International Journal of Information Technology and Knowledge Management
January-June 2011, Volume 4, No. 1, pp. 125-128

SECURITY AND PRIVACY PRESERVATION IN VANET

Yogesh A. Suryawanshi[1] & Avichal Kapur[2]

Initiatives to create safer and more efficient driving conditions have recently begun to draw strong support. Vehicular communications (VC) will play a central role in this effort, enabling a variety of applications for safety, traffic efficiency, driver assistance and infotainment. Security and privacy are indispensable in vehicular communications for successful acceptance and deployment of such a technology. Generally, attacks cause anomalies to the network functionality. A secure VANET system, while exchanging information should protect the system against unauthorized message injection, message alteration. In this paper, various security and privacy issues are discussed and try to solve it with effective cryptosystem.

1. INTRODUCTION

Vehicular networking protocols will allow nodes, that is, vehicles or road-side infrastructure units to communicate with each other over single or multiple hops; providing each other with information such as safety warnings and traffic information. As a cooperative approach, vehicular communication systems can be more effective in avoiding accidents and traffic congestions than if each vehicle tries to solve these problems individually. The network should support both private data communications and public (mainly safety) communications.

According to World Health Organizations (WHO), road accidents annually cause approximately 1.2 million deaths worldwide; one fourth of all deaths caused by injury. Also about 50 million persons are injured in traffic accidents. If preventive measures not been taken, road death is likely to become the third-leading cause of death in 2020 from ninth place in 1990.US Department of Transport states that 21,000 of the annual 43,000 road accident deaths in the US are caused by roadway departures and intersection-related incidents. This number can be significantly lowered by deploying local warning systems through vehicular communications. Departing vehicles can inform other vehicles that they intend to depart the highway and arriving cars at intersections can send warning messages to other cars traversing that intersection. Studies show that in Western Europe a mere 5 km/hr decrease in average vehicle speeds could result in 25% decrease in deaths.

The attractive features of VANETs inevitably incur higher risks if such networks do not take security into account prior to deployment. For instance, if the safety messages are modified, discarded, or delayed either intentionally or due to hardware malfunctioning, serious consequences such as injuries and even deaths may occur.

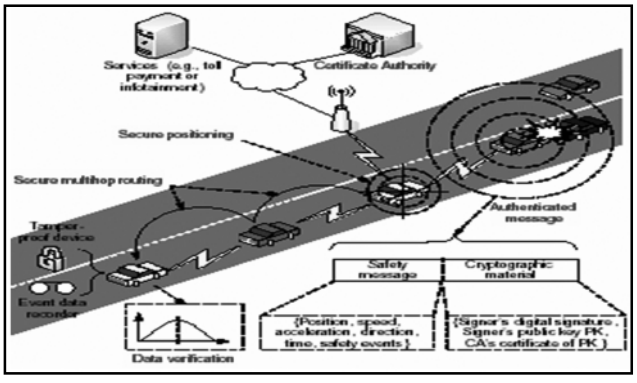

Fig. 1: Overview of the Security Architecture

1.1. Challeges in Vanet

It is essential to make sure that life-critical information not be inserted or modified by an attacker; likewise, the system should be able to help establishing the liability of drivers; but at the same time, it should protect as far as possible the privacy of the drivers & also the size of the network, the speed of the vehicles, the relevance of their geographic position, the very sporadic connectivity between them and the unavoidably slow deployment make the problem very novel and challenging.

1.2. Securing Vehicular Communications Require

- Authentication and integrity: to prevent message modification and forgery.
- Non-repudiation: to prevent nodes from denying transmission of a message.

[1]Research scholars, In Electronics Engineering, Y.C.C.E, R.T.M Nagpur University, Nagpur, India

[2]Dean (Quality Assurance) & Advisor, MGI Group, N.Y.S.S., Nagpur, Maharastra, India

Email: [1]yogesh_surya8@rediffmail.com

- Privacy: to prevent the collection or extraction of private information from vehicular communications.

2. DIGITAL SIGNATURES AS A BUILDING BLOCK

Message legitimacy is mandatory to protect VANETs from outsiders as well as misbehaving insiders. The simplest and the most efficient method is to assign to each vehicle a set of public/private key pairs that will allow the vehicle to digitally sign messages and thus authenticate itself to receivers.

$$V \rightarrow \quad : M, SigPrKV [M|T], CertV$$

Where V designates the sending vehicle, represents all the message receivers, M is the message, | is the concatenation operator and T is the timestamp to ensure message freshness. CertV is the public key certificate of V. The receivers of the message have to extract and verify the public key of V using the certificate and then verify V 's signature using its certified public key. In order to do this, the receiver should have the public key of the CA. If the message is sent in an emergency context, which means that it belongs to the liability-related class, this message should be stored (including the signature and the certificate) in the EDR for further potential investigations in the emergency.

2.1. Alternative Authentication Mechanisms

Raya and Hubaux suggested a security and privacy scheme based on digital signatures under the PKI. Each vehicle will be assigned a set of public/private key pairs. Each message sent will contain a digital signature and a corresponding certificate. Thus, the resulting total message might be three times the original message. Therefore we have considered several options to reduce this overhead notably relying on the establishment of symmetric keys.

2.1.1. Pairwise Keys

It is common practice in networks that two nodes establish a shared session key if they need to securely communicate for a long time. In fact, symmetric cryptographic primitives are much more efficient (in terms of time and space overhead) than the asymmetric ones.

We have considered the typical scenario of two vehicles A and B happening to remain in power range of each other for a while and that decide to establish a session key. One of the vehicles A sends the session key K to B encrypted with B's public key:

$$A \rightarrow B: \{B|K|T\}\ PuKB, SigPrKA [B|K|T]$$

Subsequent message exchanges can use Hashed Message Authentication Codes (HMAC) with the key

$$A \rightarrow B: m, HMACK (m)$$

With this approach we can provide only authentication but not secure transmission as well as privacy of user. The problem with this approach is, global attacker can extract information if a key is reused even on different days.

2.1.2. Anonymous Key Set Size

Anonymous key pairs that are used to preserve privacy as well as security. An anonymous key pair is a public/private key pair that is authenticated by the CA but contains neither information about nor public relationship with (i.e., this relationship cannot be discovered by an observer without a special authorization) the actual identity of the vehicle (i.e., its ELP). Yet this anonymity is conditional for liability purposes. Normally, a vehicle will possess a set of anonymous keys to prevent tracking.

A vehicle should change its anonymous key only after having used it for a certain number of messages. For example, a vehicle should change its key within an interval of around 1 min. If we assume that an average driver uses his car 2 hours per day, the number of required keys per year is approximately 43 800, which amounts to around 4.2Mbytes (assuming a storage space of 100 bytes per key, including its certificate).

The major problem associated with traditional digital signature schemes are that in order to ensure privacy, the vehicles would have to store a very large number of public/private key pairs and keys must be changed often. Secure distribution of keys, key management and storage are very difficult in this type of scheme.

To reduce the key storage space for governmental transportation authorities, anonymous keys can be derived from a master key shared between an authority and the vehicle corresponding to the keys. When verifying vehicle identities in liability-related situations, the keys can be regenerated using the master key.

3. SECURITY ANALYSIS

Compliance with the security requirements: Authentication of messages is provided by the digital signature of the sender and the corresponding CA certificate. The only guarantee that this provides is that the message comes from a vehicle that was trusted, at least when the keys were issued. Nevertheless, these mechanisms ensure that outsiders are not able to send messages to network members.

Non-repudiation is achieved as follows:

- Vehicles cannot claim to be other vehicles (masquerade attack) since all the messages they transmit are signed by their (anonymous) public keys. ELPs cannot be forged because they are unique and verifiable.

- A vehicle cannot deny having sent a message because it is signed by an anonymous key that belongs exclusively to the sender; likewise, the vehicle cannot claim that the message was replayed because a timestamp is included in each message.

3.1. Anonymity

In order to preserve the driver's anonymity and minimize the storage costs of public keys, we propose a key changing algorithm that adapts to the vehicle speed and takes into account key correlation by the attacker as described below. Let us consider the typical tracking scenario where the attacker controls stationary base stations separated by a distance datt and captures all the received safety messages;

Attaker can later use these data (including the public keys) to illegally track vehicles. In addition, we assume that the attacker can correlate two keys if the sender moves at a constant speed in the same direction and on the same lane between two observation points (e.g., given the initial position of the target the attacker can predict its position in the future and confirm this prediction if a message is received at the next observation point with correct predicted speed and position). Assume the speed of target V is vt, its transmission range is dr, and dv is the distance over which a vehicle does not change its speed and lane (the vulnerability window with respect to the correlation of keys). As Fig. 2 illustrates, the vehicle's anonymity is vulnerable over a distance equal to dv + 2dr. This means that it is not worth changing the key over smaller distances because an observer can correlate keys with high probability. This defines the lower bound on the key changing interval Tkey:

$$\min(Tkey) = dv + 2dr/vt \text{ seconds} \quad (1)$$

But if datt > dv+2dr, V can avoid being tracked (by changing its key) as long as it does not use the same key for a distance equal to or longer than datt. This in turn defines the upper bound on the key changing interval:

$$\max(Tkey) = datt / vt \text{ seconds} \quad (2)$$

Since V does not know datt, but knows dr and dv, it can choose a value of Tkey that is a little larger than min(Tkey).

If we denote by rm the message rate, one key should be used for at most:

$$Nmsg = [rm \times Tkey] \text{messages} \quad (3)$$

For example, assume datt = 2 km, rm = 3.33 msg/sec (1 message every 300 ms), dv = 30 sec × vt (i.e., V does not change its lane and speed over 30 sec), dr = 10 sec ×vt (according to DSRC, the transmission range is equal to the distance travelled in 10sec at the current speed), and vt = 100 km/h.

Then min(Tkey) = 50 seconds and max(Tkey) = 72 seconds. V can choose Tkey to be 55 seconds; as a result, Nmsg = 184 messages.

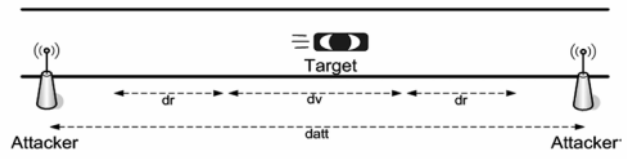

Fig. 2: To Uncover the Identity of its Targets, the Attacker Leverages on Key Correlation and the Target's Transmission Range

3.2. Estimation of the Signature Size

As we propose using a PKI for supporting security in VANETs, it is important to choose a Public Key Cryptosystem (PKCS) with an acceptable implementation overhead in the vehicular context. According to DSRC, safety-related messages are sent with a periodicity of 100 to 300 ms, given that in DSRC the minimal data rate is 6 Mbps.

This imposes an upper bound on the processing time overhead; this overhead is given as follows:

$$Toh(M) = Tsign(M) + Ttx(M|SigPrKV [M]) + Tverify(M)$$

where Tsign(M), Ttx(M), and Tverify(M) are the necessary durations to sign, transmit, and verify a message M, respectively; SigPrKV [M] is the signature of M by the sending vehicle V and includes the CA's certificate of the signing key. The above expression reveals the two factors that affect the choice of a particular PKCS: (1) the execution speeds of the signature generation and the verification operations, and (2) the key, signature, and certificate sizes.

Is Public Key Cryptography Fit?

A typical criticism of public key cryptography in wireless networks is that its overhead seriously affects the performance of the system. Each message will contain a digital signature and a corre-sponding certificate. We assume the safety message size (not considering cryp- tographic material) to be around 200 bytes, including all overheads. The resulting total message size (safety message plus a digital signature plus a certificate, which contains a public key and a signature) is between 284 and 791 bytes. The second figure may be surprising at first, as the security overhead is almost 3 times the message size.

3.3. Numerical Upper Bounds

We consider two scenarios (we assume upper bounds on all values) The channel capacity is typically 12 Mbps for safety messages with a minimum of 6 Mbps.

1. A highway with 6 lanes (3 in each direction) of 3m each. We assume a uniform presence of vehicles, with an inter-vehicle space of 30 m. Vehicles are mobile and transmit DSRC messages every 300 ms over a 300 m communication range. We consider a vehicle V located in the middle of the highway, which corresponds to a maximum of received messages; V can hear 120 vehicles per 300 ms. In the worst-case, where all vehicles contend for the channel, the system throughput is 2.53 Mbps (120 veh × 3.33 msg×sec/veh × 791 bytes/msg), to be compared with the minimum nominal capacity of DSRC, which is 6 Mbps. Before V can send a new message, it should be able to process all incoming messages within 300 ms. Assuming V receives all the 120 messages, the maximum tolerable processing delay per message is 300 ms/ 120 = 2.5 ms.

2. We consider the same highway as in the previous case but this time vehicles are very slow or stopped (congestion scenario) and spaced by 5 m (including the vehicle length). Each vehicle transmits a safety message over a range of 15 m every 100 ms. In this case, a vehicle V can hear at most 36 other vehicles per 100 ms, which amounts to a throughput of 2.28 Mbps (36 veh × 10 msg×sec/ veh × 791 bytes/msg), which is also smaller than the minimum 6 Mbps. The upper bound on the processing delay per message, assuming V receives all the messages, is 100 ms/36 = 2.78 ms.

4. CONCLUSION

In this paper, we have explained why vehicular networks need to be secured, and why this problem requires a specific approach. We have proposed a model that identifies the most relevant communication aspects; we have also identified the major threats. We have then proposed security architecture along with the related protocols; we have shown how and to what extent it protects privacy. We have shown that public key cryptography is fit for the considered problem.

To our best knowledge, this is the first paper addressing the security of vehicular networks in a systematic and quantified way.

In terms of future work, we intend to further develop this proposal with the help of modified cryptosystem.

REFERENCES

[1] Jeremy Blum and Azim Eskandarian, "The Threat of Intelligent Collisions", IT Professional, 6(1), 24–29, Jan.-Feb. 2004.

[2] Michael Brown, Darrel Hankerson, Julio L´opez, and Alfred Menezes, "Software Implementation of the NIST Elliptic Curves Over Prime Fields", Lecture Notes in Computer Science, 2020:250–265, 2001.

[3] S. Capkun and J.P. Hubaux, "Secure Positioning of Wireless Devices with Application to Sensor Networks", In IEEE INFOCOM, 2005.

[4] Sastry Duri, Marco Gruteser, Xuan Liu, Paul Moskowitz, Ronald Perez, Moninder Singh, and Jung-Mu Tang, "Framework for Security and Privacy in Automotive Telematics", In Proceedings of the 2nd International Workshop on Mobile Commerce, Pages 25–32, ACM Press, 2002.

[5] Stephan Eichler, Jerome Billion, Robert Maier, Hans-Jrg Vgel, and Rainer Kroh, "On Providing Security for an Open Telematics Platform", In 5th International Conference on ITS Telecommunications, 2005.

[6] Per Enge, "Retooling the Global Positioning System", Scientific American, May 2004.

[7] Wilfried Enkelmann, "FleetNet-applications for Inter-vehicle Communication", In IEEE Intelligent Vehicles Symposium, Pages 162–167, June 2003.

[8] Igor Furgel and Kerstin Lemke, "A Review of the Digital Tachograph System", In Workshop on Embedded IT-Security in Cars (escar), 2004.

[9] Lutz Gollan and Christoph Meinel, "Digital Signatures for Automobiles", In Systemics, Cybernetics and Informatics (SCI), 2002.