Providing security in Vehicular ad hoc networks (VANETs) through historical data collection

Dr.Kamal Jamshidi

Department of computer engineering
University of Isfahan
Isfahan, Iran
Jamshidi@eng.ui.ac.ir

Masoud Karimzadeh

Department of computer engineering
University of Isfahan
(Corresponding author)
Karimzadeh@eng.ui.ac.ir

***Abstract*-Today Vehicular Ad-hoc Networks (VANETs) are needful to improve safety on the roads. But using this kind of networks has a few issues. Providing security is one of the most important issues that users of VANETs are associated with. Our purpose of security is the reliability of information. Security is lost when a user or group of users try to send invalid information into the network for their individual purposes. The approach presented in this paper works by the following assumption. One of them is, a unique identifier (called ID) is assigned to each vehicle, and all the communicated messages contain this ID. The approach works by keeping the history of reported messages. By using probabilistic roles, we show that in an unsecure/secure environment how many reports is necessary to rely on a report (message). This reliability helps the driver in making true decisions when he has no information about the message trueness. E.g., message contains the information that an incident (collision, accident and etc) has occurred in a specific place on your way. You may change your way. But you need to ensure the message is true. Our proposed approach is based on this fact that how more an incident is reported it has more probability to be true. In the cases that message validity is not guarantied driver is responsible for trust to received information. At the end, some diagrams show, in different environment, how many reports should be received to rely on a specific report**.

Keywords- VANETs; Security; decision making;

Introduction

VANET was created in October 2002 by the (FCC). The aim of its creation was to improve safety on the roads.

A vehicular ad hoc network is also known as a vehicular sensor network by which driving safety is enhanced through inter-vehicle communications or communications with roadside infrastructure. It is an important element of the intelligent Transportation Systems (ITSs).

In a typical VANET, each vehicle is assumed to have an on-board unit (OBU) and there is road-side units (RSU) installed along the roads. A trusted authority (TA) and maybe some other application servers are installed in the backend. The OBUs and RSUs communicate using the Dedicated Short Range Communications (DSRC) protocol over the wireless channel while the RSUs, TA, and the application servers communicate using a secure fixed network (e.g. the Internet). The basic function of a VANET is to allow arbitrary vehicles to broadcast safety messages (e.g. road condition, traffic accident information) to other nearby vehicles and RSU such that other vehicles may adjust their travelling routes and RSU may inform the traffic control center to adjust traffic lights for avoiding possible traffic congestion. [15]

Problem Statement

Problem arises when one or more users try to inject false information to the network. This information is very important, and has a key role in driver's decision making. A proper decision is the result of proper information, and improper information causes improper decisions. E. g. a vehicle reports heavy traffic on a few miles ahead. But maybe a malicious user wants to cheat others for some selfish aims, e.g., to divert traffic from a given road and thus free it for themselves or for entertainment. In such case it is said that the security of VANETs is affected.

There are many security threats facing vehicular networks. Since we cannot envision all the possible attacks that will be mounted in the future on VANETs, a general classification of attacks substantiated by a list of attacks that we have identified so far is provided in [16]. In this paper there is an approach that can be used against the mentioned problem in this section.

Related works

Using digital signatures is one of the first approaches proposed for establishing security in VANET in 2002 at [6][14]. The base of this approach was to use cryptography to encrypt information.

About the same year an infrastructure for VANET was introduced, and briefly some security problems and related possible solutions have been studied, but the problem of these methods was that a kind of threat was studied and for some of the threats had nothing to say. [5]

In 2004, security architecture for VANET was introduced, this architecture had problems. One of these problems was that like before case a particular type of security attacks can be detected not all of them. Efficiency of this architecture was not significant, because a good architecture should identify all possible types of attacks not only specific types. Someone proposed a PKI (public key infrastructure) and virtual infrastructure based method. This method also had its own problems; like problems caused by overloading, and public and private key should be sent to every vehicle uses this method [3]. In the same year Hubaux, Capkun and Luo in [4], focused on privacy and secure positioning with a different perspective of the VANET. Considerable work they did was the creation of an interaction between responsibility and privacy; they also proposed a unique ID for every vehicle by electronic license plate called ELP. Their proposal, namely the use of fixed ID for each device, is used in this study, and it would be more described a bit later. The topic very relevant to security in VANET is vehicle electronic system security, which has been considered by numbers of researchers. This system actually is responsible for production and transmission of data before sending into the network. To solve this kind of problems, solutions have been proposed too. One example of this system is by the speedometer, A PKI architecture based on the speedometer system in [9] in 2004 was proposed. So in this paper, it is assumed these problems are solved.

Other works was performed in 2004 in the security field that leaded to what in [12] has been noted. Inter-layer information processing can lead to network intrusion detection. For this mean, environment sensors data are compared to the information that is reached from the message, and then if there was an inconsistency the information may be a threat.

A German team in [1] in an article entitled "*intrusion detection in VANET*" with a new approach tried to detect penetration between layers. They help raising VANET security. In this way, GPS, radar or sensors evaluate reasonableness of information received by the network. Target is to compound incidents in different layers of different institutions to detect misuse and influence. [11]

Approach

The method presented in this paper is based on the following assumptions. All the communications inside the network is done with the vehicle identifier. For this mean every vehicle is equipped with an ELP (electronic license plate) that provides a fixed ID for each vehicle, just like [4].

When a message is sent it contains both the information and ID of the sender. Every vehicle has a data base. There is a validity probability for every reported event in the data base. Suppose data base entries are message, sender ID and validity probability for each message, we call it history. The words message and report are used interchangeably. Validity probability for each event has a primary value at first in the data base, when its first report receives. Suppose that an incident, e.g. an accident or road maintenance that causes heavy traffic, has taken place in an area. A vehicle reports this incident and others receive its report. If they trust this report they may decide to change their way, but in other hand the message might be invalid (for example, a malicious user has sent it to change others way). If it is the first time this incident is reported, in other word one vehicle has reported this incident, its validity probability is not enough, but its sender ID and primary probability is saved in data base of both other vehicle and RSU. Trust to this message is not recommended and it can be used just to inform the driver. This case looks like the situation we walk on a street and someone gives you this report that you are facing a danger in the next street, and you know nothing about its authenticity. But when you hear this message more from different people you would decrease your doubt. This will help you in decision making (to keep/change your way). This simple approach helps vehicle in making true decisions on the roads. If different vehicles (with different ID) report the incident, it is more probable that it has happened. So related message validity probability for this message takes a new bigger value in data bases. For each report from different vehicles the probability for this report grows. In other words, if a specific message is reported by more vehicles then it is more reliable. This word is proved by following roles:

Assume the probability of message (report) validity of each vehicle is p, then probability of invalidity is $q = 1 - p$. Suppose n vehicles (where n is number of vehicles) send same message.(In various area, urban, road or highways probability of message trueness of each vehicle is not same). If we suppose $A_i \quad i = 1,2,\dots,n$ event of message validity by the ith vehicle, A_i' is the invalidity event and $P(A_i) = p$, $P(A_i{}') = q$·

Consider B as event of incident occurrence. We are likely to obtain the probability of this event or P (B).

Consider an event has occurred and vehicles want to hide it, independently. Then for lack of any incident, n sender should lie or in other words they send the wrong message. It means the simultaneous occurrence of: $A_1^{'}, A_2^{'},\dots, A_i^{'},\dots, A_n^{'}$ probability of such case is $P(A_1' \cap A_2' \cap \dots \cap A_i' \cap \dots \cap A_n')$.

Then the probability of occurrence the event is $P(B) = 1 - P(A_1' \cap A_2' \cap \dots \cap A_i' \cap \dots \cap A_n')$.

On the other hand we know sending each message is independent from other messages. So according to independent events Theorem we can say:

(If both α and β are independent event then $P(\alpha \cap \beta) = P(\alpha).P(\beta)$)

$$P(A_1' \cap A_2' \cap \dots \cap A_i' \cap \dots \cap A_n') = P(A_1').P(A_2') \dots P(A_i') \dots P(A_n') \quad (1)$$

$$P(A_1' \cap A_2' \cap \dots \cap A_i' \cap \dots \cap A_n') = q.q \dots q = q^n \quad (2)$$

$$\mathit{Then}\ P(B) = 1 - q^n \quad (3)$$

Hence 0≤q≤1 then growth in n causes growth in P (B).

However, depending on the message type, vehicle situation and type of attack to the network attacker (in terms of being active and inactive) efficiency of this approach is not the same in all the applications. In non-life-critical applications such as traffic prevention this approach works properly.

As we have described there is different types of attacks, but treating these attacks requires using different approaches for each kind.

There are two important parameters; q and n. q is the probability of reporting incorrect message by a vehicle. This parameter can be set by driver. Or RSU sets it for every area and sends it to vehicles.

More information can be retrieved from the latter equation (equation (3)). For example, we can obtain needful number of reports for an incident to trust it.

Suppose, report validity probability for an area is 0.1(q = 0.1). Following diagram gives the number reports in horizontal axis, and its related reliability (trueness) (P(B)) in vertical axis.

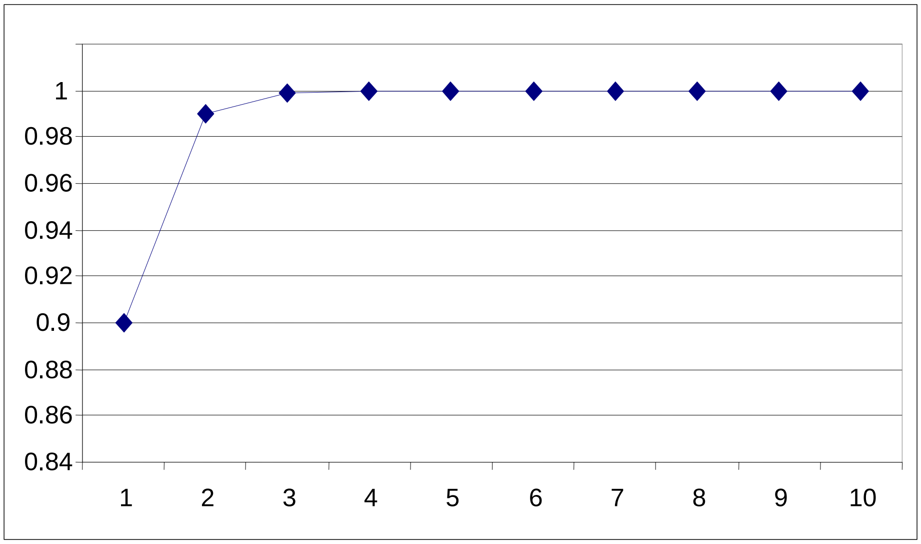


Figure 1. Diagram of probability of different reports in an area with q = 0.1

In this area when one message reports an event the probability of its occurrence is 0.9. The probability of a twice reported message is 0.99. In such area, when an event is reported more than thrice its happening probability is close to one. In other word the report is reliable.

Diagram shown in Figure 2 is for an area with q=0.25.

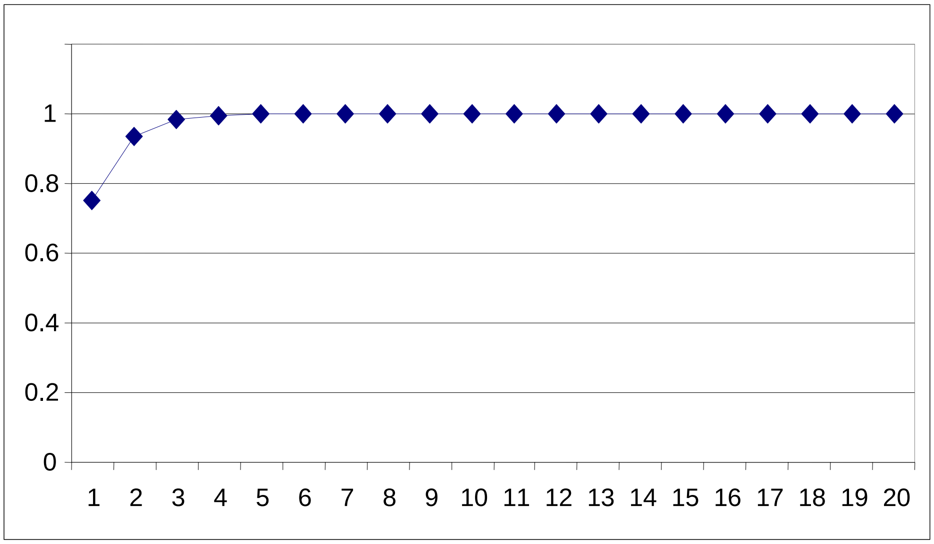


Figure 2. Diagram of probability of different reports in an area with q = 0.25

For one report P (B) =0.75, for two P (B) = 0.9375, for three P (B) = 0.984375 and for bigger number of reports the occurrence probability closes more to one.

For q=0.9 the diagram gives us in such an unreliable area more reports is required to rest on it.

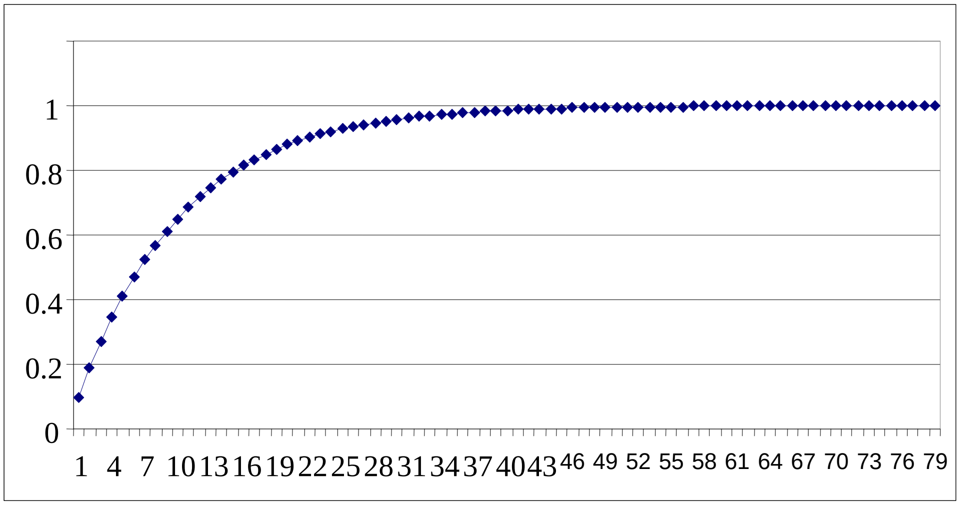


Figure 3. Diagram of probability of different reports in an area with q = 0.9

In this case, 40 reports for an event, it has 0.985219117 of occurrence probability.
Finally for q=0.99 the diagram will be just like figure 4.

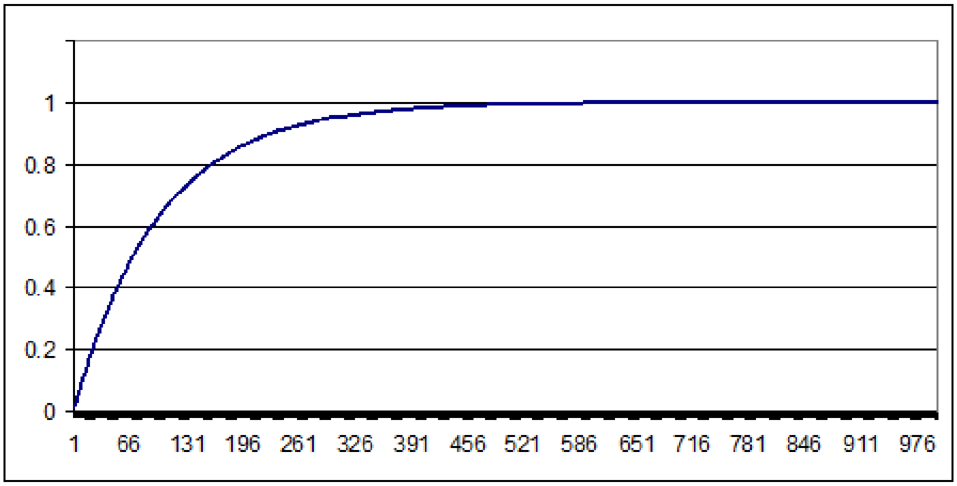


Figure 4. Diagram of probability of different reports in an area with q = 0.99

These shows in various areas different number of reports are needed. This number depends on the area reliability.

This approach is more useful in applications that vehicle drivers have the opportunity and time to colleting reports. For example, in cases like choosing the way in the streets of the city or suburban roads this approach is very responsive

Conclusion

Using this approach gives the VANETs users a proper measure to trust the reports of a specific incident. It can be used in different application in various areas of network. Using it requires a few requirements. All the equipments are fixed on the vehicle and RSU. And only one thing varies in different areas. It is the probability of message trueness of vehicle in each area (q). It is obvious that in area with a large number of vehicles this method is very useful and helps the driver to make true and proper decisions. As another advantage, decision making in this approach is very similar to human’s decision making in daily events. So it looks to be more compatible with his humor. For example If someone informs somebody from a threat or hazard in a place, he might refuse him and cross from danger situation, but if this news is reported by more number of different peoples he comes to trust more. If he changes his way it would be safer.

Reference:

[1] "Vehicular ad-hoc networks" sep.30, 2009 available: http://www.en.wikipedia.org/wiki/vehicular_ad-hoc_networks

[2] Gongjun Yan , Stephan Olariu, Michele C. Weigle "Providing VANET security through active position detection"

[3] J. Blum and A. Eskandarian," The threat of intelligent collisions", IT Professional 6(1) (2004), 24–29

[4] J.-P. Hubaux, S. Capkun and J. Luo, "The security and privacy of smart vehicles", IEEE Security and Privacy Magazine 2(3) (2004), 49–55.

[5] M. El Zarki, S. Mehrotra, G. Tsudik and N. Venkatasubramanianm," Security issues in a future vehicular network", in: Proceedings of European Wireless'02, 2002.

[6] L. Gollan and C. Meinel, " Digital signatures for automobiles", in: Proceedings of Systemics, Cyber-netics and Informatics (SCI)'02, 2002.

[7] S. Duri, M. Gruteser, X. Liu, P. Moskowitz, R. Perez, M. Singh and J.-M. Tang, " Framework for security and privacy in automotive telematics", in: Proceedings of the 2nd International Workshop on Mobile Commerce, 2002, pp. 25–32.

[8] S. Eichler, J. Billion, R. Maier, H.-J. Voegel and R. Kroh," On providing security for an open telematics platform", in: Proceedings of the 5th International Conference on ITS Telecommunications, 2005.

[9] I. Furgel and K. Lemke, A review of the digital tachograph system, in: Proceedings of the Workshop on Embedded Security in Cars (escar)'04, 2004.

[10] Ashwin Rao, Dr. Arzad A Kherani "Security Infrastructure for VANETs" final project abstract, 2006.

[11] Gyanesh Kumar Choudhary ," Providing VANET Security through Position Verification", Master's Project Final Report,2007.

[12] T. Leinm¨ uller, A. Held, G. Sch¨ afer, and A. Wolisz, "Intrusion Detection in VANETs," In proceedings of 12th IEEE International Conference on Network Protocols (ICNP 2004) Student Poster Session, Oct. 2004

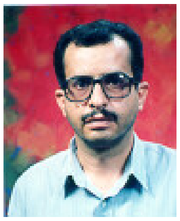
[13] S. Capkun and J.P. Hubaux. "Secure positioning of wireless devices with application to sensor networks" In IEEE INFOCOM, 2005

[14] L. Gollan and C. Meinel," Digital signatures for automobiles", in: Proceedings of Systemics, Cyber-netics and Informatics (SCI)'02, 2002.

[15] Tat Wing Chim, S. M. Yiu , Lucas C. K. Hui, Victor O. K. Li "Security and Privacy Issues for Inter-vehicle Communcations in VANETs" IEEE , (2009)

[16] Maxim Raya and Jean-Pierre Hubaux, "Securing vehicular ad hoc networks" , Journal of Computer Security 15 (2007) 39–68

Author's profile



Dr. Kamal Jamshidi is academic Member of university of Isfahan, Iran

Educational History:

B.E - Electrical Eng. - Isfahan University of Technology, Iran
M.E - Control and Instrumentation - Anna University India.
Ph.D - Fuzzy Control - I.I.T India.

Research Interests:

Wireless sensor networks, Vehicular ad hoc networks, Control and Instrumentation , Microprocessor Based Circuits, PC-Based System

Masoud Karimzadeh, university of Isfahan M.Sc student. He received his B.Sc degree in department of computer engineering, university of Isfahan, Iran.

Research interests:

Wireless sensor networks (WSN), Vehicular ad hoc networks (VANETs), Computer architecture