify the position of the claimed vehicles since it is most likely that the node in opposite direction was in the neighborhood of the claimed position just a while ago before coming in contact with the referenced vehicle. At last we calculate confidence value in order to decide whether to trust the verification or not. The confidence value is calculated as follows.

$c= \alpha w_o+\beta w_a+\gamma w_{ob}$

Where $\alpha,$ $\beta,$ and γ are optimization coefficients and w_o is the weightage of the opposite side neighbors, w_a is the weightage of the neighbors ahead in the same direction, and w_{ob} is the weightage of the obstacle. The order of the preference is $\alpha w_o > \beta w_a > \gamma w_{ob}$.

4. Conclusions

In this paper we aim at location confidentiality and location integrity in VANET. For location confidentiality we leverage geolock-based encryption mechanism. In case of Nonline-of-Sight, the location verification becomes challenging. We propose a cooperative mechanism in order to verify the claimed location of a vehicle with the help of other neighbors who have direct line of sight to the claimer. The soundness of location information is based on the trust value of each neighbor and weightage for each neighbor is calculated based on their individual trust value.

References

[1] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z.D. Ma, F. Kargl, A. Kung and J.P. Hubaux, "Secure Vehicular Communication Systems: Design and Architecture," *Ieee Commun Mag*, vol. 46, no. 11, 2008, pp. 100-109.

[2] F. Kargl, P. Papadimitratos, L. Buttyan, M. Muter, E. Schoch, B. Wiedersheim, T. Ta-Vinh, G. Calandriello, A. Held, A. Kung and J.P. Hubaux, "Secure vehicular communication systems: implementation, performance, and research challenges," *Communications Magazine, IEEE*, vol. 46, no. 11, 2008, pp. 110-118; DOI 10.1109/mcom.2008.4689253.

[3] S.D. Gupta, Y.P. Fallah and S.E. Shladover, "Sharing vehicle and infrastructure intelligence for assisted intersection safety," *Proc. Personal Indoor and Mobile Radio Communications (PIMRC), 2011 IEEE 22nd International Symposium on*, 2011, pp. 767-771.

[4] O.K. Tonguz, W. Viriyasitavat and B. Fan, "Modeling urban traffic: A cellular automata approach," *Communications Magazine, IEEE*, vol. 47, no. 5, 2009, pp. 142-150; DOI 10.1109/mcom.2009.4939290.

[5] D. Eckhoff, C. Sommer, R. German and F. Dressler, "Cooperative Awareness at Low Vehicle Densities: How Parked Cars Can Help See through Buildings," *Proc. Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE*, 2011, pp. 1-6.

[6] L. Xiaodong, L. Rongxing, Z. Chenxi, Z. Haojin, H. Pin-Han and S. Xuemin, "Security in vehicular ad hoc networks," *Communications Magazine, IEEE*, vol. 46, no. 4, 2008, pp. 88-95; DOI 10.1109/mcom.2008.4481346.

[7] R. Hussain, S. Kim and H. Oh, "Towards Privacy Aware Pseudonymless Strategy for Avoiding Profile Generation in VANET Information Security Applications," Lecture Notes in Computer Science 5932, H. Youm and M. Yung, eds., Springer Berlin / Heidelberg, 2009, pp. 268-280.

[8] C. Sommer, O.K. Tonguz and F. Dressler, "Adaptive beaconing for delay-sensitive and congestion-aware traffic information systems," *Proc. Vehicular Networking Conference (VNC), 2010 IEEE*, 2010, pp. 1-8.

[9] T. Leinm, #252, ller, E. Schoch, F. Kargl, C. Maih, #246 and fer, "Influence of falsified position data on geographic ad-hoc routing," *Book Influence of falsified position data on geographic ad-hoc routing*, Series Influence of falsified position data on geographic ad-hoc routing, ed., Editor ed.^eds., Springer-Verlag, 2005, pp. 102-112.

[10] M.H. Raya, J.-P., "Securing Vehicular Ad Hoc Networks," *J. Computer Security*, vol. 15, no. 1, 2007, pp. 30.

[11] J. Mittag, F. Thomas, J. Harri and H. Hartenstein, "A comparison of single- and multi-hop beaconing in VANETs," *Proc. VANET'09*, ACM, 2009, pp. 69-78.

[12] T. Leinmuller, E. Schoch and F. Kargl, "POSITION VERIFICATION APPROACHES FOR VEHICULAR AD HOC NETWORKS," *Wireless Communications, IEEE*, vol. 13, no. 5, 2006, pp. 16-21; DOI 10.1109/wc-m.2006.250353.

[13] B. Xiao, B. Yu and C. Gao, "Detection and localization of sybil nodes in VANETs," *Proc. 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks*, ACM, 2006, pp. 1-8.

[14] G. Yan, S. Olariu and M.C. Weigle, "Providing VANET security through active position detection," *Computer Communications*, vol. 31, no. 12, 2008, pp. 2883-2897; DOI 10.1016/j.comcom.2008.01.009.

[15] O. Abumansoor and A. Boukerche, "A Secure Cooperative Approach for Nonline-of-Sight Location Verification in VANET," *Vehicular Technology, IEEE Transactions on*, vol. 61, no. 1, 2012, pp. 275-285; DOI 10.1109/tvt.2011.2174465.

[16] Y. Gongjun, S. Olariu and M. Weigle, "Providing location security in vehicular Ad Hoc networks," *Wireless Communications, IEEE*, vol. 16, no. 6, 2009, pp. 48-55; DOI 10.1109/mwc.2009.5361178.