Securing Commercial Ad Broadcasting in Vehicular Ad Hoc Networks

Kevin Daimi
Computer Science and Software Engineering
University of Detroit Mercy
Detroit, USA
daimikj@udmercy.edu

Mustafa Saed and Scott Bone
HATCI Electronic Systems Development
Hyundai-Kia America Technical Center
Superior Township, USA
{msaed, sbone}@hatci.com

***Abstract*—Commercial advertising via vehicular ad hoc networks (VANETs) is a promising application. It allows organizations to target drivers and passengers with the aim of promoting their products and services. The implementation of such an application will not be successful without guaranteeing that these ads will not include any malicious information, and the ads will be broadcasted. This paper will apply a cryptographic protocol to secure the dissemination of commercial ads. Secure incentives for drivers reading/watching the ad will be introduced. Cheating, including multiple incentives for the same ad by the same driver will be dealt with.**

Keywords-Commercial Ad; Vehicular Ad Hoc Networks; Security; Security Architecture; Secure Incentives.

I. INTRODUCTION

Vehicular ad hoc networks (VANETs) treat vehicles in their vicinity as wireless nodes. Vehicles within this area can communicate with each other. Any vehicle exiting the zone will lose its communication with that VANET. Vehicular ad hoc networks allow vehicles to broadcast messages to all other vehicles within the range. This presents a great opportunity for various applications to be implemented on vehicles using their computing power and storage capabilities. Safety-critical information including speed, heading, and position in addition to various warning on accidents and road conditions, and infotainment can be broadcasted by vehicles using vehicle-to-vehicle communication. Vehicular ad hoc networks (VANETs) are a subclass of mobile ad hoc networks (MANETs). However, VANETs present characteristics that are noticeably different from many generic MANETs. VANETs are considered as a pledging style for future Intelligent Transportation System (ITS). They possess no static infrastructure. Consequently, they expect vehicles to deliver network functionality [1]. VANETs are extricated from other classes of ad hoc networks through their hybrid network architectures, node movement features, and non-traditional new application settings. As a result, VANETs call for numerous unique research challenges. Furthermore, the design of an effective routing protocol for VANETs is undoubtedly vital [2]. Vehicular ad hoc networks can provide a wide variety of services. However, they are subject to a number of challenges including network architecture, protocols for physical and link layers, and routing algorithms [3]. Vehicular ad hoc networks will not only make safety and lifesaving applications a reality, but will also turn out to be a formidable communication instrument for their users [4].

With the increasing number of various attacks on wireless networks, security becomes a critical challenge for VANETs and will continue to be so even after it is widely implemented. VANETs are subject to many attacks including denial of service, Sybil, hardware, software, sinkhole, impersonation, and flooding attacks. To ensure effective security, the security requirements; availability, authentication, integrity, confidentiality, and non-repudiation must be satisfied.

Considerable work on VANETs security has been pursued to ensure the above mentioned security requirements are met. Most of this work adopted cryptology. Symmetric and, asymmetric cryptology, and tamper resistance hardware were suggested. For some authors, cryptographic certificates were an option. Other authors investigated various threats, particularly threats related to security requirements, and created various security protocols. Standardization related to approaches of furnishing security services and protecting driver's privacy were analyzed. Gillani et al. [5] examined several aspects of VANETs security including security threats, challenges in providing security in VANETs environment, security requirements, and attributes of security solutions. The need for robust VANET networks is obviously related to their security and privacy characteristics. Various types of security problems and challenges of VANET, and a set of solutions to solve these challenges and problems have been analyzed and discussed in [6]. Al-Kahtani [7] stressed that designing security mechanisms to authenticate and validate transmitted messages between vehicles, and remove intruders from the network are substantially critical in VANETs. The author also reported several existing and possible security attacks and techniques to enhance the security of VANETs. Security and privacy are obligatory in vehicular communications for successful acknowledgment and utilization of VANET technology. Every vehicular application must be meticulously tested for security before it is

 ISBN: 978-1-61208-411-4

implemented in the real world. Simulation tools have proved to be very effective for such testing [8]. The security of VANET has mostly inspired the current research efforts. Thorough solutions to safeguard the vehicular ad hoc networks against adversaries and attackers still need to be developed to arrive at an adequate level for both the driver and manufacturer to achieve safety of drivers and security of applications and infotainment [9]. Details of further attempts to secure VANETs and its applications could be found in [10]-[17].

Commercial advertising via vehicular ad hoc networks (VANETs) is a promising application. It allows organizations to target drivers and passengers with the aim of promoting their products and services that can possibly solve a problem in their lives. Advertising through VANETs will get the word out rapidly and more visibly to customers. Customers in a vehicle would have the opportunity to listen to or watch ads that serve their needs. Such advertising can compete with TV ads due to the fact that many audiences ignore most of the ad breaks on TV or get/do something else during those breaks.

The growth in market prospects and potentials necessitates further research on mobile marketing, such as mobile advertisement. Mobile advertisements intermingle with customers on one-to-one basis via messages through the use of mobile devices [18]. Wireless technology has initiated new channels of marketing communication and innovation of advertisement media, such as the mobile advertisement platform. Mobile advertisement relies on the use of wireless networks to dispense information about products to consumers in a localized, specialized and customized manner [19]. People making use of modern wireless technology are more likely to consider mobile networks as their daily entertainment device than watching TV and possibly reading newspapers [20], [21]. Advertisement with mobile networks can highly target customers who will find reading or watching advertisement through mobile network more enjoyable and valuable [22]. These reasons provide mobile marketing with an effective means for advertisers to directly reach out for their potential consumers more effectively [23].

A secure incentive framework for commercial ad dissemination in VANETs was introduced by Li et al. [24]. The presented approach relied on public key infrastructure to provide secure incentives for cooperating nodes. The framework relied on vehicles receiving ads and disseminating them to other vehicles. The possibility of cheating by some drivers who can send receipts without even examining the ad is very high. Multiple receipts for the same ad by the same vehicle will go undetected. Furthermore, the authors used public keys to encrypt ads. Public keys are inefficient for encrypting large messages. Zhu [25] introduced the security requirements for service-oriented vehicular networks. Commercial content distribution is one of these services. Secure payments are possibly needed for some commercial application in VANETs [26].

This paper proposes a secure commercial ad broadcasting via VANETs. The security architecture for the dissemination of the ad is integrated with the vehicular ad hoc network security architecture proposed by the authors in [27]. Various cryptology protocols will be presented, and the security of incentives will be implemented. The approach followed in this paper also treats possible cheating including drivers passing the ad code to their friends to claim incentives without reading/watching the ad, and requesting multiple incentives for the same ad by the same vehicle. Section II presents the ad broadcasting architecture. Section III demonstrates public key certificates distribution. Organization to ad administration communication and state-level RSU to ad administration communication are introduced in Sections IV and V respectively. Section VI provides the state-level RSU to county-level RSU communication. Sections VII, VIII, and IX describe county-level RSU to city-level RSU communication, city-level RSU to street-level RSU communication, and street-level RSU to vehicle communication respectively. The paper is concluded in Section X.

II. AD BROADCASTING SECURITY ARCHITECTURE

The ad broadcasting architecture is superimposed on the multi-level security architecture for vehicular ad hoc networks introduced by the authors in [27]. It is re-drawn to serve the purpose of the ad broadcasting security architecture. The ad issuing organization (AORG), ad authority (AUTH), and the ad administration authority (ADMN) are added to it. Fig. 1 illustrates the ad broadcasting security architecture that will guide the security protocols. The right hand side of this figure represents the security architecture for vehicular ad hoc networks mentioned above. This is augmented by the left hand side part to include secure ad dissemination. Note that apart from the box for RSU_C, there supposed to be a number of boxes for all levels on the right hand side of Fig. 1 to indicate many states, counties, and cities.

The roadside units (RSU_S) are organized in a hierarchal fashion. The root of this tree is the Country-Level RSU (RSU_C). State-Level RSUs (RSU_S) are connected to the (RSU_C). Likewise, County-Level RSUs (RSU_{CO}), City-Level RSUs (RSU_{CI}), and Street-Level roadside units (RSU_{ST}) are connected to RSU_S, RSU_{CO}, and (RSU_{CI}) respectively. Each Street-Level RSU is in charge of all vehicles passing through the street (or portion of the street for long streets) under its authority. RSUs within the same level can only communicate through the parent node they belong to. The computing power and capacity of RSU increases when moving upwards through the tree. Detailed information about vehicles is stored at the State-Level RSU (RSU_S). With the exception of RSU_C, there are many RSU_S, RSU_{CO}, RSU_{CI}, and RSU_{ST} at their levels. However, only one RSU of each is shown in Fig. 1.

The ad authority (AUTH) is in charge of issuing certificates to the ad issuing organizations (companies interested in promoting their products or services), the ad administration authority (ADMN), and the State-Level RSU (RSU_S). For each state, there is only one ad authority and one ad administration authority. In other words, one AUTH and one ADMIN will manage ads for the cities within the state.

 ISBN: 978-1-61208-411-4

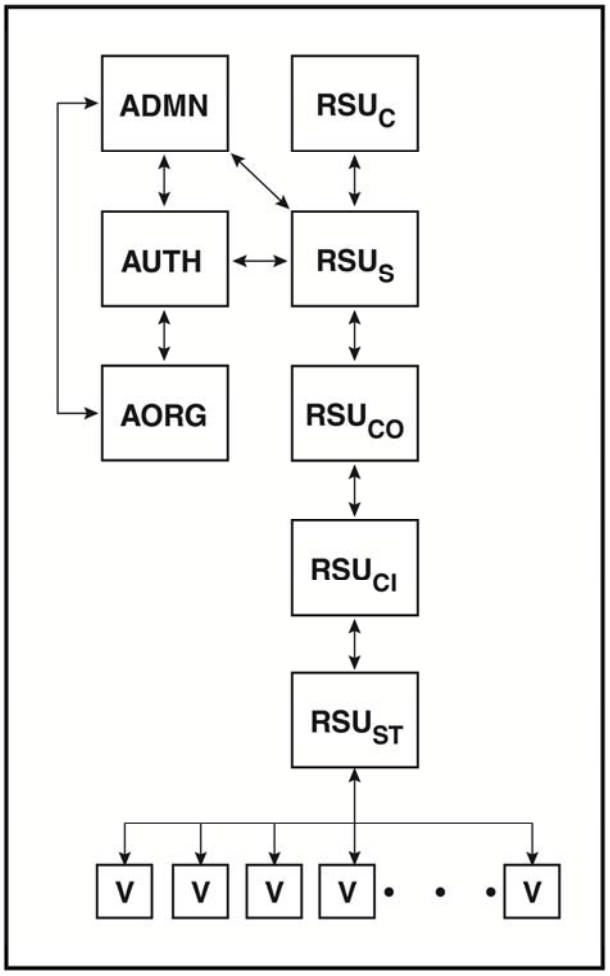

Figure 1. Ad broadcasting security architecture

The communication between RSU_{CT} and RSU_{ST}, and RSU_{ST} and vehicles follows the security protocols used in [27]. In these protocols, RSUs at each level create their own private and public keys and exchange their public keys. Each parent RSU creates a master key. The master key and the ID of the parent node are encrypted with the public keys of the children nodes and forwarded to them. At this point all nodes have a shared master key with their parent nodes. The public and private keys are then discarded. Each parent node creates a session key and encrypts it with the master key. Once the session keys are obtained, messages can be exchanged. To send any message between a child and a parent, the hash function of the message is appended to the message and both are encrypted with the session key. Note that Street-Level RSU (RSU_{ST}) creates public key certificates for all vehicles entering its street. This will be used by vehicles when broadcasting messages to other vehicles.

The ad material is sent by the ad issuing organizations (AORG) to the ad administration authority (ADMN) together with the ad ID (AID) and ad period (ADP). ADMN checks the ad against the legal, social, and ethical constraints. It later negotiates the cost with the ad issuing company. The cost includes what the administration authority charges, the State-Level RSU charges, and the coupon amount/number of points that will be allocated to vehicles reading or watching the ad. The State-Level charges include the amounts allocated to itself, the county, city, and Street-Level RSUs. Every ad contains an ad code (ADC), which will be used for incentives purposes. Upon completion of this part of the protocol, the ad material is forwarded by ADMN to the State-Level (RSUs). The Street-Level RSUs will receive the ad material from its parent City-Level node (RSU_{CI}) and securely broadcast it to the vehicles within its street authority. Ads (clip or text and images) are mainly large messages. Public key cryptology tends to be very slow and inefficient when dealing with such large messages. Therefore, the ad administration authority (ADMN) will create two session keys, K_{S1} and K_{S2}, which will be shared with AORG and RSU_S respectively. These two keys will be valid until the ad is completely administered. This will occur when ADMN receives the charges from AORG.

The Street-Level RSUs (RSU_{ST}) ensures via secure communication that vehicles within its responsibility have read/watched the ad when they receive the ad code (ADC). This can only be obtained when reaching the end of the ad. Information regarding the participating vehicles will be forwarded to the parent RSU_{CI} for charging purposes. At the expiration date of the ad, the City-Level RSU will send info about all the participating vehicles to the RSU_S via the RSU_{CO}. The RSU_S will send the charging information for all the cities within that state to the ad administration authority (ADMN) for charging purposes. Any incentive system for participating vehicles can be utilized provided it is secure. However, in this paper, coupon and points redemption will be used. RSU_S, RSU_{CO}, RSU_{CT} and RSU_{ST} will receive dollar amounts.

To better understand the protocols, the participating parties are introduced in Table 1. Table 2 depicts the protocols notations and symbols used in the protocols.

III. PUBLIC KEY CERTIFICATES DISTRIBUTION

The Ad Administration Authority (ADMN), the Ad Issuing Organizations (AORG), and the State-Level RSU (RSU_S) request their public key certificates from the Ad Authority (AUTH). The public key of the Ad Authority, PU_{AUTH} is made known to all these parties above. The public key, ID, and a nonce for each party are encrypted with the public key of the Ad Authority and forwarded to it.

$RSU_S \rightarrow$ AUTH: $E[PU_{AUTH}, (PU_S \| ID_S \| N_S)]$
ADMN $\rightarrow$ AUTH: $E[PU_{AUTH}, (PU_{ADMN} \| ID_{ADMN} \| N_{ADMN})]$
AORG $\rightarrow$ AUTH: $E[PU_{AUTH}, (PU_{AORG} \| ID_{AORG} \| N_{AORG})]$

The Ad Authority decrypts each message and creates public key certificates for the three parties and attaches the original nonce encrypted with the party's public key.

$CR_S = E[PR_{AUTH}, (PU_S \| ID_{US} \| T_1 \| T_2)]$
$CR_{ADMN} = E[PR_{AUTH}, (PU_{ADMN} \| ID_{ADMN} \| T_1 \| T_2)]$
$CR_{AORG} = E[PR_{AUTH}, (PU_{AORG} \| ID_{AORG} \| T_1 \| T_2)]$

 ISBN: 978-1-61208-411-4

AUTH → RSU_S: CR_S || $E(PU_S, N_S)$
AUTH → ADMN: CR_{ADMN} || $E(PU_{ADMN}, N_{ADMN})$
AUTH → AORG: CR_{AORG} || $E(PU_{AORG}, N_{AORG})$

The certificates include a timestamp, T_1, and a certificate validity period (expiration date), T_2. The original nonce are encrypted with the public key of the party and attached for further assurance that the message is not a replay.

TABLE 1. PARTICIPATING PARTIES

Symbol	Role
AUTH	Ad Authority
ADMN	Ad Administration Authority
AORG	Ad Issuing Organization
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

TABLE 2. 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, K_S	Symmetric Master and session Keys
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
||	Concatenation
E	Encrypt
→	Send to
H(M)	Hash of message M
T_1	Issue time
T_2	Expiration time
AID	Ad ID
ADP	Ad Period
ADC	Ad Code
C/P	Coupon amount/Number of points
ID_V, ID_{VA}	Real and Anonymous ID of vehicle
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_S	ID of State-Level RSU
ID_{AORG}	ID of Ad Issuing Organization
ID_{ADMN}	ID of Ad Administration Authority
PU_{AORG}	Public key of AORG
PR_{AORG}	Private key of AORG
PU_{ADMN}	Public key of ADMN
PR_{ADMN}	Private key of ADMN
T_{AORG}	Time stamp added by AROG
N_i	Nonce, i = S, AROG, ADMN
K_{S1}	Session key shared by ADMN and AORG
K_{S2}	Session key shared by ADMN and RSU_S

IV. ORGANIZATION-TO-AD ADMINISTRATION COMMUNICATION

This sub-protocol involves the ad approval and costing, and securely handling incentives.

A. Ad Approval and Costing

During this communication, the ad will be either accepted or rejected. In addition, the charges will be set. These charges will include the incentives which will be paid to vehicles. These will be taken care of later in this paper. The integrity of all messages is important.

The Ad Issuing Organization (AORG) and Ad Administration Authority (ADMIN) exchange certificates, validate the currency of each other's certificate, and extract the public key and ID of the other party. ADMN creates a session key, K_{S1}, to be shared with AORG. This session key and the ID of ADMN are encrypted with PR_{ADMN} and then with PU_{AORG} and forwarded to AORG. After carrying out the needed decryptions to get K_{S1} and verifying the sender, AORG sends a request to ADMN for ad dissemination. The request includes the ad ID (AID), the ad as a clip or text (AD), ad period (ADP), hash of the ad, H(AD), AORG's ID, and a timestamp, T_{AORG}. AD and H(AD) are encrypted with K_{S1}. The rest are encrypted with AORG's private key and then with the public key of ADMN.

$Z = E[K_{S1}, AD \,||\, H(AD)]$
$X = AID \,||\, ID_{AORG} \,||\, ADP \,||\, T_{AORG}$
AORG → ADMN: $E[PU_{ADMN}, E(PR_{AORG}, X)] \,||\, Z$

ADMN will first decrypt the first part of the message using its private key and then with the public key of AORG. It then decrypt Z with K_{S1} to get AD and H(AD), calculates the hash code of AD and compare it with H(AD). It will also check the timestamp to ensure the message's currency. Having verified the hash and timestamp, ADMN will examine the Ad to see if is not violating any legal, social, or ethical requirements. It then, extracts the Ad Code (ADC), which can only be obtained when the end of the ad is reached. The ADC will be used for incentive purposes in the future. ADMN also uses it as an assurance to AORG that the ad has been processed by ADMN. Finally, a message containing AID, ADC, ID, Reject/Accept (R/A), and Ad Dissemination Cost (ACOST) will be encrypted with AORG's public key PU_{AORG}. This implies one of the messages below will be sent depending on whether the ad is accepted or rejected. Let $Y = AID \,||\, ADC \,||\, ID_{AORG} \,||\, ID_{ADMN}$.

ADMN → AORG: $E[PU_{AORG}, A \,||\, Y \,||\, ACOST]$ or
ADMN → AORG: $E[PU_{AORG}, R \,||\, Y]$

If the ad is rejected, no further communication for that ad will be followed. Otherwise, AORG decrypts the message and verifies AID and ADC. It either agrees or disagrees with the cost. ID_{AORG} and ID_{ADMN} are used as assurance components. If AORG agrees, it sends the following message to ADMN:

 ISBN: 978-1-61208-411-4

AORG → ADMN: E[PU_{ADMN}, (PR_{AORG}, Y || ACOST || AGREE)]

Upon receiving this message and decrypting it, ADMN will verify the agreement and the stated cost. Once again, the two IDs, ID_{AORG} and ID_{ADMN}, are used for assurance purposes.

B. Secure Incentives Handling

ADMN adds the total amounts for the coupons/points received from the RSU_S to its charges and the charges of the state. This represents the total amount charged for that ad.

M = ID_{AORG} || ID_{ADMN} || ADC || AID || TOTAL
ADMN → AORG: E[PU_{AORG}, E(PR_{ADMN}, M || H(M)]

AORG will subtract ACOST from TOTAL to get the total incentives for vehicles. It will then divide the result by the coupon value or number of points allocated to this ad to find out how many vehicles read/watched the ad. Having done that, TOTAL will be transferred to ADMN using any secure approach.

V. State-Level RSU-to-AD Administration Communication

This section introduces the ad material and incentive forwarding sub-protocols.

A. Ad Material Forwarding

The Ad Administration Authority forwards the ad material to the State-Level RSU. In addition, ADMN sends the monetary amount to the RSU_S. It will either accept the ad or return to ADMN in case of any problem. Both ADMN and RSU_S swap over certificates. If the certificate is valid, the ID and public keys are retrieved. ADMN creates a session key, K_{S2}, to be shared with RSU_S. ADMN then forms a message containing ID_{ADMN}, the ad ID (AID), ad code (ADC), ad period (ADP), ID_{AORG}, and coupon amount or number of points (C/P) all encrypted with PR_{ADMN} first and then with PU_S. It then attaches AD || H(AD) after encrypting them with K_{S2}. The resulting message is sent to RSU_S.

Z = E[K_{S2}, AD || H(AD)]
X = ID_{ADMN} || AID || ADC || ADP || ID_{AORG} || C/P
ADMN → RSU_S: E[PU_S, E(PR_{ADMN}, X)] || Z

RSU_S performs the needed decryptions, verifies the hash code of the ad equals H(AD), ensures the ad code is the same as ADC and ID_{ADMN} is a valid ID. It also validates the ad period to make sure it is not an expired ad. If there is an issue with all these checks, a message containing the problem will be sent. Examples include "Invalid ID" and "Mismatched ADCs." The world "PROBLEM" will be used. If there is no problem, "VALID" will be attached to the message.

Y = ID_S || ADC || AID
RSU_S → ADMN: E(PU_{ADMN}, Y || PROBLEM)
RSU_S → ADMN: E(PU_{ADMN}, Y || VALID)

B. Incentive Forwarding

The responsibility of the RSU_S in this communication is to forward a list of vehicles to the ADMN for incentives purposes. The information about vehicles involved in the ad will be received from the County-Level RSUs (RSU_{CO}).

At the expiration date of an ad (ADP), the RSU_S first ensures that no vehicle within the state will get multiple incentives for the same ad. Having done that, the State-Level RSU sends a message, M, containing the name of the driver, ID_V, address (ADR), ADC, AID, C/P, and H(M) encrypted with PR_S and then with ADMN's public key.

M= ID_S || NAME || ADR || ADC || ID_V || AID || ADC || C/P
RSU_S → ADMN: E[PU_{ADMN}, E(PR_S, M || H(M))]

ADMIN decrypts this message and verifies there are no duplicate incentives for the same ad for the ID_V that was received. The total incentives (coupon amount or number of points) are then updated. This will be done for all the different ads. At the end of the month, a coupon or total number of points will be mailed to the vehicle's driver.

VI. State-Level RSU-to-County-Level RSU Communication

The State-Level RSU maintains vehicle database. It transmits the ad materials to all counties and receives all the anonymous IDs used for each vehicle at all counties, and the incentive details for all vehicles. It uses the received information to update its database of vehicles. In US, the minimum number of counties is 3 and the maximum is 254. Large counties will have more streets. This will demand more street-level RSUs (RSU_{ST}) and more advanced equipment's to improve performance. The stretch of a street assigned to an RSU will designate the maximum number of vehicles under the responsibility of that RSU. Therefore, the limit on the number of vehicles is only determined by the capacity of the allocated street section.

The state forwards the ad material continued in M below after encrypting it with the session key, K_{SC}, shared with RSU_{CO} to the County-Level RSU:

M= ID_{CO} || ID_S || AID || ADC || AD || H(AD) || ADP || C/P
RSU_S → RST_{CO}: E(K_{SC}, M|| H(M))

The RSU_S receives the ID_V and ID_{VA} for all vehicles from all counties. The records in the State-Level database will be updated for each vehicle. Note, ID_{ST} indicates where the ID_{VA} was issued. In other words, it is the ID of street accommodating the vehicle at that time.

M = ID_{CO} || ID_S || ID_{ST} || ID_V || ID_{VA}
RSU_{CO} → RST_S: E(K_{SC}, M|| H(M))

 ISBN: 978-1-61208-411-4

Each county will send the incentives information for all vehicles within its cities after verifying no duplications exist for a vehicle among its cities with regards to the same ad.

$M = ID_{VA} || ID_{CO} || AID || ADC || ADP || C/P$
$RSU_{CO} \rightarrow RST_S: E(K_{SC}, M|| H(M))$

VII. County-Level RSU-to-City-Level RSU Communication

In this communication sub-protocol, the ad material dispatching, storing vehicle information and incentive handling will be dealt with.

A. Ad Material Dispatching

The RSU_{CO} sends the ad material to the City-Level RSUs in addition to its ID and the ID of each RSU_{CI} within that county.

$M= ID_{CI} || ID_{CO} || AID || ADC || AD || H(AD) || ADP || C/P$
$RSU_{CO} \rightarrow RST_{CI}: E(K_{SCO}, M|| H(M))$

K_{SCO} is the shared session key between RSU_{CO} and RSU_{CI}. RSU_{CI} will decrypt this message, verify the sender, check the integrity of the ad, and obtain the ad material.

B. Storing Vehicle Information

The County-Level RSU (RSU_{CO}) receives all vehicle IDs with all their ID_{VA}'s, and the location where ID was issued. This location is in fact the Street-Level RSU's ID. The RSU_{CI} sends the RSU_{CO} the following information about each vehicle at each location (street):

$M = ID_{CO} || ID_{CT} || ID_{ST} || ID_V || ID_{VA}$
$RSU_{CI} \rightarrow RST_{CO}: E(K_{SCO}, M|| H(M))$

Here, K_{SCO} is the session key shared between RSU_{CI} and RSU_{CO}. There could normally be a number of such messages for the same vehicle, but for different ads. The RSU_{CO} will store this information together with that received from the State-Level RSU as mentioned above in its database. This history information will be beneficial for law enforcement authority to trace a vehicle if a need arises.

C. Incentive Handling

Having verified there are no multiple incentives for the same ad, the RSU_{CI} sends the message $E(K_{SCO}, M|| H(M))$ to the RSU_{CO} at the expiration of the ad.

$M = ID_{CO} || ID_{CI} || ID_V || ID_{VA} || AID || ADC || ADP || C/P$
$RSU_{CI} \rightarrow RST_{CO}: E(K_{SCO}, M|| H(M))$

After decrypting the message, verifying the sender, and validating the ad material introduced in M above, the County-Level RSU checks that there are no multiple vehicle incentive requests by the same vehicle for the same ad among all the cities belonging to that county.

VIII. City-Level RSU-to-Street-Level RSU Communication

The City-Level RSU, RSU_{CI}, receives vehicles IDs and all anonymous vehicle IDs from the Street-Level RSU. It also receives the needed ad information for incentive purposes. RSU_{CI} sends the ad material to all Street-Level RSUs within the city.

A. Vehicles ID Storing

Each RSU_{ST} send a list of real IDs and anonymous IDs for each vehicle passing through that street. As mentioned in Section II, RSUs communicate using a shared session key. Therefore, the list of IDs and the hash code of the list is encrypted with the shared session key for Street-Level and City-Level RSUs (K_{SCI})

$M = ID_{ST} || ID_{CI} || ID_V || ID_{VA}$
$RSU_{ST} \rightarrow RST_{CI}: E(K_{SCI}, M|| H(M))$

The RST_{CI} updates its database to add all new ID_{VA} issued for the vehicle during that period.

B. Sending Ad Material

The RST_{CI} sends a message, M, composed of its ID, the Street-Level ID, AID, ADC, ADP, C/P, and AD. The hash code of M is also attached.

$M = ID_{ST} || ID_{CI} || AID || ADC || ADP || AD || H(AD) || C/P$
$RSU_{CI} \rightarrow RST_{ST}: E(K_{SCI}, M|| H(M))$

The Street-Level RSU confirms the sender and the message integrity. It then saves AID, ADC, ADP, C/P, and AD.

C. Incentive Forwarding

The Street-Level RSU sends its RSU_{CI} incentive messages for each participating vehicle:

$M = ID_{VA} || ID_{ST} || AID || ADC || ADP || C/P$
$RSU_{ST} \rightarrow RST_{CI}: E(K_{SCI}, M|| H(M))$

The City-Level RSU checks that there are no duplications for any ad's incentives within its streets. In other words, because RSU_{CI} has the incentive information from all its streets, it makes sure no vehicle has sent multiple ADC for the same ad whether within the same street (driving through it more than once) or at various streets within the city. At the end, each ad participating vehicle will have just one incentive for an ad. Definitely, multiple incentives for different ads are acceptable.

IX. Street-Level RSU-to-Vehicle Communication

The Street-Level RSU, RSU_{ST}, receives the real ID of the vehicle, ID_V, when entering its zone, and provides its public key, PU_{ST}, to that vehicle. The RSU_{ST} uses a three-measurement technique [6] to create an anonymous ID, ID_{VA}, for the vehicle. Each vehicle will create its own public and

 ISBN: 978-1-61208-411-4

private keys (PU_V, PR_V), and forwards its public key to its RSU_{ST}.

RSU_{ST} creates a secret label, L, for each vehicle entering its zone. It creates a random key, K_L, and encrypts the ad ID (AID) and ID_{VA} with it. In other words, $L = E(K_L, AID \| ID_{VA})$. K_L is not shared with the vehicle. It will only be used once for each ad to control cheating. Without this label, vehicles can cheat by sending the ADC to other vehicles within the street, or another street, possibly in another city. With the absence of such a label, vehicles receiving the ADC can submit the required details without reading/ watching the ad and to earn incentives. L is encrypted with the public key of the vehicle and forwarded to it. Vehicles requesting incentives should attach L to other incentive requirements.

$RSU_{ST} \rightarrow V: E(PU_V, L)$

RSU_{ST} sends the ad materials to the vehicle. It appends the ad ID (AID), ID_{VA}, C/P, the ID of the Street-Level RSU, ID_{ST}, AD, and the hash code of the ad, H(AD) together to get the message X. The hash function is used to ensure the integrity of the ad. RSU_{ST} relies on broadcasting messages. To achieve broadcasting, the RSU_{ST} selects a random key, K_r, to encrypt X. It then encrypts K_r with the public key, PU_V, of each vehicle. Finally, the ID of the vehicle is attached to both encrypted messages and broadcasted to all vehicles in the zone.

$X = ID_{VA} \| AID \| ID_{ST} \| AD \| H(AD) \| C/P$
$RSU_{ST} \rightarrow V: ID_{VA} \| E(PU_V, K_r) \| (K_r, X)$

Recognizing their IDs, vehicles will decrypt with their public key PU_V first to get K_r, and then with K_r to get the message X. The vehicle will verify the sender. It then ensures the message is integral. Later, the vehicle's driver will decide if he/she is interested in the ad based on the value of C/P. To be eligible for incentives, the driver must watch the clip to the end, or read the text of the ad to the end in order to extract the ad code (ADC). The ad code is the proof that will be used for providing incentives. If the ad is followed to the end, the vehicle sends a message containing the ADC, AID, anonymous ID of the vehicle, ID of RSU_{ST}, and the label (L) all encrypted first with the vehicle's private key and then with the public key of the RSU_{ST}.

$V \rightarrow RSU_{ST}: E[PU_{ST}, E(PR_V, AID \| ID_{VA} \| ID_{ST} \| ADC \| L)]$

After carrying out the decryptions and recognizing the sender, the RSU_{ST} verifies the received ADC matches the ADC of one of the ads, and ensures the AID in the message is the same as the AID of that ad. Finally, it verifies the ad period (ADP), which was forwarded to it by the RSU_{CI} to ensure the ad is still valid. If there is any problem, the received message is ignored. Finally, verification against cheating is carried out by decrypting L with K_L and checking that AID and ID_{VA} of the label match the received AID and ID_{VA}. If verification is positive, an acknowledgment (ACK) is sent to the vehicle. The Keys, K_L and K_r, will be discarded once the expiration date of the ad in question is reached.

$RSU_{ST} \rightarrow V: E[PU_V, E(PR_{ST}, AID \| ID_{VA} \| ID_{ST} \| ACK)]$

X. CONCLUSION

The advent of vehicular ad hoc networks (VANETs) widely opened the door for various commercial applications. An important application is the commercial ad broadcasting. For such application to be successful and effective, dissemination of ad should be carried out in a secure manner to protect various communications. Securing the ad dissemination without providing incentives will render the application ineffective as many drivers will just ignore the ads. This paper introduced a secure architecture, which is implemented by a secure protocol to protect communications and incentives. The protocol also prevented dishonest drivers, if any, from cheating.

This paper adopts coupon and points redemption for incentive purposes. The management of incentives including selecting the incentive type and dealing with inappropriate behavior by vehicles is beyond the scope of this paper. This is left to the states to decide as it involves legal, social, and accounting factors.

REFERENCES

[1] S. Yousefi, M. S. Mousavi, and M. Fathy, "Vehicular Ad Hoc Networks (VANETs): Challenges and Perspectives," *in Proc. the 6th International Conference on ITS Telecommunications*, Chengdu, pp. 761-766, 2006.

[2] F. Li and Y. Wang, "Routing in Vehicular Ad Hoc Networks: A Survey," *IEEE Vehicular Technology Magazine*, vol. 2, no. 2, pp. 12-22, 2007.

[3] Y. Liu, J. Bi, and J. Yang, "Research on Vehicular Ad Hoc Networks," in Proc. the 21st Annual International Conference on Chinese Control and Decision (CCDC'09), Guilin, pp. 4466-4471, 2009.

[4] H. Kabir, "Research Issues on Vehicular Ad hoc Network," *International Journal of Engineering Trends and Technology (IJETT)*, vol. 6, no. 4, pp. 174-179, 2013.

[5] S. Gillani, F. Shahzad, A. Qayyum, and R. Mehmood, "A Survey on Security in Vehicular Ad Hoc Networks," *Communication Technologies for Vehicles, Lecture Notes in Computer Science*, vol. 7865, pp 59-74, 2013.

[6] G. Samara, W. Al-Salihy, and R. Sures, "Security Analysis of Vehicular Ad Hoc Nerworks (VANET)," *in Proc. the Second International Conference on Network Applications Protocols and Services (NETAPPS)*, Kedah, pp. 55-60, 2010.

[7] M. S. Al-Kahtani, "Survey on Security Attacks in Vehicular Ad hoc Networks (VANETs)," *in Proc. the 6th International Conference on Signal Processing and Communication Systems (ICSPCS)*, Gold Coast, QLD, pp. 1-9, 2012.

[8] M. K. Jhariya, P. K. Shukla, and R. Barskhar, "Assessment of Different Attacks and Security Schemes in Vehicular Ad-hoc Network," *International Journal of Computer Applications (IJCA)*, vol. 98, no. 22, pp. 24-30, 2014.

[9] M. K. Nasir, D. Hossain, S. Hossain, M. Hasan, and B. Ali, "Security Challenges and Implementation Mechanism for Vehicular Ad Hoc Network," *International Journal of Scientific & Technology Research (IJSTR)*, vol. 2, no. 4, pp. 156-161, 2013.

 ISBN: 978-1-61208-411-4

[10] A. Agrawal, A. Garg, N. Chaudhiri, S. Gupta, D. Pandey, and T. Roy, "Security on Vehicular Ad Hoc Networks (VANET): A Review," *International Journal of Emerging Technology and Advanced Engineering (IJETAE)*, vol. 3, no. 1, pp. 231-235, 2013.

[11] 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.

[12] 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.

[13] 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.

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

[15] M. Raya and J. Hubaux, "The Security of Vehicular Ad Hoc Networks," in *Proc. the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks*, pp. 11-21, 2005.

[16] F. Sabahi, "The Security of Vehicular Ad Hoc Networks," in Proc. the 3rd International Conference on Computational Intelligence, Communication Systems, and Networks, pp. 338-342, 2011.

[17] R. Shringar, M. Kumar, and N. Singh, "Security Challenges, Issues and Their Solutions for VANET," *International Journal of Network Security & Its Applications (IJNSA)*, vol. 5, no. 5, pp. 95-105, 2013.

[18] U. M. Z. Usman and Z. B. Mohammed, "The Impact of Mobile Advertisement and Communication on Customer Relationship Management (CRM)," *in Proc. the 2012 International Conference on Economics, Business and Marketing Management*, Singapore, pp. 118-212, 2012.

[19] K. Siau and Z. Shen, "Building Customer Trust in Mobile Commerce," *Communications of the ACM*, vol. 46, no. 4, pp. 91-94, 2003.

[20] S. J. Barnes, "Wireless Digital Advertising: Nature and Implications," *International Journal of Advertising*, vol. 21, pp. 399-419, 2002.

[21] A. L. Gilbert and J. D. Kendall, "A Marketing Model for Mobile Wireless Services," *in Proc. the 36th Hawaii International Conference on System Sciences (HICSS-36)*, Hawaii, pp. 89b, 2003.

[22] S. J. Barnes and E. Scornavacca, "Mobile Marketing: The Role of Permission and Acceptance," *International Journal of Mobile Communication*, vol. 2, no. 2, pp. 128-139, 2004.

[23] P. Barwise and J. U. Farley, "The State of Interactive Marketing in Seven Countries: Interactive Marketing Comes of Age," *Journal of Interactive Marketing*, vol. 19, no. 3, pp. 67-80, 2005.

[24] S. Lee, G. Pan, J. Park, M. Gerla, and S. Lu, "Secure Incentives for Commercial Ad Dissemination in Vehicular Networks," in *Proc. the 13th Annual International Conerence on Mobile Computing and Networking*, pp. 150-159, 2007.

[25] H. Zhu, R. Lu, X. Shen, and X. Lin, "Security in Service-Oriented Vehicular Networks," *IEEE Wireless Communications*, pp. 16-22, 2009.

[26] 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.

[27] K. Daimi, M. Saed, and S. Bone, "A Multi-Level Security Architecture for Vehicular Ad Hoc Network," *in Proc. International Conference of Information Security and Internet Engineering (ICSIE'14)*, London, UK, pp. 440-455, 2014.

 ISBN: 978-1-61208-411-4