Scientiae Mathematicae Japonicae

AN INTELLIGENT MESSAGE AUTHENTICATION SCHEME FOR EMERGENCY AND SAFETY RELATED MESSAGES IN A VEHICULAR NETWORK

Prakash Veeraraghavan and Dalal Hanna
Department of Computer Science and Information Technology
La Trobe University, Victoria 3086, Australia

Abstract. Road safety and traffic efficiency are two important applications of a Vehicular Ad-hoc Network (VANET). In VANET, safety and emergency messages are broadcasted to all vehicles in a risk zone before the validity of the message expires. Emergency and safety-related communications have a very strict real-time requirement of 100ms latency from an originating host's application layer to destination host's application layer and a Packet Delivery Ratio (PDR) of 90% and above. Due to one-to-many nature of these emergency messages, public-key encryptions may not be employed. Furthermore, vehicles on the road have no constant access to the Roadside infrastructure. Thus, access to a Public-key Infrastructure or a Certificate Authority is not always guaranteed. Exploiting this weakness, any attacker with malicious intention can broadcast falsified emergency messages with spoofed identity to disrupt the normal operation. They may also do in order to launch a terror-like attack. Since the identity of the originating malicious vehicle cannot be established, it is not possible to take any legal action against the owner of these vehicles.

In this paper, we propose a smart digital certificate mechanism using a modified threshold cryptography scheme, that we call it as a pseudo-identity based encryption to identify the origin of every emergency message. Since the keys are not forgeable, any such malicious activities are immediately known to the receiving host vehicles and vehicle registration authorities, thus facilitating legal action. The main advantage of our proposed scheme is that it can work without constant access to a Public-key Infrastructure or a Certificate Authority. Our scheme satisfies the identical security requirements as that of the underlying public-key cryptography and incurs the same memory and run-time complexity.

The proposed scheme can also be implemented in a Mobile Ad hoc environment or a distributed environment, where source authentication is an important factor, and there is no constant access to the backbone of the network.

1 Introduction In this paper, we demonstrate a class of attack on the emergency and safety message transmission in a *Vehicular Ad hoc network* (*VANET*), by exploiting the integrity and the authentication of the message transmission. Due to real-time requirements, the current state-of-art in a vehicular network does not offer any solution to this problem. In this paper, we introduce a mathematical framework that we call as a *Pseudo-identity based encryption* that can potentially offer an efficient solution to the demonstrated attack without incurring many overheads.

An ad hoc network is a new paradigm of wireless communication for mobile nodes. It has two special characteristics, which make it different from the conventional wired network. First, there is no fixed infrastructure like a wired or a cellular phone network. There are no base stations, switching centers or routers to route packets to destinations. Secondly,

in an ad hoc network, the network topology is not fixed due to the mobility of nodes. In ad hoc networks, nodes that are in the same radio range of each other communicates directly in a peer-to-peer fashion. However, nodes that are not in the same radio range may still communicate through the help of intermediate nodes. In this case, intermediate nodes act as routers to establish a multihop communication. Thus in a mobile ad hoc network (*MANET*), a node may act as a router as well as an end-node. Depending on the application environment a mobile node may have more than one role to play apart from acting as a router and an end node. Even though these networks were originally developed for military tactical applications, due to the reduction in the cost of wireless transceivers, hardware and the increase in the popularity of ubiquitous applications, ad hoc networks are deployed everywhere from a small home, video games to a battle field.

Vehicular Ad hoc Network (*VANET*) is a special type of a Mobile Ad Hoc Network (MANET), where the mobile hosts are the vehicles on the road. They communicate with each other wirelessly to establish a network. Although, passenger (and driver) safety technologies such as airbags, seat belts and anti-skid brakes are available, the deaths due to road accidents have not come down. At this moment, road traffic fatalities are the 8th leading cause of death globally, and the leading cause of death for young people aged between 15 and 29 [1]. If no action is taken to address the current crisis, global road traffic fatalities are forecasted to rise to more than 2.4 million deaths per annum by 2030 [7]. In order to reduce the number of fatalities and serious injuries, expensive sensors, radars, cameras and other state-of-art technologies are currently integrated into vehicles. These devices communicate with neighbouring vehicles in an ad hoc fashion when it detects an abnormal situation like an accident, slippery road conditions or any other noticeable hazard.

Dedicated Short-Range Communication (*DSRC*) refers to the use of *Vehicle-to-Vehicle* (*V2V*) and *Vehicle-to-Infrastructure* (*V2I*) communication that was designed to improve road safety and transportation efficiency. DSRC supports several applications. Among them, *Cooperative Collision Avoidance* (*CCA*) is the most important one. In DSRC, V2V communications are established through the use of VANET. VANETs use on-road vehicles as nodes to create an ad hoc network. DSRC supported applications can be classified into three major classes. They are: Safety-related applications, Non-safety-related applications and Infotainment. Speed management and Cooperative navigation are two examples of non-safety applications. Tourist and Traveller Information Support, Streaming music are two examples of Infotainment. These two classes of applications require communication infrastructure such as Roadside Unit (RSU). The motivation for allowing non-safety applications over DSRC is to create commercial opportunities, thereby, making the DSRC technology more cost-effective.

Road safety is not the only road issue. Traffic efficiency is another major issue, especially in metropolitan areas all around the world. The cost of the time spent sitting in traffic has been estimated at $11.1 billion, annually [6]. This figure does not include the cost of the fuel burned waiting for traffic to move, the cost to the environment or the flow-on costs to the nation's health system. Particularly in Australia, statistics show that the cost of congestion was $9.4 billion in 2005, and the social costs of congestion are forecasted to reach $20.4 billion by 2020 [3]. These figures and statistics indicate that the need for a significant reduction in both traffic congestion and vehicle crashes is a serious challenge throughout the world.

In VANET, safety messages are broadcasted to all vehicles in a risk zone before the validity of the message expires. A risk zone is the area in which the content of a specific

safety message is relevant to all vehicles. The size of the risk zones varies depending upon the requirements of different safety applications. The risk zone of a particular application might be much larger than the one-hop transmission range of the source node. As a result, multi防op broadcasting is required for vehicles in the risk zone which are not in the one-hop transmission range of the source node. Thus a vehicle receiving a multi-hop safety message needs to rebroadcast before the expiry of its lifetime. The Time-to-live (TTL) value is the number of hops the emergency message is valid before it is discarded. The source or the originating vehicle of an emergency message sets the TTL value. Every vehicle that receives an emergency message reduces this value by one before the message is rebroadcasted. A vehicle that receives an emergency message with a TTL-value 1 will not rebroadcast the message.

Vehicle-to-Vehicle (V2V) safety communication has a very strict real-time requirement of 100ms latency from source host's application-layer to a destination host's application-layer, and a Packet Delivery Ratio (PDR) of at least 90% [12]. Most of the safety messages in a vehicular network are applicable to a region (or a smaller neighbourhood like accident zone), rather than to another individual vehicle. Thus, broadcasting is the most efficient way of disseminating emergency messages. Due to this real-time requirement, heavy cryptography mechanisms are not employed. Furthermore, due to one-to-many nature of the safety messages, the use of any encryption is not preferred. Whenever a vehicle received a safety message from another vehicle, it is impossible to identify the source and the authenticity of the message. To verify the identity of the source vehicle, digital signature may be used. However, without access to a Public-Key Infrastructure (PKI) or a local trusted Certificate Authority (CA); it is impossible to verify a digital signature. In a vehicular communication, we cannot always assume that a vehicle has access to a Roadside Unit (RSU) to obtain the public-key information. We exploit this weakness in this paper to demonstrate a message falsification attack. This is presented in Section 2. In Section 3, we define a pseudo-identity based encryption scheme based on Shamir's threshold cryptography [10]. Based on the proposed scheme, the identity of the transmitting vehicle can immediately be identified even if there is no access to a RSU or CA or PKI. In Section 4, we present our solution architecture to solve the message falsification attack presented in Section 2. In Section 5, we present the concluding remarks and future direction.

The readers are referred to Hartenstein and Laberteaux [5] for more fundamental details on VANET.

2 Message Falsification attack In this section, we explain how a malicious vehicle can exploit the absence of a safety message authentication to launch a message falsification attack. Traditional security threats in wireless communication, such as eavesdropping, forgery, and modification, could be easily taken advantage of in VANETs [13]. In order for the CCA to work effectively, all vehicles in the road network must trust each other and are able to trust the alerts and warnings issued by V2V devices working with messages from other V2V devices. This is a major assumption and can be exploited to launch an attack.

Any vehicle that detects a road-safety concern will immediately broadcast an emergency message. The message will contain information about the specific condition. All vehicles that receive this safety message must process them and take appropriate action. If the message is applicable to a multi-hop environment, the receiving vehicle must rebroadcast the safety message.

Let T be a vehicle with a modified DSRC protocol stack. It is capable of sending forged

Figure 1: [12]

emergency messages using falsified vehicle identification. Since DSRC use the traditional 802.11 wireless spectrum, the vehicle may also be equipped with one or more mobile wireless devices capable of sending forged emergency messages. Even though the DSRC standard dictate the amount of transmission power to be used in broadcasting emergency messages, T may violate this standard and transmit these forged messages at a much higher power level to reach a larger region. T may transmit a variety of safety-critical messages such as accident, road closure, severe congestion-ahead etc. to divert the vehicles behind through an alternative congested route. Even though T may not gain any financial advantage through this attack, he may disrupt the legitimate DSRC services to launch a *Denial of Service* (*DoS*) attack. In a worst case scenario, the aides of T may launch a terror like attack on the congested road.

In the following subsection, we simulate an emergency communication in a vehicular network and demonstrate how important is the central region surrounding an emergency zone (like an accident, or the eye of a congestion).

2.1 Communication overhead in a Central region In our simulation, we follow the DSRC standard that every vehicle's transmitter has the same transmission range as that of other vehicles in the network (typically 300m). In the literature, vehicles on the roads are modeled as an *Interval graph* [5]. However, we note that this modeling is valid only for single lane traffic. In typical multilane freeway traffic, vehicles are located in an $n \times m$ rectangle. Since each vehicle has the same transmission distance, without loss of generality, we assume that all the vehicles have the unit transmission distance. If the distance between two vehicles is less than one, we join them by an edge. Thus, it is easy to see that the network topology in this case is a *unit-disc* graph. For each vehicle T, we define $r(T)$ as the number of emergency messages the vehicle T has rebroadcasted. A realistic vehicular scenario is presented in Figure 1.

We use the *Simulation of Urban Mobility* (*SUMO*) traffic simulator to place k number of vehicles (k range from 5 to 100 in step of 5) in a $1km \times 8$-lane road grid (4 lanes on either direction). We create a random emergency zone within the first 50m of this grid, as in Figure 1. Any vehicle that approaches this emergency zone will trigger an emergency broadcast message. We set a *Time-to-live* (*TTL*) value of 3 for each triggered message. Thus every vehicle that receives an emergency message with a TTL value of 2 or 3 will rebroadcast the emergency message after reducing the TTL value by one. For a given experiment, we find the maximum, minimum, mean and median number of emergency messages rebroadcasted by a vehicle. For each k, we generate 50 different topologies. We take the average across all the 50 different topologies to remove any random simulation artifacts. We present our findings in Figure 2. As we can see min $\{r(T)\}$ is almost zero for the all the topology we generated. This is because that, there are always vehicles in the edge of the emergency zone that do not rebroadcast any message. On the otherhand, the max $\{r(T)\}$ grows rapidly with respect to the number of vehicles in the topology. On a topology with 100 vehicless, the max $\{r(T)\}$ is 1500. At all the stages the mean and median are close-by (this property also proves that our simulation results are unbiased and the traffic generation is symmetric). We have the mean and median values close to 33% of the maximum $\{r(T)\}$.

Figure 2: Communication overload

Based on the above experiment, a vehicle (or a group of vehicles) with malicious intention will transmit as many as thousands of falsified emergency messages using different forged vehicle identifications to launch a DoS attack. They may also use the TTL-value other than 3 to pretent that they are not the originating source of an emergency message. In the absence of any digital certificate, it is hard for a law enforcing agencies to take legal action against these vehicles.

3 Smart message authentication scheme for safety and emergency messages in a Vehicular network In this section, we propose a smart message authentication scheme to protect vehicular communication from the message falsification attack mentioned in Section 2. Even though, there are a number of proposals available in the literature, our proposed scheme will work in the absence of any PKI or CA. Thus, our proposal is more suitable for a VANET and MANET environments, where there is no guarantee to have access to a central infrastructure.

In VANET, message falsification attack is possible due to the lack of a message authentication feature. However, traditionally, digital certificate is used to solve the message authentication problem. In order for the message authentication system to work effectively, the public key of the transmitting vehicle must be available with all the receiving vehicles. This can be done in two ways; the local registration authority may load securely the public key of all registered vehicles to every vehicle in the country. A list of revoked keys is transmitted to vehicles whenever, they have access to RSU. Thus every vehicle 痴 public-key database is up to date to a certain degree. However, the database will be large due to the number of registered vehicles in every city (or state or country). This not only requires more storage, but increases the latency due to database search. In the worst case scenario, database search consumes $O(n)$-time complexity for a linear search or $O(log(n))$ time, in case the data is organized in a binary tree. Thus, the real-time requirement of 100ms for emergency and safety messages in a vehicular network may not be achievable. An alternative to the offline storage of public key is to have a constant access to a trusted certificate authority to obtain the public key of the transmitting vehicle. This requirement may be achievable in a wired network; however, in a VANET or in a MANET environment, there is no guarantee to have a constant access to a trusted CA.

These requirements force us to look for a new paradigm to provide solution to the message falisification attack.

In our earlier paper [9], we introduced the notion of pseudo-identity based encryption. In this paper, we extend our original idea and provide a solution to the message falsification attack in a vehicular network.

In a vehicular network, more than one vehicle may detect the same road emergency condition. If the condition is severe like road accident, road closure or severe congestion, several vehicles may detect it simultaneously. Thus, if the same emergency condition is transmitted by several vehicles as the originating source (with the maximum TTL value), then the transmitted message may be trustable. We also incorporate this observation in our framework. For this purpose, we use the threshold cryptography introduced by Shamir [10].

In a (k, n)-threshold cryptographic scheme, the secret key d is divided among n-shareholders such that

- The knowledge of k or more shares make it possible to compute the global secret key d.
- The knowledge of k-1 or fewer share make it impossible to compute the global secret key d.

In threshold cryptographic systems, k is chosen in such a way that any adversary can break (k-1) or less shareholders. Thus the system may have less than k malicious shareholders.

Since our proposed algorithm is based on threshold cryptographic scheme, we describe briefly here for completeness.

The threshold cryptography is based on *polynomial interpolation.* Given k distinct points in the two dimensional plane $(x_1, y_1), (x_2, y_2), \ldots (x_k, y_k)$, (with distinct $x_i's$), there is one and only polynomial $P(x)$ of degree k-1 passing through all the k-points.

Let P_{pub}, P_{pri} be the public and the private key for an underlying public key cryptography (like RSA). k-threshold cryptography is used to share the private key P_{pri} to all legitimate nodes (called shareholders), through a random polynomial $f(x)$ of degree k-1.

Even though, polynomial interpolations are defined over $\mathbb{R}$ or over any general ring, threshold crypto systems use polynomial interpolation over $\mathbb{Z}_n$. The choice of n will be decided by the underlying public key crypto system.

Let $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots a_{k-1} x^{k-1}$ be a polynomial of degree k-1 such that $f(0) = P_{pri} mod\, n$ and $a_1, a_2, \ldots, a_{k-1}$ belong to some arbitrary ring $\mathcal{Q}$. For each legitimate node with node identity v_i, its secret share is $SK_i = (f(v_i) mod\, n)$. For any coalition of k-nodes $v_1, v_2, \ldots v_k$, Lagrange interpolation states that $f(0) = P_{pri} = \sum_{j=1}^{k} SK_j * l_{V_j}(0)\ mod(n)$, where $l_{V_j}(x) = \frac{(x-v_1)(x-v_2)\ldots(x-v_{j-1})(x-v_{j+1})\ldots(x-v_k)}{(v_j-v_1)(v_j-v_2)\ldots(v_j-v_{j-1})(v_j-v_{j+1})\ldots(v_j-v_k)}$ is the Lagrange coefficient. Let $P_{V_j} = SK_j * l_{V_j}(0)$. The knowledge of P_{V_j} can expose SK_j. Thus, they cannot be revealed to any one.

Let X be any arbitrary message for which we wish to compute the digital signature $X^{P_{Pri}}$. Since, none of the shareholders have the knowledge of P_{pri}, we have to contact k shareholders, say, (v_1, v_2, $\cdots$, v_k) to obtain their partial digital signatures X^{SK_i}. Since the discrete log problem is computationally hard, from the partial signature, no adversary can compute SK_i. We can then compute the digital signature of X using the formula: $\prod_{j=1}^{k} (X^{SK_j})^{l_{V_j}(0)} = (X)^{\sum_{j=1}^{k} SK_j * l_{V_j}(0)} = X^{P_{pri}}$.

Thus by the coalition of k-shareholders, any message can be digitally signed by the global secret key without the presence of an CA. Therefore, there is no need for the CA after the bootstrap process.

The threshold cryptography in its original form has the following disadvantages:

1. From partial digital signatures X^{SK_i}, it is impossible to obtain the identity of the signed shareholder.

2. It is not possible to verify whether a shareholder whose identity is v_i has signed properly or not.

Since the above two properties are important for providing solution to message falsification attack, we cannot use the threshold cryptography.

Shamir [11], proposed the concept of *identity based cryptography*. In this scheme, a user's public identity like the email address is used as his public key. As a result identity-based cryptography eliminate the need for a PKI or a CA. Although Shamir proposed the concept, he was unable to construct any identity-based cryptographic scheme and conjectured the existence of such a scheme. His conjecture was independently solved by Boneh and Franklin [2] and Cocks [4].

Boneh and Franklin's solution is based on the *Weil Paring*. Their algorithm is called as *BasicIdent*. Elliptical curve variant of the *bilinear Diffie-Hellman* (BDH) problem is considered as the underlying hard problem in their scheme. It has been proved that in a random-oracle model, the protocol is semantically secure under the BDH assumption. Though their algorithm is computationally secure, it is hard to implement on a MANET/VANET environment due to its processor and memory requirements. In a VANET environment, BasicIdent may not satisfy the real-time requirement due to its run-time complexity.BasicIdent is not chosen ciphertext secure. However, Fujisaki-Okamoto transformation allows for conversion to a scheme having this property called *FullIdent*.

Cocks model uses *quadratic residues modulo* over a large composite integer as their underlying hard-problem. Though his solution is much simpler compared with [2], it is not practical as it uses bit-by-bit encryption, which is not economical.This scheme also does not preserve key-privacy, i.e. a passive adversary can recover meaningful information about the identity of the recipient observing the ciphertext.

3.1 Pseudo-Identity based threshold cryptography It is important to note that in a threshold cryptographic scheme, the private share of each shareholder may not have a public key component. Even, if some private share has a public key component, the public key may not reflect the identity of the node.

In this section, we modify the threshold cryptographic scheme in such a way that every secret share has a corresponding public key component and the public key component will be related to the identity of the node. We call it as pseudo-identity based threshold cryptography. We outline the importance of the threshold parameter and its releveance to our work in the following subsection. In vehicular communication, the CA may be the local registration authority or someone designated by the local registration authority.

As like the Shamir's threshold cryptography, the CA must construct the global private and public key pair for any underlying public key cryptography (We assume it to be RSA here). We outline the process as follows:

Let P, Q be two *safe-primes*. That is $P = 2P_1 + 1$ and $Q = 2Q_1 + 1$, where P_1 and Q_1 are prime numbers. Let $N = P * Q$. N is used as the modulus for both the public and private keys. The RSA, being a block cipher, both the plain text and the cipher text are integers between 0 and N-1. Then the Euler's tortient function $\phi(N) = (P-1)(Q-1) = 4P_1Q_1$. The CA then choose a non-trivial number d as its *global secret key* in such a way that d has no common factor with N and $\phi(N)$. Since $\phi(N)$ is an even number, it follows that d must be an odd number. The CA then choose the global public key e in such a way

that $d * e \equiv 1(mod\, \phi(N))$. It is easy to see that d and e will have the following properties:

1. They are odd numbers
2. e and d are not equal to P, P_1, Q, Q_1 and their multiples.

We now outline the modification that leads to our proposed design:

Let $k \neq 1$ be the threshold system parameter. Let $f(x) = d + R(x)$; where $R(x) = a_1x + a_2x^2 + \ldots + a_{k-1}x^{k-1}$ and $a_i's$ belong to some ring of integers $\mathcal{Q}$ be the threshold system polynomial. Except k, all the other system parameter are kept secret and not known to anyone except the CA.

Let X_i be the identity of the i-th node in the network. Then according to the traditional threshold cryptography, its secret share is $SK_i = f(X_i) = d + R(X_i)\ (mod\, N)$, where N is the integer modulo defined above. In order for SK_i to have a public key component, it must satisfy the above two properties.

We first derive a condition to ensure that SK_i is odd for every integer i. Since d is an odd number, SK_i is an odd number if and only if $R(X_i)$ is an even number.

Theorem 1. *Let $R(x) = a_1x + a_2x^2 + \ldots + a_{k-1}x^{k-1}$, where $a_i's$ belong to some ring of integers $\mathcal{Q}$. $R(i)$ is an even number for every integer i if and only if the number of odd $a_i's$ are even.*

Let $R(x)$ be an even integer for every integer $i \in \mathcal{Q}$. In particular, $R(x)$ is an even integer for $x = 1$. That is $R(1) = a_1 + a_2 + \ldots + a_{k-1}$ is an even integer. By grouping odd and even $a_i's$, we have $R(1)$ = (sum of odd $a_i's$) + (sum of even $a_i's$). This implies that (sum of odd $a_i's$) is an even number; and hence the number of odd $a_i's$ are even.

Conversely, let the number of odd $a_i's$ are even. Let x be an even integer. Then a_ix^i is always an even integer. Since $R(x)$ is a sum of even integers, it is an even integer. Now let y be an odd integer. Then a_iy^i is an even number whenever a_i is an even number and odd number if a_i is an odd number. Since the number of odd $a_i's$ are even, it follows that in this case also $R(y)$ is an even integer.

We now present an algorithm in which the keys are computed in such a way that every secret share has a corresponding public key component.

Step 1: Let X be the i-th shareholder whose non-forgeable identity (similar to the MAC address; in case of VANET, it is the vehicle's registration number (REGO)) is X_i. Let $f(x) = d + R(x)$ be the secret polynomial, where $R(x)$ is an even number for every integer x. Choose the smallest integer r_i such that $SK_i = f(X_i + r_i) = d + R(X_i + r_i)(modN)$ has a public key component and SK_i is not distributed to any shareholder before. Since the modulo N is large, such r_i will always exist.

Now SK_i is the secret share for the node X with the non-forgeable ID X_i and PK_i is its public key component for this corresponding SK_i. $< SK_i, PK_i, N >$ is loaded on to X_i's secure module during the registration or bootstrap process.

Step 2: After computing the public key for n-shareholders whose non-forgeable IDs are $X_1, X_2, \ldots, X_n$, the CA then computes the *public key polynomial* $P(x) = b_0 + b_1x + b_2x^2 + \ldots + b_{n-1}x^{n-1}$ of degree $n - 1$ as whose $b_i's$ are given as follows:

$$\begin{bmatrix} 1 & X_1 & X_1^2 & \dots & X_1^{n-1} \\ 1 & X_2 & X_2^2 & \dots & X_2^{n-1} \\ 1 & X_3 & X_3^2 & \dots & X_3^{n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & X_n & X_n^2 & \dots & X_n^{n-1} \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ \vdots \\ b_{n-1} \end{bmatrix} = \begin{bmatrix} PK_1 \\ PK_2 \\ PK_3 \\ \vdots \\ PK_{n-1} \end{bmatrix}$$

Since $X_1, X_2, \cdots, X_{n-1}$ are different, the above matrix equation has a unique solution. Thus there is a unique polynomial $P(x)$ of degree $n-1$ such that $P(X_i) = PK_i$. We call this polynomial as a *hash polynomial* for our threshold crypto system. The CA will load this hash-polynomial in the tamper-resistant available in every vehicle. This polynomial is used to generate the public key of any shareholder, provide a vehicle know the REGO of a shareholder. If, all the coefficient of this hash-polynomial is known to an adversary, he will not able to compromise the system. The main advantage in distributing this polynomial is that if a node knows the identity of any other node, it can easily compute its public key without the presence of an CA.

After this step, there is no need for the existence of an CA.

4 The Solution Architecture In this section, we provide an elegant solution to the message falsification attack in a vehicular network. We make the following natural assumptions about the system.

1. Each vehicle on the road has a unique registration number provided by the registration authority. This registration number is used as a public identity of the vehicle.
2. We assume that vehicles are equipped with an on-board camera that can recognize the registration number of vehicles in front and behind. Even, some of the current budget model cars are equipped with an onboard camera that can recognize street signs, speed limits and traffic signals.
3. Vehicles are equipped with tamper-resistant storage and processor modules like (Trusted Platform Module (TPM) [8]), where the hash function and crypto schemes are securely stored by the registration authority. Since the current and the future generation cars are controlled by real-time onboard computers, their kernel needs to be protected from malware. Thus, a tamper-resistant module is necessary.

   For every vehicle with REGO X_i its shared private key component SK_i, the hash-polynomial are securely loaded to the tamper-resistant module by the certificate authority.
4. Whenever a vehicle has access to the roadside infrastructure (RSU), vehicles will sync their key revocation information with the certificate authority.

The threshold value k is chosen by the CA in such a way that some severe road conditions (like major accident, road closure, etc.) can be detected by k vehicles independently within a reasonable amount of time.

We now present the black box model of our proposed crypto scheme. We call it as a black box model the entire architecture is implemented in a tamper-resistant hardware like Trusted Platform Module [8].

Figure 3: Singature generation module

4.1 Emergency and Safety Message Transmission Whenever a vehicle's hardware detects a safety and emergency condition, it will pass on the message to the secure module for digitally signing the message. For our discussion, we assume that the underlying crypto system is RSA. This may be replaced with any public-key cryptography. The RSA engine will securely retrieve the private key SK_i from the secure storage space. Then <Plain text emergency message, signed emergency message, REGO >is broadcasted to every vehicle with the appropriate TTL value.

The block diagram is presented in Figure 3

4.2 Signature verification Let a vehicle T receive an emergency message. The following steps are taken for verifying the signature:

1. The onboard camera reads the REGO of vehicles around to see if the REGO in the message can be recognized. If the REGO is recognized, then the *onboard_camera_check* flag is set to 1; otherwise, it is set to 0. In several cases, due to obstructions, it may not be possible to verify the REGO by the onboard camera. This flag is not going to influence the action to be taken for this emergency message. It will only serve as an extra layer of security.

   If the same emergency message from the same REGO is seen before either with a same TTL value or lower, the message is discarded.

2. The REGO is passed on to the hash polynomial module as an input. The hash polynomial will output PK_i, the public-key component for this REGO.

3. PK_i along with the signed message is passed on to the RSA module. The RSA module will decrypt the signed message using PK_i and outputs the plain text.

4. The received plain text message along with the decrypted plain text message is passed on to the comparison module. If both the messages are the same, the signature is verified; else the signature verification failed. The received message is discarded if the signature verification failed.

Once the signature is verified, the following actions are taken:

a. Appropriate response to this emergency message is taken.

b. If the message is applicable to a multi hop region, and the TTL value is greater than one, T will rebroadcast the message after reducing the TTL value by one and append its REGO along with the originally received REGO.

c. If the message is critical and needs to obtain the global signature the threshold cryptography, the message is passed on to the temporary storage area, until k similar messages from different originating vehicles are obtained.

The process block diagram for this module is given in Figure 4

Figure 4: Singature Verification module

Figure 5: Global Singature generation module

4.3 Global signature generation If a critical safety-related message independently originates from k or more vehicles, any vehicle can combine all the partial signatures to a globally signed message. Once k similar messages from different originating vehicles are available in the temporary storage area, it is then passed on to the threshold signature generation module. This module will combine all partial signatures and generate the globally signed message as per the threshold cryptographic algorithm outlined in Section 2.

The process block diagram for this module is given in Figure 5

5 Conclusion and Future direction In this paper, we proposed an elegant source authentication scheme based on the modified threshold cryptography. The proposed scheme can be modified effectively to identify vehicles that transmit false safety and emergency messages with fictitious vehicle identity. Our proposed scheme is also used by the law enforcing agencies to precisely to identify the owner of the malicious vehicles. They may also able to revoke their registration dynamically. The key revocation information is transmitted to every vehicle whenever they have access to RSU.

We present below the security analysis of our proposed scheme.

5.1 Security Analysis of the proposed solution

1. Since SK_i and the hash polynomial are loaded onto a tamper-resistant module securely by the registration authority, no user has access to them.
2. The secure module will not sign any non-standard emergency messages. This is to ensure that no user (including the owner of the vehicle) launch a chosen plaintext attack to guess the secret key. The crypt-analysis of our proposed scheme is equivalent to the crypt-analysis of the underlying RSA and the threshold system. Since the underlying RSA and the threshold cryptography are secure, it follows that our proposed model is secure.
3. Since the private key share and the hash polynomial are not disclosed to the owner of a vehicle, even change of ownership of a vehicle does not affect the security of the key.
4. In the event that a key is revoked (incase the associated vehicle registration is suspended), the CA will communicate with every vehicle, whenever they have access to a RSU. During this time, vehicles will sync their key revocation database. This database is stored in the secure storage area.

Our proposed architecture can also be implemented in a MANET or in a distributed environment where the source authentication is an important factor, and there is no constant access to the backbone network. Our future work involves implementing the proposed

scheme in VANET hardware to obtain the real-time performance measures, especially, to evaluate the introduced latency of our scheme in a sparse, average and dense vehicular network.

References

[1] K.Bilstrup, A survey regarding wireless communication standards intended for a high-speed vehicle environment, Technical Report; IDE0712, Halmstad University, Halmstad, 2007.

[2] D.Boneh and M.Franklin. Identity-based encryption from the weil pairing. Proceedings of CRYPTO'01, LNCS, pages 213-229, 2001.

[3] Bureau of Transport and Regional Economics (BTRE). Estimating urban traffic and congestion cost trends for Australian cities, working paper 71. Australian Government, Department of Transport and Regional Services, BTRE, Canberra ACT, 2007.

[4] C.Cocks. An identity-based encryption scheme based on quadratic residues. Proceedings of IMA'01, LNCS, 2260:360-363, 2001.

[5] H.Hartenstein and K.P.Laberteaux, VANET: Vehicular Applications and Inter-Networking Technologies, John Wiley & Sons, NY, USA (2010)

[6] IBM. The roads to a smarter planet from the ibm executive series: Smarter thinking for a smarter planet @ONLINE. https://www.ibm.com/smarterplanet/global/files /nz_en_nz_health_ibmlbn0041_transtasman_book.pdf, May 2015.

[7] X.Ma and X.Chen. Saturation performance of IEEE 802.11 broadcast networks. Communications Letters, IEEE, 11(8): 686-6898, 2007.

[8] TPM: The Trusted Platform Module, @ONLINE. https://en.wikipedia.org/wiki/ Trusted_Platform_Module, Dec.2017

[9] P.Veeraraghavan, Pseudo-identity based encryption and its application in mobile ad hoc networks, IEEE 10th Malaysia International Conference on Communications, (2011), Malaysia.

[10] A.Shamir. How to share a secret. Communications of the ACM, 22(11):612-613, 1979.

[11] A.Shamir. Identity-based cryptosystems and signature schemes. Proceedings of CRYPTO84, LNCS, pages 47-53, 1984.

[12] H. Trivedi, P. Veeraraghavan and et.al., Routing mechanisms and cross-layer design for Vehicular Ad Hoc Networks: A survey, 2011 IEEE Symposium on Computers Informatics (ISCI), 2011.

[13] F.Wang et.al., 2FLIP: A Two-Factor Lightweight Privacy-Preserving Authentication Scheme for VANET, IEEE Transactions On Vehicular Technology, VOL. 65, NO. 2, February 2016