RESEARCH ARTICLE OPEN ACCESS

A Score Based Trustworthy Declaration Scheme For Vanets

A.Jenifer Sophia
Raja College of engineering and technology, Madurai-625020

Abstract
Vehicles are allowed to generate and broadcast messages about road conditions, such as traffic congestion and accidents to nearby vehicles in Vehicular ad hoc networks (VANETs). These kinds of messages may improve road safety and traffic efficiency of neighboring vehicles. However, messages generated by vehicles may not be reliable. Then propose the secure algorithm through a novel announcement system. The neighboring vehicle utilizes this information within a seconds through the **SHA1- RSA** algorithm and be aware form the road conditions. The reputation system is to find the evaluation of the reliability of the message is based on the digital score which is stored in the server.

I. INTRODUCTION

A vehicular ad hoc network is formed by roadside infrastructure and mobile nodes embedded within vehicles which are connected in a self-organized way. Active research in VANETs is demonstrated by numerous papers in the academic literature VANETs allow vehicles to generate and broadcast messages about road conditions, such as traffic congestion, accidents and road conditions. We call these kinds of messages road-related messages and a scheme that facilitates vehicles to generate and broadcast road-related messages an announcement scheme. Broadcast of road related messages may help vehicles to be aware of the situation ahead of them and, as a result, may provide a safer driving environment. In addition, it also has the capability to improve efficiency of traffic on road networks. However, these benefits can only be realized if the road-related messages generated by vehicles are reliable.

Here say that a message is reliable if it reflects reality. Unreliable messages may result in various consequences, for example journey delays or accidents. Unreliable messages may be the result of vehicle hardware malfunction. For example, if a sensor in a vehicle is faulty then the messages generated based on the information provided by the faulty sensor may be false. Unreliable messages can also be generated intentionally. For example, some vehicles may generate and broadcast false road congestion messages with the intention to deceive other vehicles into avoiding certain routes. In the extreme case, unreliable message may lead to injuries and even deaths. Hence, evaluation of the reliability of vehicle-generated Messages is of importance in VANETs.

In a large VANET environment, vehicles are assumed to have a weak trust relationship with each other. Vehicles decide whether to rely on a message. Here address this problem by proposing a novel reputation based announcement scheme for VANETs. The reliability of a message is evaluated according to the reputation of the vehicle that generates this message. A message is considered reliable provided that the vehicle that generates the message has a sufficiently high reputation. The reputation of a vehicle is represented by a numerical score. This reflects the extent to which the vehicle has announced reliable messages in the past. It is computed based on feedback reported by other vehicles. Feedback contains a numerical score representing the feedback reporting vehicle's evaluation of the reliability of the message. The score is collected, updated and certified by a trusted party. The reputation score evolves, as time elapses, based on the reliability of messages that the vehicle announces. Vehicles tend to give positive feedback for reliable messages. This increases the reputation score. Meanwhile, a reputation score decreases when negative feedback is reported.

II. SYSTEM DESCRIPTION

In Existing system, Opinion Piggybacking, Role-Based trust, Majority-Based trust mechanism are used to find the reliability.

A) OPINION PIGGYBACKING

A vehicle generates a message and broadcasts it to neighbouring vehicles. A receiving vehicle will append its own opinion about the reliability of the message, which may be based on the content of the message or the aggregated opinions already appended to the message. Upon receiving a message, a vehicle is required to compute and aggregate previous opinions appended to the message before it decides and generates its own opinion. This may create a computational burden on receiving vehicles.

B) ROLE-BASED TRUST

Rolebased trust exploits certain predefined roles that are enabled through the identification of vehicles. For example, vehicles may have more trust towards traffic patrol or law enforcing authorities compared to other vehicles. To avoid impersonation attacks, each vehicle is required to possess a certificate that includes its name, role and public key, issued by a trusted authority for authentication purposes.

C) EXPERIENCE BASED TRUST

Experience based trust is established based on direct interactions: a vehicle determines who to trust based on how truthful they have been in their past interactions it also requires vehicles to store information regarding vehicles that they have encountered in the past.

III. PROPOSED SCHEME

KEY REPUTATION CERTIFICATE RETRIEVAL:

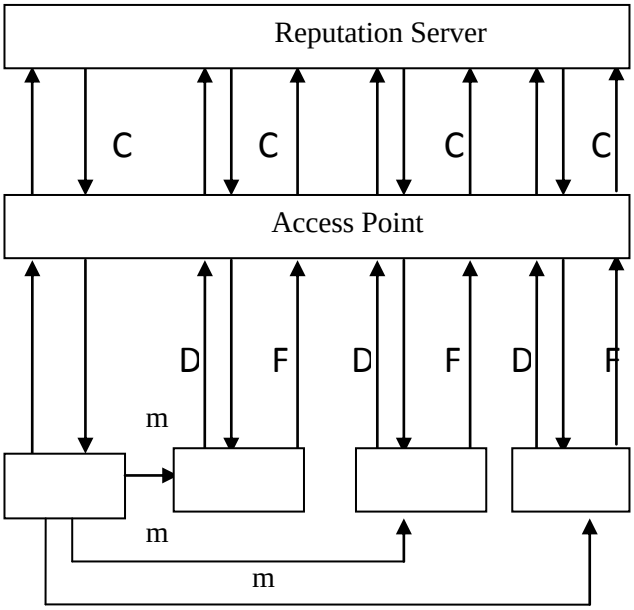
In this phase, a vehicle retrieves its latest reputation certificate from the reputation server. When a vehicle Vb drives into wireless communication range of an access point, it retrieves its own reputation certificate from the central server via the access point as follows:

Vb sends its identity idVb to the server via the access point. The reputation server generates a reputation certificate *C* for the vehicle, where:

C = (idVb , pkVb , tc, rsVb ,□);

In which *tc* denotes the time when *C* is generated and it is obtained from the reputation server's clock, rsVb denotes the reputation score of Vb at time tc, and □ **= Sign1(idVb , pkVb , tc, rsVb)skS** denotes a digital signature using the algorithm(SHA1withRSA) Sign1 and private key skS on (idVb , pkVb ,tc, rsVb).

The reputation server sends *C* to Vb via the access point. Once Vb obtains C, it stores the reputation certificate locally. Previously obtained reputation certificates can then be deleted.



Message Broadcast:

Here Vb generates a road-related message and broadcasts it to its neighboring vehicles. This is described as follows:

The trusted hardware retrieves the current time tb from its embedded clock and generates a time stamped signature Ø, where

Ø=Sign2(tb,H(m))skVb

and Vb outputs tb and Ø. Vb forms a message tuple M, where:

M = (m, tb, Ø, C);

and Vb broadcasts M to its neighboring vehicles.

Message Reliability Evaluation:

Upon receiving the message tuple

M = (m, tb, Ø, C),

a receiving vehicle Vr performs the following procedure:

Vr checks:

Whether σ ε C is valid, by using the verification algorithm Verify1 and the public key of the reputation server pkS

If all checks are positive, then vehicle Vb is considered to be reputable. Message m is thus considered as reliable.

Feedback Reporting:

When vehicle Vr has its own experience about the event that the message m describes, it is able to judge the reliability of the message. Then if Vr wants to report feedback to the reputation server, it performs the following procedure.

The trusted hardware retrieves tr from the tuple (tr, Ø) that was previously stored during the message reliability evaluation phase, computes a message authentication code (MAC) value δ, where:

□ **= MAC(idVb , idVr , fr , tb, tr,H(m), Ø)mkVr ;** and the trusted hardware then outputs tr and δ.

Vr forms a feedback tuple F, where:

F = (idVb , idVr , fr ,tb, tr,H(m), Ø, □):

We say that F is positive feedback if fr = 1 and negative feedback if fr = 0.

Reputation Update:

The reputation server updates the reputation score rsVb of vehicle Vb on receipt of a feedback tuple

F = (idVb , idVr , fr , tb, tr,H(m), Ø, □)

IV. ALGORITHAM

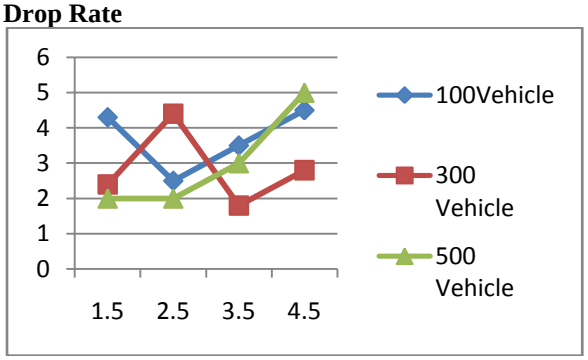
The hash-value is calculated from the concatenation of the following information:

- L(Modulus),V(Modulus),L(Exponent),V(Exponent) where
- L(x) is the length of x in bits and
- V(x) is the value of x as an array of bytes, high byte first If the length of one element is less than or equal to 127, the length-value L(x) is exactly one byte with the length as value.

V. EVALUATION

The density of vehicles also impacts on the message drop rate. We observe a decrease of message drop rate when the density of vehicles increases. A modest but noticeable decrease is seen when the density of vehicles

Drop Rate



Increases from 100 to 500 vehicles in the selected road network of ten square kilometres. This is reasonable because more feedback tends to be reported for a vehicle
in a vehicle-dense road network.

VI. CONCLUSION

Here present a novel reputation-based announcement scheme for VANETs in order to evaluate message reliability. In the current scheme a vehicle and its human driver are represented by a single entity. It might be of interest to extend our scheme to reflect the potentially different reputations of human drivers and vehicles separately. In the current scheme a message broadcast by a vehicle is only utilized by its neighboring vehicles.

REFERENCES

[1] Golle, P., Greene, D.H., Staddon, J.: Detecting andcorrecting malicious data in VANETs. In: Proceedingsof the 1st ACM International Workshop on Vehicular Ad Hoc Networks, ACM (2004)

[2] Hubaux, J., Capkun, S., Luo, J.: The security and privacy of smart vehicles. IEEE Security & Privacy**2**(3) (2004)

[3] Hubaux, J., Papadimitratos, P., Raya, M.: Securing vehicular communications. IEEE Wireless Communications Magazine **13**(5) (2005)

[4] D¨otzer, F., Fischer, L., Magiera, P.: VARS: A vehicle ad hoc network reputation system. In: Proceedingsof the Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks. Volume 1. (2005)

[5] Patwardhan, A., Joshi, A., Finin, T., Yesha, Y.: A data intensive reputation management scheme for vehicular ad hoc networks. In: Proceedings of the 3rd Annual International Conference on Mobile and Ubiquitous Systems. (2006)

[6] Daza, V., Domingo-Ferrer, J., Seb´e, F., Viejo, A.: Trustworthy privacy-preserving car generated announcements in vehicular ad hoc networks. IEEE Transaction on Vehicular Technology **58**(4) (2009)

[7] Domingo-Ferrer, J., Wu, Q.: Safety and privacy in vehicular communications. In: Privacy in Locationbased Applications. Volume 5599 of LNCS. (2009)

[8] Raya, M., Papadimitratos, P., Gligor, V., Hubaux, J.:On data-centric trust establishment in ephemeral ad hoc networks. In: INFOCOM, IEEE (2008)

[9] Schmidt, R., Leinm¨ uller, T., Schoch, E., Held, A.,Sch¨afer, G.: Vehicle behavior analysis to enhance security in VANETs. In: Proceedings of 4th Workshop on Vehicle to Vehicle Communications (V2VCOM). (2008)

[10] Wu, Q., Domingo-Ferrer, J., Gonz´alez-Nicol´as, U.:Balanced trustworthiness, safety, and privacy in vehicle-to-vehicle communications. IEEE Transactions on Vehicular Technology **59**(2) (2010)

[11] C2CC: The Car-to-Car Communication Consortium. (2011) http://www.car-to-car.org.

[12] Chen, L., Ng, S., Wang, G.: Threshold anonymous announcement in vanets. IEEE Journal on Selected Areas in Communications **29**(3) (2011)