# A Multi-Level Security Architecture for Vehicular Ad Hoc Network

Kevin Daimi, Mustafa Saed, and Scott Bone

***Abstract*—Within few years, vehicles communicating with other vehicles to provide information about road conditions, accidents, fires, or emergency cases, will be a reality. Vehicles will also have access to the internet. As a result, future vehicles networks security should be designed to cope with various kinds of attacks. Furthermore, security requirements including confidentiality, integrity, privacy, and nonrepudiation should be enforced. This paper introduces multi-level security architecture for vehicular ad hoc networks (VANETs). Based on this architecture, the security protocols for Vehicle-to-Vehicle (V2V), Vehicle-to-Roadside Unit (V2R), and Roadside-to-Roadside Unit (R2R) will be presented.**

***Index Terms*— vehicular ad hoc network security, security architecture, security protocols, security requirements**

## I. Introduction

VEHICULAR ad hoc networks (VANETs) have been appealing to researchers working in both vehicle industry and academia. This interest stemmed from the would-be applications, which will drive the intelligent transportation systems (ITS). The Vehicular ad hoc network (VANET) is a subclass of the Mobile Ad-Hoc Network (MANET) [1]. Safety–critical information, such as speed, heading, and position is broadcasted by the vehicle in Vehicle-to-Vehicle (V2V) communication networks to the nearby vehicles, which are in the range of their wireless communication. Even warning message regarding accidents can be propagated by the vehicles to other vehicles, which are not in the vicinity of the accident [1] [2]. These warning messages can assist drivers to avoid any further collisions and take safety measures, such as driving through alternative routes and eluding traffic congestions. Intelligent Transportation System (ITS) can be supported by the new and evolving technologies, especially the DSRC (Dedicated Short Range Communications) at 5.9 GHz, which will furnish data communication between entities, such as vehicles and infrastructure. The use of infrastructure sensors was suggested in order to determine the location of vehicles, and accordingly the transmission of information to several other vehicles approaching the intersection through CSMA MAC protocol has been proposed by researchers for intersection collision warning system [3]. Traditionally, there are two types of communications in the VANET: Vehicle-to-Vehicle (V2V) in which vehicles exchange important messages, such as road condition, accidents, and fire, and Vehicle-to-Infrastructure (V2I), which allows a vehicle to establish a connection with the roadside units for communicating with a number of services, such as the internet, restaurants, and gas stations. This paper will refer to V2I as Vehicle-to-Roadside Unit (V2R) communication. A third VANET communication type proposed by this paper is the Roadside Unit-to-Roadside Unit (R2R). This will be used to enhance security of the VANETs.

All the above types of VANET communications will be the focus of various passive and active attacks. Security is the most critical concern facing VANETs, and will continue to be so for many years after the VAENT is implemented. At the network security level, particularly wireless network, there have been many threats and breaches. Since ad hoc vehicular networks will be utilized in many ways in our modern life, any attack on VANETs could be one of the most disastrous events resulting in possibly fatal consequences. We are facing an increasing severity and sophistication of security attacks on our computerized systems, and internet-based systems. These attacks could easily span VANETs if precautions are not enforced. To counter-attack these attempts, we need a strategy that demands the deployment of dedicated hardware and software techniques in addition to well-trained professionals [4]. Well-prepared security professionals should be equipped with a deep insight of the likely security vulnerabilities of computing and network systems, the foundational protection techniques and procedures for such systems, and the limitations of such protection mechanisms [5]. These requirements are even more demanding for VANETs.

To attain dominant and efficient security, cryptology should be embraced. As there are normally parties, such as vehicles and RSUs communicating, cryptographic protocols are prerequisites for ensuring security. A protocol is a multiparty process represented as a sequence of steps that exactly determines the actions required of two or more parties in order to accomplish an identified end [6]. A cryptographic protocol is one that applies cryptology. Cryptographic protocols encompass exchanging of messages between parties. Protocols are probably the most difficult part of cryptography [7].

Considerable research efforts have been devoted to the field of VANET security. Mishra et al [8] surveyed a number of research work in VANET security. Based on

Manuscript received October 10, 2013; revised February 6, 2014.

K. Daimi is with Computer Science and Software Engineering, the University of Detroit Mercy, Detroit, MI 48221 USA (phone: 313-993-1060; fax: 313-993-1187; e-mail: daimikj@udmercy.edu).

M. Saed is with the HATCI Electronic Systems Development, Hyundai-Kia America Technical Center, Superior Township, MI 48198 USA (e-mail: msaed@hatci.com).

S. Bone is with the HATCI Electronic Systems Development, Hyundai-Kia America Technical Center, Superior Township, MI 48198 USA (e-mail: sbone@hatci.com).

their survey, they concluded that there are three types of applications of VANETs: safety, convenience, and commercial applications. Examples of these include slow/stop vehicle advisor (SVA), emergency electronic brake light (EEBL), post-crash notifications (PCN), road hazard control notification (RHCN), cooperative collision warning, congested road notification, remote vehicle personalization/diagnostics (RVD/D), parking availability notification (PAN), and service announcements (SA). All these are critical applications and call for high level of security enforcements. Raya et al [9] analyzed threats and described design decisions that have more than technical implications. They provided some security protocols to protect privacy, and then analyzed their robustness via some quantitative assessment. They stressed that a vehicle normally possesses a large set of anonymous keys to prevent tracking. We believe this approach is risky as it makes key management extremely hard for vehicles with their limited capabilities. In addition, the large set of keys demands a lot of storage.

Wang et al [10] emphasized that dividing the road side units (RSUs) into application-RSUs (AP-RSUs) and authentication-RSUs (AU-RSUs) in application layer will enhance the security of vehicular ad hoc networks. According to the authors, their functional division of RSUs results in a more logically clear VANETS. In their setting, the AU-RSUs capture and record a vehicle's identity and provide temporary certificates that protect the vehicle's real identity. They added that by doing that, vehicle anonymity and realizing its traceability are guaranteed.

Reviewing the standardization process covering the methods of providing security services and preserving driver privacy for Wireless Access in Vehicular environments (WAVE) applications was carried out by Lin et al [11]. They addressed two fundamental concerns; certificate revocation and conditional privacy preservation to make the standards practical. For this purpose, they introduced a suite of novel security mechanisms. Raya et al [12] studied the security of vehicular networks. They explained the basic safety messaging protocol and investigated various attacks on vehicular network. A number of security requirements were stated including authentication, availability, nonrepudiation, privacy, and data consistency.

Sabahi [13] discussed the security issues of vehicular ad hoc networks. The author analyzed some of the threats related to security requirements. The black hole attack, malware, broadcast tampering, spamming, greedy drivers, and denial of service represented examples of threats to availability. Concerning authentication, the author cited masquerading, replay attack, GPS spoofing, tunneling, Sybil attack, message tampering, and ID disclosure as potential threats.

Privacy is a critical issue in VANETs. Plößl et al [14] proposed a security infrastructure that deploys both symmetric and asymmetric cryptology and tamper resistance hardware. Their aim was to protect the privacy of the vehicular ad hoc network users. To this end, they discussed its efficiency in terms of computational needs and bandwidth overhead. Location privacy, as one of principle security challenges for VANETs was studied by Wasef et al [15]. The goal was to deter attackers from tracing a specific vehicle. Random encryption periods based on a privacy preserving group communication protocol were presented. To prove their approach is legitimate, they relied on detailed analysis and simulation.

Commercial services, such as Internet access, and video streaming, highlight another area that drew the attention of researchers. The essential requirements of authentication, privacy, and billing for service dispensing in vehicular networks were identified by Zhu et al [16]. They reviewed the available research attempts in academia and industry regarding service-oriented vehicular networks. They considered distributed key revocation and V2I authentication as the two main security challenges. Lee et al [17] examined securing incentives for commercial ad dissemination in V2V communication. They introduced the Signature-Seeking Drive (DSS) as a secure incentive framework for commercial ads propagation which does not depend on tamper-proof hardware but adopts Public Key Infrastructure (PKI) to enforce the secure incentives. Further research attempts dealing with various aspects of vehicular ad hoc networks security could be found in [18]-[24].

This paper presents multi-layer security architecture for vehicular ad hoc networks and the needed protocols to support this architecture. The Roadside units are divided into five levels: country, state, county, city and street. Section II introduces the multi-level security architecture. Section III deals with the RSU-to-RSU security protocol. The security protocols for RSU-to-Vehicle and Vehicle-to-Vehicle are presented in sections IV and V respectively. In section VI, the fulfillment of the security requirements is discussed. Finally, the conclusion is provided in section VII.

## II. MULTI-LEVEL SECURITY ARCHITECTURE

To achieve the highest possible security, a tree structure is suggested. As shown in Fig. 1, the road side units (RSUs) are distributed over five levels; *stree*t, *city*, *county*, *state*, and *country* levels. Nodes at the city level and above have children nodes. The physical locations of these RSUs (nodes) will be determined by the authorities in charge to provide the needed optimal and secure arrangement. Each node manages the security of its children. RSUs at the street level ($RSU_{ST}$) are in charge of vehicles within their ranges. If a node is attacked, the parent node can inactivate that RSU, resolve the problem, re-distribute keys with the children, and then re-activate it.

Computing power increases as the tree is traversed upward. The country-level node ($RSU_C$) controls all the state-level nodes ($RSU_S$) and transmits nationwide alert messages. It acts as the point of contact with infrastructure of other countries. It exchange messages with other countries and provide state-level nodes ($RSU_S$) with information about foreign vehicles. If no information is obtained about the foreign vehicle either because that country is not implementing the ad hoc vehicle network infrastructure, or because of any technical reason, that vehicle will not be part of the street nodes. If the information is obtained later, it will be transferred through the state level until it reaches the street level.

The state-level RSUs ($RSU_S$) maintain the vehicle database for its state. This is currently the case even before implementing the ad hoc vehicle networks. Therefore, the state-level RSUs will verify any information needed by the county-level nodes. In particular, a state-level RSU will ensure the received vehicle ID is for a legal vehicle and is valid. A state-level RSU receives alerts from county-level RSUs ($RSU_{CO}$) and propagates them to other counties within the state. If the alert is important for other states, it will be forwarded to the country-level RSU ($RSU_C$) to inform all other state-level RSUs ($RSU_S$).

County-level RSUs ($RSU_{CO}$) send the IDs received from the city-level nodes ($RSU_{CI}$) to the state-level nodes ($RSU_S$) for verification and notify the city-level nodes. They receive the actual ID, all anonymous IDs ($ID_{VA}$) assigned to a particular vehicle, and the location at the time the anonymous ID was assigned. The county-level RSU ($RSU_{CO}$) then stores this information together with further information received from state-level RSU ($RSU_S$), such as vehicle model, color, and registration number, and the city-level ID ($ID_{CI}$). This history data would be important for law enforcement authority when problems occur.

If an alert message is necessary to pass beyond the current street section, the city-level RSU ($RSU_{CI}$) will take care of informing other street-level RSUs ($RSU_{ST}$). Furthermore, city-level RSUs receive vehicle ID ($ID_V$) with all the anonymous IDs ($ID_{VA}$) used for this vehicle. It stores this information with the ID of the street-level RSU ($ID_{ST}$). The city-level RSU ($RSU_{CI}$) is in charge of forwarding the vehicle ID received from the street-level RSU ($RSU_{ST}$) to the county-level RSU ($RSU_{CO}$) for verification purposes. As mentioned above, the county-level RSU ($RSU_{CO}$) will forward the $ID_V$ to state-level RSU ($RSU_S$) for the actual verification.

The street-level RSU ($RSU_{ST}$) will be communicating with vehicles in the street section they are responsible for. They are also in charge of issuing the temporary security certificates for vehicles. They store the most recent version of the certificate, current anonymous IDs, and some parameters, which will be explained below, to manipulate the current *ID* and generate the next anonymous ID ($ID_{VA}$). No real IDs will appear in the certificates. The street-level RSU ($RSU_{ST}$) does not need to store the actual ID.

Public key cryptology is the only technique used with RSU-to-vehicle and vehicle-to-vehicle communications. These keys are periodically changed by the vehicle or upon request from street-level RSU when it needs to issue new certificates. For RSU-to-RSU communications, both symmetric and asymmetric keys are used. Symmetric cryptology is used for exchanging messages, which could possibly be long. Note that public key cryptology tends to be very slow with long messages. PKI is only used to distribute the master (symmetric). Once the master keys are distributed, both the public and private keys can be discarded. If physical distribution of the master keys is feasible, then there is no need for PKI. An alternative to using both symmetric and a symmetric cryptology would be to rely only on PKI and have each higher level node create a certificate for the nodes below it. However, the overhead of revoking certificates and controlling these certificates will be a critical issue. Moreover, the number of RSUs and their locations are fixed. This is unlike the number vehicles and their ever changing locations.

Three different protocols are implemented for this security architecture; RSU-to-RSU, RSU-to-Vehicle, and Vehicle-to Vehicle. The participating roles and notations used in these protocols are depicted in Table I and Table II respectively.

It is a critical physical design issue to have the city-level RSUs broadcast messages to the street-level RSUs and from there to the vehicles in no more than 300 micro seconds. If there is a need to communicate with even higher level, this constraints must never be violated to ensure safety.

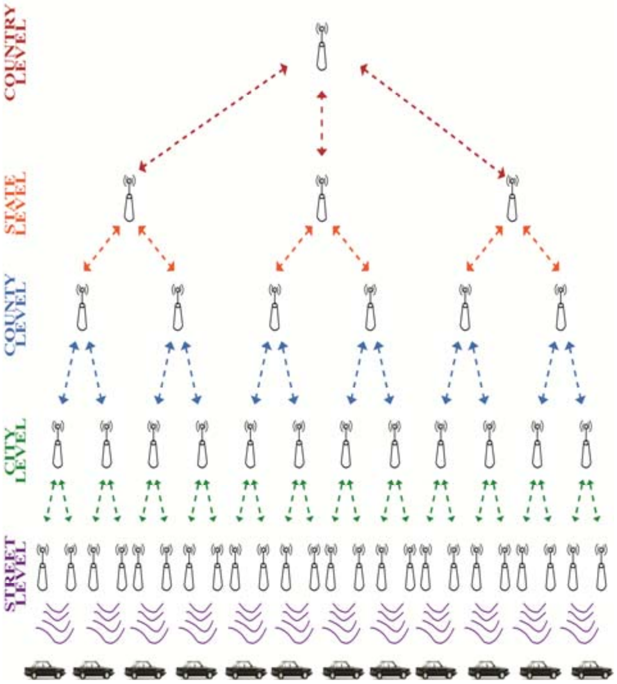

Fig. 1. Multi-Level Security Architecture

TABLE I
PARTICIPATING PARTIES

| Symbol | Role |
|---|---|
| *RSU* | Road side unit |
| $RSU_C$ | Country-level RSU |
| $RSU_S$ | State-level RSU |
| $RSU_{CO}$ | County-level RSU |
| $RSU_{CI}$ | City-level RSU |
| $RSU_{ST}$ | Street-level RSU |
| *V* | Vehicle |

## III. Roadside Unit-to-Roadside Unit Communication

The roadside-to-roadside (RSU-to-RSU) communication cryptographic protocol is described as follows:

1. RSUs at each level create their own public and private keys. Parents and children nodes exchange their public keys.
   a. $RSU_C$ creates $PU_C$, $PR_C$ and sends $PU_C$ to $RSU_S$.
   b. $RSU_S$ creates $PU_S$, $PR_S$ and sends $PU_S$ to $RSU_C$ and $RSU_{CO}$.
   c. $RSU_{CO}$ creates $PU_{CO}$, $PR_{CO}$ and sends $PU_{CO}$ to $RSU_S$ and $RSU_{CI}$.

d. $RSU_{CI}$ creates $PU_{CI}$, $PR_{CI}$ and sends $PU_{CI}$ to $RSU_{CO}$ and $RSU_{ST}$.

e. $RSU_{ST}$ creates $PU_{ST}$, $PR_{ST}$ and sends $PU_{ST}$ to $RSU_{CI}$

2. Each parent node (RSU) creates a master key (symmetric key). At this point, we have the keys; $K_{MC}$, $K_{MS}$, $K_{MCO}$, and $K_{MCI}$ created.
3. The master symmetric key and the ID of the node are encrypted with the public keys of the children nodes (RSUs) and sent to them.

a. $E(PU_S, K_{MC}) \rightarrow RSU_S$

b. $E(PU_{CO}, K_{MS}) \rightarrow RSU_{CO}$

c. $E(PU_{CI}, K_{MCO}) \rightarrow RSU_{CI}$

d. $E(PU_{ST}, K_{MCI}) \rightarrow RSU_{ST}$

4. Each node will use its private key to decrypt the message and obtain the master key and verify the ID. After decrypting each of the above, the master keys $K_{MC}$, $K_{MS}$, $K_{MCO}$, and $K_{MCI}$ will be obtained by $RSU_S$, $RSU_C$, $RSU_{CI}$, and $RSU_{ST}$ respectively. The public and private keys could now be discarded.
5. Parent nodes create session keys (symmetric keys) and encrypt them with the master key. This is then forwarded to the nodes (children) at the next lower level. Each child will receive a different session key. This implies that children share different session keys with their parents. Note that nodes (RSUs) belonging to different parents do not share keys.

a. $E(K_{MC}, K_{SC}) \rightarrow RSU_S$

b. $E(K_{MS}, K_{SS}) \rightarrow RSU_{CO}$

c. $E(K_{MCO}, K_{SCO}) \rightarrow RSU_{CI}$

d. $E(K_{MCI}, K_{SCI}) \rightarrow RSU_{ST}$

6. To exchange a message between a parent node and its child node, the following protocol is followed.

a. The message digest ($H(M)$) of the message is calculated

b. The message and its digest are concatenated and encrypted with the session key. At this point the message is sent. Note that steps (i) – (iv) below represent messages sent from the parent node to its children. Step (v) involves sending a message from the children ($RSU_{ST}$) to the parent node ($RSU_{CI}$). This is valid because a parent node and its children nodes share the same session key ($K_{SCI} = K_{SST}$).

i. $E[K_{SC}, M \| H(M)] \rightarrow RSU_S$

ii. $E[K_{SS}, M \| (H(M)] \rightarrow RSU_{CO}$

iii. $E[K_{SCO}, M \| H(M)] \rightarrow RSU_{CI}$

iv. $E[K_{SCI}, M \| H(M)] \rightarrow RSU_{ST}$

v. $E[K_{SST}, M \| H(M)] \rightarrow RSU_{CI}$

c. The receiver will decrypt the message with the session key, calculate the hash of the original message, and compare the two hash values. If they are equal, it will accept the message

7. Children nodes do not exchange messages directly. Messages have to go to the parent node, and if needed, to the children.

TABLE II
PROTOCOL NOTATIONS

| Symbol | Meaning |
|---|---|
| $PU_C$ , $PR_C$ | Public & private key of country-level RSU |
| $PU_S$ , $PR_S$ | Public & private key of state-level RSU |
| $PU_{CO}$ , $PR_{CO}$ | Public & private key of county-level RSU |
| $PU_{CI}$ , $PR_{CI}$ | Public & private key of city-level RSU |
| $PU_{ST}$, $PR_{ST}$ | Public & private key of street-level RSU |
| $PU_V$, $PR_V$ | Public & private key of vehicle |
| $K_M$ | Symmetric Master Key |
| $K_S$ | Symmetric Session Key |
| $K_{MC}$, $K_{SC}$ | $K_M$, $K_S$ shared by country and state RSUs |
| $K_{MS}$, $K_{SS}$ | $K_M$, $K_S$ shared by state and county RSUs |
| $K_{MCO}$, $K_{SCO}$ | $K_M$, $K_S$ shared by county and city RSUs |
| $K_{MCI}$, $K_{SCI}$ | $K_M$, $K_S$ shared by city and street RSUs |
| $K_{MST}$, $K_{SST}$ | $K_{MST} = K_{MCI}$, $K_{SST} = K_{SCI}$ |
| $\Vert$ | Concatenation |
| $E$ | Encrypt |
| $\rightarrow$ | Send to |
| $H(M)$ | Hash of message M |
| $V2V$ | Vehicle-to-vehicle communication |
| $V2R$ | Vehicle-to-RSU communication |
| $R2R$ | RSU-to-RSU communication |
| $T_I$ | Issue time |
| $T_E$ | Expiration time |
| $ID_{VA}$ | Anonymous ID of vehicle |
| $ID_C$ | ID of country-level RSU |
| $ID_S$ | ID of state-level RSU |
| $ID_{CO}$ | ID of county-level RSU |
| $ID_{CI}$ | ID of city-level RSU |
| $ID_{ST}$ | ID of street-level RSU |
| $ID_V$ | Real ID of vehicle |

## IV. VEHICLE-TO- ROADSIDE UNIT COMMUNICATION

Vehicles communicate with the street-level RSUs only. Below is the proposed protocol.

1. The street-level RSU, $RSU_{ST}$, receives the real ID of the vehicle, $ID_V$, and sends its Public key, $PU_{ST}$, to the vehicle.
2. The vehicle creates its own public and private key pairs ($PU_V$, $PR_V$), and sends its public key, $PU_V$, in addition to the three measurements; temperature inside the vehicle, rpm, and odometer reading all encrypted with street-level RSU's public key, $PU_{ST}$, to the street-level RSU, $RSU_{ST}$.
3. The street-level RSU, $RSU_{ST}$, adds these three quantities together and then selects the first three nonzero digits, r1, r2, and r3. Although very rare, if the second and/or third nonzero digits are not found, they will be taken as 1. If r1 is odd, street-level RSU, $RSU_{ST}$, will rotate the ID (currently it is the real one, but subsequent IDs will be the last ones used) r3 times left. If r1 is even, it rotates the ID r3 times right. Later, it multiplies the resulting number by r2 to get the anonymous ID. These anonymous IDs, $ID_{VA}$, together with the real ID, $ID_V$ will be

ISBN: 978-988-19252-7-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

forwarded to the city-level RSU to be stored in case there is a need to track the driver of the vehicle by police or for any other purpose.

4. The street-level RSU, $RSU_{ST}$, will send the vehicle its certificate, which contains ($ID_{VA}$ || $PU_V$ || $T_I$ || $T_E$) after encrypting it with its private key, $PR_{ST}$. The issue time, $T_I$, will be saved. It also sends the $T_I$ encrypted with the vehicle's public key, E ($PU_V$, $T_I$).
5. If the expiration time, $T_E$, is reached, a message encrypted with the private key of the street-level RSU, $PR_{ST}$, will be broadcasted indicating it is time to change certificates.
6. To issue the next certificate,
   a. The street-level RSU, $RSU_{ST}$, will send a message to the vehicle indicating it will issue a new certificate.
   b. The vehicle, $V$, will create new pair of keys ($PU_V$, $PR_V$) and send the current ID, $ID_{VA}$, and the public key, $PU_V$, encrypted with the public key of the street-level RSU, $PU_{ST}$.
   c. The street-level RSU, $RSU_{ST}$, decrypts the message, verifies the $ID_{VA}$, and obtains the new public key, $PU_V$, of the vehicle.
   d. If the current ID, $ID_{VA}$, is valid, the $RSU_{ST}$ will randomly select one of the combinations (r1,r2,r3), (r2,r3,r1), (r2,r1,r3), (r3,r2,r1), (r3,r1,r2), (r1,r3,r2), and carry out the rotation and multiplication of step 3 above to create the new anonymous ID, $ID_{VA}$.
   e. The new certificate containing the newly created ID, the new vehicle's public key, issue time, and expiration time, all encrypted with street-level RSU's private key, $PR_{ST}$, will be issued.
7. At any time, the street-level RSU, $RSU_{ST}$, can request the vehicle to refresh the three values (r1, r2, r3) in step 2 above. This could happen when suspecting attacks taking place or when there is traffic jam. Traffic jams allow enough time for attackers to carry out their attacks.
8. To exchange messages between the street-level RSU and a vehicle, both parties need to authenticate each other.
   a. The vehicle, $V$, sends its certificate encrypted with the street-level RSU's public key, $PU_{ST}$. After decrypting the message by the street-level RSU using its private key, $PR_{ST}$, the $ID_{VA}$ and $PU_V$ pairs of the vehicle are checked. In addition, issue and expiration times ($T_I$, $T_E$) of the certificate are verified. The issue time, $T_I$, of the certificate must not be less the time stored by street-level RSU, $RSU_{ST}$, when the certificate was issued.
   b. If authentication is successful, the street-level RSU, $RSU_{ST}$, sends the vehicle its $ID_{VA}$, $PU_V$, and a time stamp all encrypted with its private key, $PR_{ST}$. The vehicle will decrypt this using the RSU's public key, $PU_{ST}$, and verify that it contains its $ID_{VA}$ and $PU_V$, and then verify the currency of this message based on the time stamp.
9. Messages can now be exchanged. Each party (street-level RSU or Vehicle) will calculate the cryptographic hash of its message, encrypt the message with the public key of the other party, and then sign the encrypted message and the hash with its own private key. The cryptographic hash will ensure the integrity of the message.
10. To enhance security, the street-level RSU, $RSU_{ST}$, will change its public and private keys periodically. For vehicles still within the range, the new public key is broadcasted. Upon receiving the new public key, the vehicles will create their own public and private keys and request a new certificate as above.
11. At any time, a vehicle can create new pair of keys ($PU_V$, $PR_V$) and request a new certificate. This should be done whenever there is a suspicious activity or a long traffic delay.

## V. Vehicle-to-Vehicle Communication

Vehicles broadcast messages to all other vehicles (and RSU) within the allowable range. They transmit their GPS position, speed, acceleration, heading, transmission state, brake status, steering wheel angle, path history, and path prediction all in one message every 100ms. In addition, they broadcast alert messages. Receiving Vehicles have 300ms to analyze a message and respond. When vehicles communicate, the following protocol is applied:

1. Each vehicle decrypts the encrypted $T_I$ that was sent with the certificate by the $RSU_{ST}$ to get $T_I$. It then saves it
2. Each vehicle, $V$, broadcasts a message that contains the following: original certificate of the vehicle, and the appropriate message with its hash signed by the sender's private key, $PR_V$.
3. Upon receiving the concatenated message, vehicles will do the following:
   a. Decrypt the certificate with street-level RSU's public key, $PU_{ST}$, verify the expiration time, $T_E$, of the certificate, and obtain the public key of the sender vehicle, $PU_V$.
   b. Extract the issue time, $T_I$, of the sender's certificate and compare to the receiving vehicle's saved *issue time*.
   c. If the $T_I$ (sender) >= $T_I$ (receiver), step (d) is executed. Otherwise (sender time < receiver time), the invalid certificate and the message "Invalid certificate" are concatenated and broadcasted to all vehicles and the street-level RSU, $RSU_{ST}$, in charge. This serves two goals; it

allows the $RSU_{ST}$ to take action, and prevents other vehicles from sending the same message.

d. Use the extracted public key of the sender, $PU_V$, to decrypt the encrypted message and its hash.

e. Hash the plain message and compare the two hashes.

f. If not equal, ignore the message and forward to the $RSU_{ST}$ indicating an integrity problem.

g. If successful, accept the message and act accordingly if necessary.

4. If any vehicle is in doubt, it can forward the message to the street-level, RSU, $RSU_{ST}$, for further verification.

## VI. Fulfilling Security Requirements

The above protocols and security architecture guarantee that the security requirements, nonrepudiation, confidentiality, integrity, authentication, and anonymity are satisfied.

### *A. Nonrepudiation*

The sender, whether it is the RSU or vehicle, cannot deny the message was sent. This is because the message and its hash are signed (encrypted) with the private key of the sender. The following cannot be denied:

a. The street-level RSU, $RSU_{ST}$ sends the vehicle its certificate, after encrypting it with its private key, $PR_{ST}$ (section IV, step 4).

b. If authentication is successful, the street-level RSU, $RSU_{ST}$, sends the vehicle its $ID_{VA}$, $PU_V$, and a time stamp all encrypted with its private key, $PR_{ST}$ (section IV, step 8b).

c. If the expiration time, $T_E$, is reached, a message encrypted with the private key of the street-level RSU, $PR_{ST}$, will be broadcasted indicating it is time to change certificates (section IV, step 5).

d. For messages exchanged between the RSU and Vehicle, the encrypted message and the hash are encrypted with each party's own private key (section IV , step 9)

e. Each vehicle, *V*, broadcasts a message, which contains the following: original certificate of the vehicle, and appropriate message signed by the sender's private key, $PR_V$ (section V, step 2)

### *B. Confidentiality*

Messages that are sent are encrypted with the public key of the receiver. This ensures no one can read the message but the receiver. Only the receiver can decrypt the message with its private key.

a. The vehicle sends its public key, $PU_V$, in addition to the three measurements; temperature inside the vehicle, rpm, and odometer reading all encrypted with street-level RSU's public key, $PU_{ST}$, to the street-level RSU, $RSU_{ST}$ (section IV, step 2).

b. The vehicle, *V*, will send the current ID, $ID_{VA}$, and the public key, $PU_V$, encrypted with the public key of the street-level RSU, $PU_{ST}$ (section IV, step 6b).

c. The vehicle, *V*, sends its certificate encrypted with the $RSU_{ST}$'s public key, $PU_{ST}$ (section IV, step 8a).

d. Each party (street-level RSU or Vehicle) will calculate the cryptographic hash of its message, and encrypt the message with the public key of the other party (section IV, step 9).

e. The master symmetric key and the ID of the node are encrypted with the public keys of the children nodes (RSUs) and sent to them (section III, step 3).

f. The message and its digest are concatenated and encrypted with the session key (section III, step 6b).

### *C. Integrity*

To ensure the message has not been modified, a cryptographic hash is used.

a. Each party (street-level RSU or Vehicle) will calculate the cryptographic hash of its message, encrypt the message with the public key of the other party, and then sign the encrypted message and the hash with its own private key (section IV, step 9).

b. The message digest (*H (M)*) of the message is obtained using a hashing technique (section III, step 6a).

c. Each vehicle, *V*, broadcasts a message that contains the following: original certificate of the vehicle, appropriate message signed by the sender's private key, $PR_V$, and the hash of the message (section V, step 2).

### *D. Authentication*

To ensure that a party is communicating with the ones claiming they are, certificates are used.

a. The vehicle, *V*, sends its certificate encrypted with the street-level RSU's public key, $PU_{ST}$ (section IV, step 8a).

b. If authentication is successful, the street-level RSU, $RSU_{ST}$, sends the vehicle its $ID_{VA}$, $PU_V$, and a time stamp all encrypted with its private key, $PR_{ST}$ (section IV, step 8b).

c. Each vehicle, *V*, broadcasts a message that contains the following: original certificate of the vehicle, appropriate message signed by the sender's private key, $PR_V$, and the hash of the message (section V, step 2).

### E. *Anonymity*

Vehicle ID anonymity is achieved by randomly selecting three values based on inner temperature, rpm, and odometer reading to the RSU (section IV, step2). The RSU applies the randomly selected rotation and multiplication to create the new anonymous ID.

## VII. Conclusion

To enhance the security of vehicular ad hoc network, multi-level security architecture has been proposed. The tree structure isolates an RSU from its neighboring RSUs and allows connection to the parent node only. The suggested protocols aim at enforcing security and satisfying the security requirements; nonrepudiation, confidentiality, integrity, authentication and anonymity. For the street-level RSU and vehicle communication, public key infrastructure (PKI) is the best choice since multiple temporary certificates are needed.

## References

[1] U.S Department of Transportation, National Highway Traffic Safety Administration, Vehicle Safety Communications Project, "*Identifying Intelligent Vehicle Safety Applications Enabled by DSRC"*, Task 3 Final Report, 2005.

[2] L. Briesemeister, L. Schafers and G. Hommel, "Disseminating messages among highly mobile hosts based on inter-vehicle communication" in *Proc. the IEEE Intelligent Vehicles Symposium*, 2000, pp. 522-527.

[3] A. Dogan, G. Korkmaz, Y. Liu, F. Ozguner, U. Ozguner, K. Redmill, O. Takeshita and K. Tokuda, "Evaluation of intersection collision warning system using an inter-vehicle communication simulator," *in Proc. the 7th International IEEE Conference on Intelligent Transportation Systems*, 2004, pp. 1103 – 1108.

[4] W. Stallings and L. Brown, *Computer Security Principles and Practice*. New Yourk, NY: Prentice Hall, 2012, ch. 1.

[5] D. Gollmann, *Computer Security*. Chichester, West Sussex: Wiley, 2011, ch. 2.

[6] A. Menezes, P. van Oorschot and S. Vanstone. (1996, October). Handbook of Applied Cryptology, CRC Press [Online]. Available: http://cacr.uwaterloo.ca/hac.

[7] B. Schneier, *Practical Cryptology*. New York, NY: John Wiley, 1996, ch. 2.

[8] B. Mishra, P. Nayak and S. Behera, "Security in vehicular ad hoc networks: a survey," in *Proc. International Conf. Communication, Computing and Security*, 2011, pp. 590-595.

[9] M. Raya and J. Hubaux, "The security of VANETs," in *Proc. the second ACM International Workshop on Vehicular Ad Hoc Networks*, 2005, pp. 93-94.

[10] J.Wang and N. Jiang, "A simple and efficient security scheme for vehicular ad hoc networks," in *Proc. the IEEE International Conf. Network Infrastructure and Digital Conten*t, 2009, pp. 591-595.

[11] X. Lin, R. Lu, C. Zhang, H. Zhu, P. Ho and X. Shen, "Security in vehicular ad hoc networks," *IEEE Communications Magazine*, pp. 88-95, Apr. 2008.

[12] M. Rsya and J. Hubaux, "The security of vehicular ad hoc networks," in *Proc. the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks*, 2005, pp. 11-21.

[13] F. Sabahi, "The security of vehicular ad hoc networks, in *Proc. the 3rd International Conf. Computational Intelligence, Communication Systems, and Networks*, 2011, pp.338-342.

[14] K. Plößl and H. Federrath, "A privacy aware and efficient security infrastructure for vehicular ad hoc networks," *Computer Standards and Interfaces*, vol. 30, pp. 390-397, 2008.

[15] A. Waswf and X. Shen, "REP: Location privacy for VANETs using random encryption periods," *Mobile Networks and Applications*, vol. 15, no. 2, pp. 172-185, 2010.

[16] H. Zhu, R. Lu, X. Shen and X. Lin, "Security in service-oriented vehicular networks," *IEEE Wireless Communications*, pp. 16-22, Aug. 2009.

[17] S. Lee, G. Pan, J. Park, M. Gerla and S. Lu, "Secure incentives for commercial ad dissemination in vehicular networks," in *Proc. the 13 Annual International Conf. Mobile Computing and Networking*, 2007, pp. 150-159.

[18] J. Isaac, J. Camara, S. Zeadally and J. Marquez, "A secure vehicle-to-roadside communication payment protocol in vehicular ad hoc networks," *Computer Communications*, vol. 31, no. 10, pp. 2478-2484, 2008.

[19] C. Li, M. Hwang and Y.Chu, "A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks," *Computer Communications*, vol. 31, no. 12, pp. 2803-2814, 2008.

[20] C. Zhang, X. Lin, R. Lu and P. Ho. "RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks," in *Proc. the IEEE International Conf. Communications*, 2008, pp. 19-23.

[21] J. Sun, C. Zhang, Y. Zhang and Y. Fang, "An identity-based security system for user privacy in vehicular ad hoc networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 219, no. 9, pp. 1227-1239, 2010.

[22] K. Plößl, T. Nowey and C. Mletzko, "Towards a security architecture for vehicular ad hoc networks," in *Proc. the First International Conf. Availability, Reliability and Security*, 2006, pp. 374-381.

[23] M. Raya and J. Hubaux, "Securing Vehicular ad hoc networks," *Journal of Computer Security*, vol. 15, no. 1, pp. 39-68, 2007.

[24] P Kamat, A. Baliga and W. Trappe, "Secure, pseudonymous, and auditable communication in vehicular ad hoc networks," *Security and Communication Networks*, vol. 1, pp. 233-244, 2008.