EURASIP Journal on Wireless Communications and Networking
a SpringerOpen Journal

RESEARCH Open Access

Secure protocols for data propagation and group communication in vehicular networks

Meng-Yen Hsieh[1*], Hua-Yi Lin[2], Chin-Feng Lai[3] and Kuan-Ching Li[1]

Abstract

Vehicular networks are organized with high-mobility vehicles, which are a challenge to key agreement and secured communication among vehicles; hence, efficient cryptography schemes for lightweight ciphers are essential. Many security schemes for vehicular networks particularly take the secure propagation of traffic-related information into account. Group communication is desirable in vehicular networks, while groups of friends drive the vehicles to travel together. In this study, it is applied an asymmetric key mechanism and a group-based Elliptic Curve cryptograph to authenticate data propagation as also to individually secure group communication. The data propagation includes a flooding delay mechanism, where each vehicle participant in the propagation calculates an individual delay for propagation. As groups of vehicles move on the roadway toward same destinations, two alternative schemes of group key agreement in vehicle-to-vehicle and vehicle-to-infrastructure modes are proposed to secure group communication among the vehicles. Security analysis results present that the proposed schemes can effectively prevent malicious vehicle from participating in vehicular communications. Evaluation results show that the propagation delay mechanism can effectively reduce broadcast collision, and the delay results of the group key agreement schemes are acceptable.

Keywords: vehicle, group communication, elliptic curve

1. Introduction

Secure data transmission in vehicle ad hoc networks (VANETs) has been an important issue. The disclosure environments with wireless connection are vulnerable to eavesdrop and spoofing; hence, a number of security researches in VANETs have been presented. Most of them have the same goal and vision to protect the vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications. Public key cryptography is always addressed as a foundation for VANET security requirements, since vehicles have enough capabilities, and be able to connect to the Internet through fixed stations. The propagation of traffic-related data such as traffic conditions, road safety, danger warnings, and vehicle's emergency braking is essential in order to keep safety for all vehicles moving on the roadway. In the real world, groups of friends could drive vehicles to travel together, so group communications are possible in VANETs. For the above reasons, the study focuses on the secure protocols for the traffic-related data propagation and group-based communication. The security issue for the propagation should be authentication replacing encryption cryptography in order to achieve fast broadcasting. Confidential communications are necessary, since the vehicles in a group always intent to share data solely among themselves. This study authenticates the propagation of traffic-related information in the V2V mode, while other vehicles can authenticate a disclosed propagation from a vehicle source using the asymmetric signature scheme. Structures of secure group communication are implemented in the V2V and V2I modes in order to overcome the high-frequency change in the vehicular topology. Vehicle groups apply the elliptic curve cryptography [1] to the group key agreement protocols.

Basically, a VANET is organized with heterogeneous connections, supporting inter-vehicle, vehicle-to-station, and inter-station communications. Inter-vehicle as V2V communication is unstable due to high-mobility vehicles on the roadway. Road-side stations (RSUs) are deployed

* Correspondence: mengyen@pu.edu.tw
[1]Department of Computer Science and Information Engineering, Providence University, Taichung, Taiwan
Full list of author information is available at the end of the article

on the roadside to assist vehicles in Internet connection and obtaining key-related materials. Most key materials for VANETs are mainly to safeguard the propagation information. A reliable propagation of traffic-related information is essential, so that vehicles can travel safely and keep the traffic flowing freely over the roadway. It is a challenge that a vehicle authenticates the incoming traffic notifications of vehicles next to each other using ad hoc key cryptography. Multi-hop routing in V2I mode is hard to achieve directly and timely significant traffic propagation between any two neighboring vehicles. In addition, the deployment of RSUs on each roadside to cover all moving vehicles is impossible. Real-time safety applications always achieve the purpose of accident avoidance and cooperative driving in VANETs. The data propagation in the V2V mode without a propagation schedule will induce the problems of communication collision and broadcast storms.

Public-key infrastructure (PKI) can protect vehicular communication using the public key cryptography. Vehicles have to apply for a valid key pair, certificated by trusted third party such as Certificate Authority (CA). In the V2I mode, vehicles connect to the PKI services through roadside RSUs, since RSUs always support wireless and wired techniques. Basically, one participant represented as a mobile vehicle or a fixed RSU should have an individual public/private key pair with the certificate for authentication, communication confidentiality, and integrity in VANETs. The asymmetric cryptography is not suitable to secure group communication, while one vehicle wants to transmit confidentially huge amount of data such as digital map-based information and multimedia to other vehicles in a group. Additionally, unstable V2V links cannot endure long periods of group communication. With the aid of RSUs in the V2I mode, the scattered vehicles can keep connections during a group communication session. Using a symmetric key to secured group communication improves the performance of delivering confidential data by comparing the data protected by all individual asymmetric-based keys of all participants.

Although vehicular computer has enough storage and computational capabilities without power-supply problems, light-weight, and strict security schemes are still essential to timely process data transmission in fast changes of VANET's topology. It is applied in this research the Elliptic Curve Diffie-Hellman (ECDH) to establish group keys to achieve secure group communication. ECDH belonging to the elliptic curve cryptography is a variant of the Diffie-Hellman (DH) key agreement scheme, allowing that two parties create a common secret key over an insecure channel. ECDH with 160-bit key lengths provides the same security level as the DH secret sharing protocol [2]. The original DH protocol with exponential operations needs a key of at least 1, 024 bits to achieve adequate security, and therefore includes additional computational overhead. For instance, vehicles A and B try to construct a shared key, and the public parameters (a prime and base point P as a well-known generator in DH, coefficients a and b, elliptic curve $y^2 = x^3 + ax + b$) must be set first. A or B must have an appropriate key pair for elliptic curve cryptography, comprising an ECC private key, k (a randomly selected integer) and public key Z ($Z = kP$). Both A and B have a key pair each. Then, A and B exchange their public keys, so that A and B calculate particularly a secret key, $GK_1 (= k_A Z_B = k_A k_B P)$ and $GK_2 (= K_B Z_A = k_B k_A P)$.

The remaining of this paper is organized as follows. A number of security issues in VANETs are described in Section 2, while Section 3 defines the communication scenarios and security requirements in a general vehicle architecture, where a propagation delay mechanism is also discussed. Section 4 details the key agreement schemes for group communication, followed by security and delay analyses in Section 5. Section 6 evaluates the performance of the proposed schemes in term of communication delay, and message loss ratio, and finally conclusions remarks and future work are presented in Section 7.

2. Related works

Vehicular communication has specific characteristics different from ad hoc communication, which characteristics may affect the security decisions that developers have to take. The features exhibited in the V2V and V2I modes contain the geographically constrained topology, directional movement, predictable mobility, sufficient power consumption, and route-based driving cooperation. Most of security issues in ad hoc networks are not entirely employed nor considered in vehicular communication.

Key pre-distribution schemes [3] relies on a probability of a large number of common keys among nodes that are not suitable for vehicles with open environments. Group-based security methods [4-9] usually outperform other methods in secure one-to-many transmission in terms of performance, scalability, and communication overhead. Lin et al. [4] addressed a security protocol, named Group Signature and Identity-based Signature (GSIS), to provide not only the requirements of security and privacy preserving, but also a group-based signature scheme to verify data transmission using a group's public key. The GSIS solves the mutual authentication problem for inter-vehicle group communication applications. A receiver accepting a group message can only confirm whether the sender is a member in the group, though not identifying the sender. A larger

computational overhead is generated in GSIS for maintaining a revocation list. The efficient traceability can be achieved without the storage overhead of managing a number of certificates at membership and tracing manger. A group key agreement method, called GDH [5], generalizes upon the well-known DH key exchange. A sender generates and delivers a list of partial keys replacing the whole shared key to a receiver over the public network, so the receiver uses its partial key to compute the group secret. In addition, the particular member of the group is charged with the task of building and distributing this list. For this reason, this study adopts the ECDH-based key agreement protocol to establish group keys for secured group communication among vehicles.

The position-based routing protocol [10] is suitable for vehicular communication, since the GSP system is always one of the basic equipments inside vehicles. Broustis et al. collected some routing schemes to vehicular communication, such as MDDV [11] and GSR [12]. Most of ad hoc routing schemes are inappropriate, since vehicle mobility and data forwarding are required with a direction. One vehicle in MDDV knows the road topology through a digital map, and its position can be found in the road network via a GPS device, as also the existence of their neighbors. MDDV is performed in two phases, namely forwarding and propagation phases, to exchange data between two vehicles and to address the questions about which vehicle can transmit, when to transmit, and when to store/drop messages. In the GSR protocol, a vehicle source predicts the position of a vehicle destination for communication. The source discovers the destination with a request once, and the destination responds its position and velocity back to the source. Based on the map information, the source transfers data to the destination after predicting its position. Consequently, GSR combines the position-based routing with the topological information. In this research, one head tries to deliver a key product to the next neighboring head in a global group using the above-mentioned routing protocol.

Zarki et al. [13] proposed a potential simple security infrastructure for vehicular communication on the highway, called DAHNI. The infrastructure turns vehicles to have the capabilities of location awareness, ad hoc routing, accessing to fixed base stations. The DAHNI provides the security issues including, at least, digital signature, time-stamping and sequencing, and a certification infrastructure. Data in DAHNI environment can be addressed with three types, namely, fixed spatial data, spatio-temporal data, and mobile data. Unfortunately, the DAHNI still presents problems to enable secure collection and dissemination of data timely. Cryptographic mechanisms of the identity-based encryption [14] and the proxy signature [15] are often adapted in V2I communication scenarios. Choi et al. [16] developed security mechanisms to protect vehicular communication. In the initial phase, vehicles and RSUs need to register their identities with the trust authority (TA) to capture their temporary key-related materials and private/public key pair of elliptic curve cryptography. One vehicle gains a pseudo-ID and essential parameters for implementing a temporal signature after authentication. BSU also receives confidentially a private key and proxy signature's parameters from the TA, after authentication. In any of V2I communication scenarios, vehicle and RSU have a mutual authentication in order to share a session key. The vehicle accepts a temporal anonymous certificate from the RSU, and the data transmission is protected by the session key. In V2V communication scenarios, each vehicle has a key pair and a certificate by the Elliptic Curve Digital Signature Architecture (ECDSA) [17]. Broadcasting traffic-related information signed by one vehicle with its private key can be authenticated by others with its disclosure valid certificate. This study applies the temporary asymmetric cryptography and signature to the proposed delay propagation and travel-based group communication scenarios. Each participant needs to hold a key pair based on the elliptic curve cryptography in advance. The procedures of authenticating the delay propagation and securing the agreement of group-based key are the main contributions in the study.

3. System model

A vehicle network under highways and rural roads as presented in this section not only complies with the security requirements, but also has some assumptions: (1) each vehicle is equipped with a wireless omni-directional antenna, GPS device, and digital map, (2) RSUs connect to the Internet through wired or wireless technologies, where two neighboring RSUs can communicate easily and quickly each other, (3) any two vehicles equipped with the dedicated short range communications (DSRC) protocol as IEEE 802.11p [18] has the same transmission range for inter-vehicle communication, (4) vehicles have event-based sensors to sense traffic and road statuses, and share a digital map such as Google Map, (5) each vehicle periodically sends a hello beacon to its neighborhood, and a beacon only contains the identity of the sender, and (6) RSUs on the roadway are managed by the servers on the Internet, and the servers connect to the trusted third party in the PKI services, as shown in Table 1.

Vehicles and RSUs are authenticated by trusted third party through the authentication procedure [16] at the initialization of a VANET. After identity authentication, each of them has a valid key pair and warranty/certificate.

Table 1 Notations in this study

Notations	Descriptions
E(Msgs, K)	The messages (Msgs) are encrypted by the key, K
R_i or RSU_i	The identity of a fixed station on the roadside
TP_{map}	A travel route, tp, in the Google MAP
PK/SK	An asymmetric key pair, issued by the trusted third party
$K_{i,j}$	A secret key between v_i and v_j
k/kP	A key pair, private/public keys in the Elliptic Curve Cryptography
VGK	A virtual group key among the vehicles in a V2I virtual group
GGK	A global group key among the vehicles in a V2V global group
GK_{set}, $GK_{set}P$	A ECDH-based key pair, generated by the trusted third party at a time, Tstamp, for a set of RSUs, $\{R_j\}$, on the route (tp) to service the vehicles, $\{v_i\}$, when they travel during the required trip period, ΔT. (i.e. set = hash(tp‖ΔT‖$\{R_j\}$‖$\{v_i\}$‖Tstamp))
$Cert_{vi}$	The certificate with a valid public key of v_i, issued by the trusted third party
GPS_{vi}	The GPS position (x, y) of v_i
v_i or V_i	The identity of vehicle i
$Event_k$	An event type of traffic-related information
TH	A head vehicle in a one-hop physical group, moving with a steady velocity (or approximately steady velocity)
$NList_x$	The latest identities of neighboring vehicles of Vehicle x
gk_x	A group key, shared between all members and their head, x, in a physical group
Sign(Msg, SK)	The digital signature of Msg, signed by the private key, SK
MAC(Msg, K)	The MAC code of Msg, encrypted with the secret key, K
$v$limit	The maximum speed limit on the roadway
R_T	The standard transmission range of a vehicle
$\Delta dpj_{s\to R}$	The projection distance from Sender(S) to Receiver (R) over the vector from the preceding sender of *Sender*
Δ^t_p	The delay time for the propagation of traffic-related information, defined in Equation (1)
Δ^t_A	The delay time for the role announcement of a TH, defined in Equation (2)
ΔT	The trip period required by groups of friends, when they travel together
Warn#	A warn message for the propagation of the traffic-related information
Req#	A request message for that a vehicle applies for a virtual group
Resp#	The response message corresponding to the Req#
Req@	A request message for that one TH tells its members to start the group key agreement process
Notify#	A notification message from a RSU to the vehicles contains the information, "the RSU set is ready for your trip"
"‖"	The meaning of "join"

3.1. Vehicular network architecture and communication scenarios

Two types of communication modes, V2V and V2I, in the vehicle network are depicted in Figure 1. The position of one vehicle can be tracked by the neighboring vehicles in a short period through the announced GPS and velocity information [19]. The GPS data of vehicles should not be disclosed in VANETs at will, since adversaries easily track vehicles according to their GPS and speed data. Vehicle applications require that vehicles share their position to each other to achieve the computation or routing purposes. In this study, vehicles need to announce their GPS data to participate the delay propagation of traffic-related information and becoming a head for the V2V group communication. The VANET performs the real-time propagation of the emergency information in the V2V mode, when a traffic-related event is happening. The vehicles in movement on a roadway with the reverse direction, different on where the event happened will not participate in the propagation, even if received the information; moreover, the vehicles moving from the front of the event location on the roadway will also not propagate the information. For example, Car 2 has a traffic event in Figure 1, while Cars 1 and 10 will not participate in the propagation of the traffic event in the network.

Group communication is desirable in vehicle networks, while groups of friends drive vehicles to travel together. They can establish a group to share data such as multimedia and map information, even if their vehicles are moving close or apart from each other on the same roadway. Their group communication scenarios are implemented through the V2V or V2I mode in this study. A physical group with the subset of the vehicles moving closely each other in the V2V mode must have a mobile head, and the head always moves at a steady velocity up or down a slight degree incline. The head has one-hop neighboring vehicles as its members in the physical

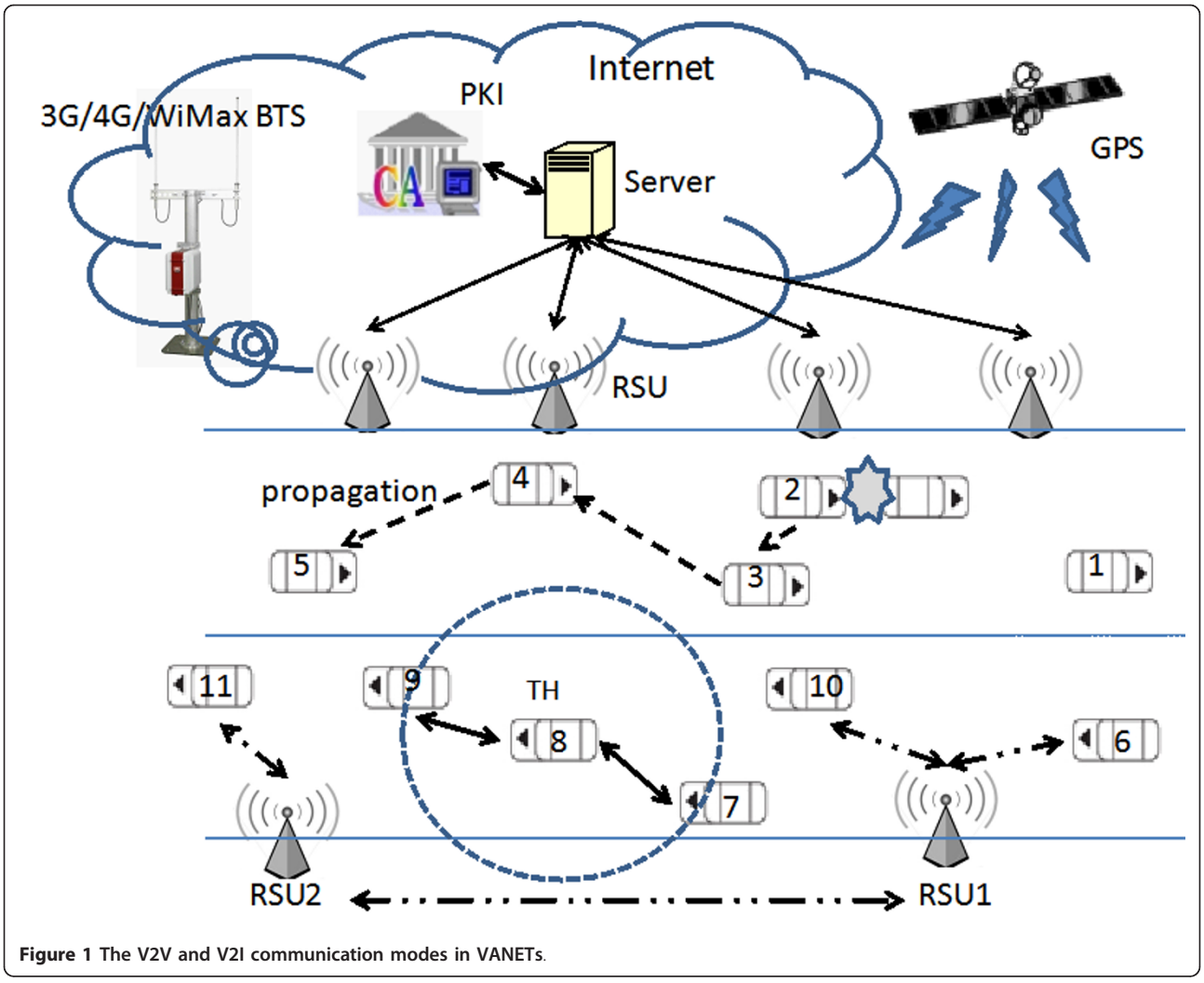

Figure 1 The V2V and V2I communication modes in VANETs.

group. All of the physical groups only organized by the scattered vehicles form a hierarchical group, denoted as a global group. In Figure 1, Cars 7-9 know about each other and could organize a physical group, and Car 8 is the head. The other alternative of group communication is to establish a virtual group in the V2I mode. The vehicles organize multiple localized groups with the RSUs on the roadside of the travel path. One of the RSUs organizes a localized group with the subset of the vehicles; hence, all of the localized groups form a virtual group. The RSUs participating in the virtual group are denoted as head avatars to service for all of the vehicles. Still in the Figure 1, cars 6, 10, and 11 on the same roadway organize a virtual group with RSU1 and RSU2. The set of RSUs on the roadside is managed by the trusted server on the Internet; hence, the server must connect the trusted party to maintain the security requirements of the RSUs. If a vehicle tries to apply for a virtual group, then the server will select the appropriate RSUs for it. Consequently, V2V-based global and V2I-based virtual groups are addressed, with different ways of selecting their heads. A global group is appropriate to the vehicles without connection gaps, and a virtual group is appropriate to them with high-frequency broken connections.

3.2. Propagation delay mechanism

A self-determined delay scheme is combined with the data propagation in order to avoid broadcast storms and propagation collision. A vehicle, denoted as r, receives a fresh traffic-related warning message from one of its front vehicles, denoted as s, and must delay a little time before propagation, denoted as Δt, given by the following equation:

$$\Delta t_p = \alpha \times \frac{(1 - ((\text{Speed}_s - \text{Speed}_r)/v\text{limit}))}{(\Delta dpj_{s \to r}/R_T)} \quad (1)$$

where, $v$limit is the maximum speed limit in the area where the vehicle moves, Speed_s and Speed_r are the

velocities of s and r, individually, smaller than $v$limit, R_T is the transmission range of vehicles, Δdpj is the projection distance from s to r over the vector from the preceding sender of s to s, and α is a value proportional to the number of the rear neighboring nodes of r. For example, v_{i+1} , v_{i+2} , and v_i are represented as s, r, and the preceding sender of s in Figure 2. Vehicle v_{i+2} must wait a self-determined delay time as calculated in Equation (1), once v_{i+2} receives the traffic-related information from v_{i+1} . Vehicle v_{i+2} will continue to propagate if receives no same message from its rear neighboring vehicles, after waiting the delay time. To calculate the projection distance, v_{i+2} needs to gain the GPS positions and the velocities of v_i and v_{i+1} . The sensitive data of v_i and v_{i+1} are attached to the propagation from v_i to v_{i+2} , and furthermore v_{i+2} has to verify the data. Section 4.1 details the procedure of propagating a warning message within an authentication format.

3.3. Security requirements

A traffic-related message always involves safety-critical information. Attackers could try to endanger road-traffic or node-vehicle safety by broadcasting incorrect or tamping messages. For the reason, the propagation generated from a source must achieve data integrity and identity authentication. The propagation of a traffic-related message is attached with GPS data of vehicles for calculating their individual delay time; hence, the propagation procedure involves the verification of the sensitive data.

A session group key for a global or virtual group should be established quickly among participating vehicles, due to fast topology changes in VANETs. The vehicles use the valid group key to achieve secure communication in terms of data authentication, data confidentiality, and data integrity. Group communication in this study is designed with the purpose that groups of friends drive vehicles traveling together; hence, the vehicles always know about each other. To apply for a virtual group, one of them has to connect to the server on the Internet through one of its neighboring RSUs. The mutual authentication between Vehicle and BSU is necessary to prevent against adversaries masquerade as legal participants. An attacker could apply for a virtual group using a travel route of the digital map, where the vehicles are traveling at present; hence, it is important that how to prevent those applications from the attacker. Head avatars in a virtual group need to hold essential key materials for the vehicles, and thus, the vehicles on a travel route will share securely data through the head avatars in the virtual group. Two groups with different members cannot produce the same group key, even if they travel on the same route toward same destinations. Groups without any RSU need a global key to communicate securely among the vehicles.

4. Proposed security mechanisms

This section introduces the procedures of the delay propagation of a traffic-related message and secure group communication.

4.1. Authentication of the delay propagation

If detecting a traffic-related event, one vehicle will broadcast a new warning message to the neighborhood, and as any of the neighboring vehicles receive the message will ignore the propagation if received other warnings recording the same event in advance. Basically, traffic-related events happen to close or same to the locations of the vehicle sources, and the neighboring vehicle can detect whether the propagations are same or not by comparing to the event type, the position of the event happenings, and timestamps provided by the sources.

Suppose a propagation path containing the participating vehicles (v_i, $i \in 0 \sim i + 2$) is denoted as $v_0 \rightarrow v_1$

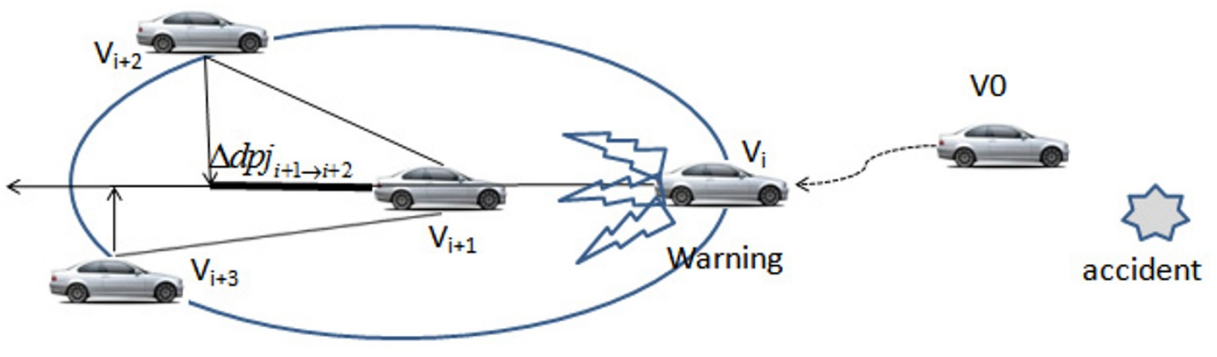

Figure 2 Example of the delay propagation of the traffic-related information.

$\rightarrow ... \rightarrow v_i \rightarrow v_{i+1} \rightarrow v_{i+2}$, and v_0 is the vehicle source, first broadcasting a fresh traffic-related warning message. The message, denoted as Warn#0, includes the sensitive data (i.e., identity, GPS, and speed) of v_0, an event type ($Event_k$), and the timestamp. Vehicle v_0 has to sign the Warn#0, so that other vehicles can verify the message in the future. Vehicle v_1 modifies the Warn#0 by adding its sensitive data and timestamp, once received and verified it. Vehicle v_2 performs same tasks as Vehicle v_1, after receiving the Warn#1 from v_1. Accordingly, the other vehicles in the propagation path can follow a format to make their warning messages. The warning format only retains the identities, GPS data, and velocities of two closest previous participants for computing the individual delay time. The certificates in the format will verify whether the participants and their attached data are valid in VANETs. Consequently, a warning message propagating in a lengthy path can efficiently be authenticated in each hop, while the packet size of the message is constant. The authentication procedure of the delay propagation in the path is given as follows:

1. v_0 detects a traffic event, and propagates immediately a warning message:

Warn#0(v_0, GPS_{v0}, $Speed_{v0}$, $Event_k$, Tstamp#0), Sign (Warn#0, SK_{v0}), $Cert_{v0}$.

2. v_1 verifies the source, and calculates the delay time. The direct distance from v_0 to v_1 replaces the projection distance of the delay time, since v_1 has the preceding sender of v_0. After waiting the delay time, v_1 propagates the modified warning message:

Warn#1(v_0, v_1, GPS_{v0}, GPS_{v1}, $Speed_{v0}$, $Speed_{v1}$, $Event_k$, Tstamp#0, Tstamp#1, Speed#1), Sign(Warn#0, SK_{v0}), Sign(Warn#1, SK_{v1}), $Cert_{v0}$, $Cert_{v1}$.

3. v_2 verifies the source, and calculates the delay time, the two preceding senders, v_0 and v_1. After waiting the delay time, v_2 propagates the Warn#2 as follows:

Warn#2(v_0, v_1, v_2, GPS_{v0}, GPS_{v1}, GPS_{v2}, $Speed_{v0}$, $Speed_{v1}$, $Speed_{v2}$, $Event_k$, Tstamp#0, Tstamp#1, Tstamp#2), Sign(Warn#0, SK_{v0}), Sign(Warn#1, SK_{v1}), Sign(Warn#2, SK_{v2}), $Cert_{v0}$, $Cert_{v1}$, $Cert_{v2}$.

4. v_3 performs the same tasks as v_3, but removes the data of v_1 in the modified warning message, since the data are useless to v_4, in calculating the delay time. After waiting the delay time, v_3 propagates the Warn#3 as follows:

Warn#3(v_0, v_2, v_3, GPS_{v0}, GPS_{v2}, GPS_{v3}, $Speed_{v0}$, $Speed_{v2}$, $Speed_{v3}$, $Event_k$, Tstamp#0, Tstamp#2, Tstamp#3), Sign(Warn#0, SK_{v0}), Sign(Warn#2, SK_{v2}), Sign(Warn#3, SK_{v3}), $Cert_{v0}$, $Cert_{v2}$, $Cert_{v3}$.

5. The propagation continues by following on the remainder path: $v_3 \rightarrow v_4 ... \rightarrow v_{i-1} \rightarrow v_i \rightarrow v_{i+1}$. The warning format of v_{i+1} 's propagation is denoted as:

Warn#i(v_0, v_i, v_{i+1} , GPS_{v0}, GPS_{vi}, GPS_{vi+1}, $Speed_{v0}$, $Speed_{vi}$, $Speed_{vi+1}$, $Event_k$, Tstamp#0, Tstamp#i, Tstamp#i+1), Sign(Warn#0, SK_{v0}), Sign(Warn#v_i, SK_{vi}), Sign(Warn#v_{i+1} , SK_{vi+1}), $Cert_{v0}$, $Cert_{vi}$, $Cert_{vi+1}$.

4.2. Secure communication in a global group without RSUs

When areas have no RSU such as rural roads, the vehicles traveling together organize a number of one-hop physical groups. Each of them can know its neighboring vehicles by broadcasting periodically a hello beacon. Each physical group needs a head, called TH, moving with a steady velocity in order to coordinate the establishment of a group key. Any of vehicles keeping a steady velocity for a tiny period of time will automatically become a TH and announce the role with a two-hop broadcast strategy, while having no neighboring THs. The two-hop broadcast strategy means that an announcement can be forwarded to two-hop neighboring nodes. To avoid communication collisions during the announcement period of THs, each TH announces its role after waiting the individual delay time, as determined by Equation (2):

$$\Delta t_A = \beta \times \frac{\Delta d^{tp}_{\mathrm{THj}\rightarrow \mathrm{Dest}}}{\mathrm{Max}(\{\Delta d^{tp}_{\mathrm{THj}\rightarrow \mathrm{Dest}}\})} \times \mathrm{NumofTHs},\ j \in 0 \sim n, \quad (2)$$

where the NumberOfTHs is the predictive number of THs, larger than or equal to the number of the practical THs (n), $\Delta d^{tp}_{\mathrm{THj}\rightarrow \mathrm{Dest}}$ is the approximate distance between the locations of TH_j and the traveling destination, *Dest* on the route of the digital map, the $\mathrm{Max}(\{\Delta d^{tp}_{\mathrm{THj}\rightarrow \mathrm{Dest}}\})$ as a function will return the maximum value of the set, $\{\Delta d^{tp}_{\mathrm{THj}\rightarrow \mathrm{Dest}}\}$, and β is a value proportional to the average propagation delay of one hop. In Equation (2), vehicular computers using the map-based service APIs such as GoogleMap [20] can easily calculate the approximate distance between two locations on a route in the digital map. The announcement information contains the GPS position of the TH.

Each of the one-hop neighboring vehicles that receive the announcement will respond as it becomes a member of the TH. Each member selects only one TH as its head in the physical group.

Suppose one TH, TH_x, has as one-hop neighboring members, denoted $\{M_i\}$. TH_x broadcasts a request to $\{M_i\}$ for establishing a group key, after appending its identity, velocity, GPS, and the list of $\{M_i\}$ within a particular sequence, denoted as $NList_x$ to the request. The vehicles in $\{M_i\}$ moving on the front locations of the travel roadway have a high priority on the front of the arrangement of $NList_x$. The request is defined as follows:

$TH_x \rightarrow \{M_i\}$: Req@(v_x, $Speed_x$, GPS_x, $NList_x$), Sign (Req@, SK_{THx}), $Cert_x$.

Suppose that the vehicles $\{M_1, M_2, ..., M_{(x-1)}\}$ in the $NList_x$ are neighbors to TH_x, and $\{M_i\}$ exchange the ECDH-based public keys each other. Each of M_i generates a private and public key pair, K_1 and K_1P, while P is a well-known generator. In addition, TH_x also has its key pair, K_x and K_xP. At the beginning of the key agreement protocol, M_1 as the first vehicle broadcasts its neighborhood immediately. M_2 cannot broadcast its K_2P until it receives the K_1P from M_1. Just like M_2, the others broadcast their public keys according to the order in $NList_x$. TH_x can help one of $\{M_i\}$ forwarding its public key to the next member. After exchanging completely public keys, each M_i has to unicast the result $(K_1K_2...K_{(i-1)}\ K_{(i+1)}...K_{(x-1)}P)$ without the K_iP to TH_x. TH_x returns individually a response by multiplying its private key for M_i, such as $(K_1K_2...K_{(i-1)}K_{(i+1)}...K_{(x-1)}K_xP)$. Finally, M_i multiplies the response with its private key to have granted the group key, $gk_x \left(= \prod_{i=1}^{x} K_iP\right)$. Consequently, the group key is shared among the TH_x and its $\{M_i\}$ in order to secure communication in the physical group.

Any TH knows its two-hop neighboring THs, after completing the announcement procedure. All of the THs in the physical groups establish a global group key for all of the vehicles based on the position-based routing. To avoid the key disclosure, each TH multiplies a pseudo private and public key pair, gk' and $gk'P$. The TH moving at the top of the traveling path must become the root to start the key agreement process, while the other THs are always moving behind itself. Supposing that there are multiple THs, denoted as (TH_1, TH_2, ..., TH_{n-1}, TH_n), and TH_j always moves behind TH_{j-1}. The procedure started by TH_1 using the on-demand routing in the V2V mode for establishing a global group key is detailed as follows:

1. TH_1 forwards its $<gk_1'P>$ to its neighboring TH_2 using one of ad hoc routing schemes such as the position routing [10]. Once the data is stored, TH_2 generates and sends a product $<gk_2'gk_1'P>$ to TH_3. Just like the previous TH, TH_3 generates and sends a product $<gk_3'gk_2'gk_1'P>$ to TH_4.

2. The process of forwarding the product continues by following the remainder path: $TH_4 \rightarrow TH_5 \rightarrow ... \rightarrow TH_{n-1}$. TH_{n-1} delivers the $\prod_{i=1}^{n-1} gk_i'P$ to TH_n, after storing the product $\prod_{i=1}^{n-2} gk_i'P$ from TH_{n-2}.

3. TH_n generates the global group key, $\prod_{i=1}^{n} gk_i'P$, by multiplying the product of TH_{n-1} with its pseudo private key, gk_n'. However, TH_n must return its public key, $gk_n'P$, back to TH_{n-1} using the previous routing path.

4. TH_{n-1} can generate the global group key, after multiplying $\prod_{i=1}^{n-2} gk_i'P$ by $(gk_{n-1}'gk_n'P)$, and returns the $gk_{n-1}'gk_n'P$ to TH_{n-2}.

5. Just like TH_{n-1}, TH_{n-2} generates the key, and returns the product $gk_{n-2}'gk_{n-1}'gk_n'P$ to TH_{n-3}.

6. Returning the product continues by following on the remainder path: $TH_{n-3} \rightarrow TH_{n-4} \rightarrow ... \rightarrow TH_j ... \rightarrow TH_1$. TH_j returns the product to its previous TH_{j-1}, $\prod_{i=1}^{n} gk_i'P$ after generating the group key.

7. TH_1 receives the product, $\prod_{i=2}^{n} gk_i'P$ from TH_2. The key agreement process is done, and the group key, $\prod_{i=1}^{n} gk_i'P$ has shared among the THs.

8. Finally, each TH distributes the global group key to its member by encrypted with the physical group key, gk_x. The message is defined as follows:

$$< E(\mathrm{GGK},\ gk_x),\ \mathrm{MAC}(gk_x) >, \text{where } \mathrm{GGK} = \prod_{i=1}^{n} gk_i'P$$

If the last step is excluded, there are the extra encryption/decryption overheads. The secure group communication from M_i to the others is then detailed as follows:

$M_i \rightarrow TH_i$:

Stream#(M_i, Multimedia, Tstamp), MAC(Stream#, gk_i), or E(Stream#(v_1, Multimedia, Tstamp), gk_i), MAC(E(...), gk_i)

$TH_i \rightarrow \{TH_j | j \in 1 - n, j! = i\}$:

Stream#, MAC(Stream#, GGK), or E(Stream#, GGK), MAC(E(...), GGK)

$TH_j \rightarrow \{M_j\}$:

Stream#, MAC(Stream#, gk_j), or E(Stream#, vgk_j), MAC(E(...), gk_j), where $\{M_j\}$ are the members of TH_j.

4.3. Secure communication in a virtual group with multiple RSUs

According to the vehicle architecture in Section 3.1, legal RSUs on the roadside are managed by a number of servers on Internet. The servers are assumed to be able to connect to the trusted third parties. The scattered vehicles moving in the trip can organize a virtual group with the RSUs. Figure 3 illustrates that v_1 asks for a virtual group to establish group communication, while the vehicles (v_1-v_n) travel on the route toward the common destination. The others (v_2-v_n) could also apply for the group through their neighboring RSUs during traveling. Suppose that the v_1 sends a request with the travel-related information to a valid RSU, RSU_i. The RSU_i checks whether v_1 and the request are valid, by examining the certificate and the attached timestamp. If the request is not yet expired, RSU_i checks its local storage whether the RSU set exists or not, in order to serve the same vehicles on the route within the same trip period. RSU_i responds immediately to v_1, if the set is always available in the storage; otherwise, if the set is not existent or has been expired, RSU_i will forward the request to its server on the Internet, denoted as Root. The

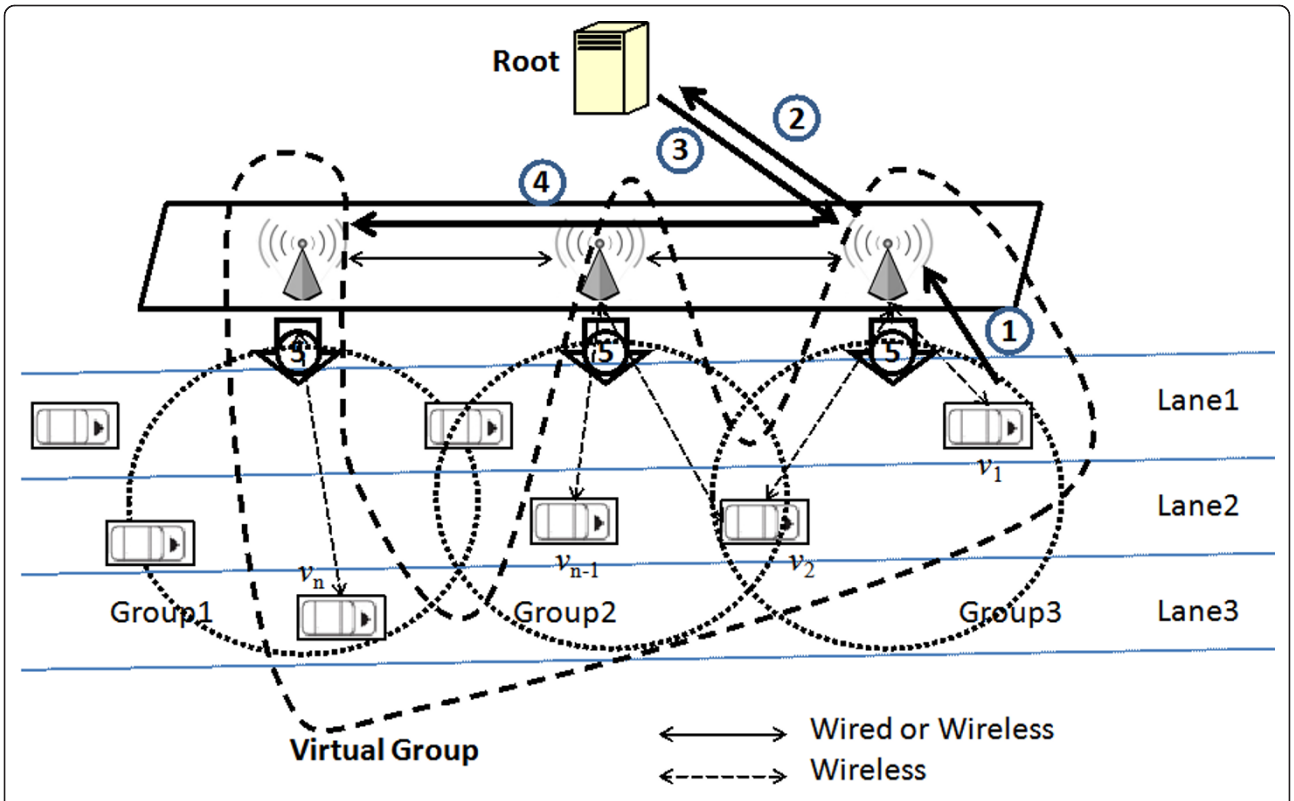

Figure 3 Illustration of the architecture of a virtual group, and the five phases of the key agreement to establish a VGK, shared among the vehicles (v_1 - v_n). Assume that the vehicles travel on the route toward the common destination.

procedure is that v_1 applies for a set of the RSUs using the information of a travel route which is detailed as follows:

Phase 1. Vehicle v_1 sends Req# to RSU_i, and attaching with the identities of the vehicles, the required trip period (ΔT), the current timestamp (Tstamp), and the travel route in a digital map (TP_{map}). The request is signed with its private key.

$v_1 \rightarrow RSU_i$: Req# (v_1, ΔT, Tstamp, TP_{map}, $\{v_i \mid i \in 1\text{-}n\}$), Sign(Req#, SK_{v1}), $Cert_{v1}$

Phase 2. Suppose that the set of RSUs is not existent for the request. RSU_i forwards the request to the Root with an attached MAC code, while sharing a common key with the Root. If RSU_i and Root have no common key, the signature of RSU_i will replace the MAC code.

$RSU_i \rightarrow$ Root:

Req# (v_1, ΔT, Tstamp, TP_{map}, $\{v_i\}$), Sign(Req#, SK_{v1}), $Cert_{v1}$, MAC(Req#||Sign, $K_{Root,\ RSUi}$), or

Req# (v_1, ΔT, Tstamp, TP_{map}, $\{v_i\}$), Sign(Req#, SK_{v1}), Sign(Req#, SK_{RSUi}), $Cert_{v1}$, $Cert_{RSUi}$

Phase 3. Root authenticates the Req# using the v_1's PK_{v1}, and RSU_i is verified through the MAC code or its signature. If the authentication is successful, Root determines the subset of RSUs located on the route, TP_{map}, and sends an encrypted Resp# back to RSU_i. The Resp# is attached with the identities of the selected RSU_j, the TP_{map}, and an expiration time (ETime), a VGK, and a key pair for $\{R_j\}$, (GK_{set}, $GK_{set}P$) (i.e., set = hash(tp||ΔT||$\{R_j\}$||$\{v_i\}$||Tstamp)). The response is encrypted by the key shared between RSU_i and Root, or the public key of RSU_i to prevent eavesdropping and modification from attackers on the Internet.

Root→RSU_i:

E#(Resp#'$_{tp}$, Sign#$_{Root}$, E(Resp#$_{tp}$, Sign#$_{Root}$, PK_{v1}), $K_{Root,\ RSUi}$), MAC(E#, $K_{Root,\ RSUi}$), or

E#(Resp#'$_{tp}$, Sign#'$_{Root}$, E(Resp#$_{tp}$, Sign#$_{Root}$, PK_{v1}), PK_{RSUi}), where Resp#$_{tp}$ is generated for the vehicles (i.e., Resp#$_{tp}$ = Resp#($\{R_j\}$, TP_{map}, ETime)), Resp#'$_{tp}$ is generated for the chosen RSUs (i.e., Resp#'$_{tp}$ = Resp#(VGK, GK_{set}, $GK_{set}P$, $\{R_j\}$, $\{v_i\}$, TP_{map}, ETime, ΔT)), and Sign#$_{Root}$ (or Sign'#$_{Root}$) represents that the Resp#$_{tp}$ (or Resp#'$_{tp}$) is signed by SK_{Root}.

Phase 4. RSU_i forwards the Resp#'$_{tp}$ to the other RSUs in the $\{R_j\}$. Any two RSUs connecting to the Internet can easily establish a shared secret key, $K_{RSUi,\ RSUj}$. In addition, RSU_i has to forward the encrypted Resp#$_{tp}$ to $v1$.

$RSU_i \rightarrow \{RSU_j \mid j \in 1\text{-}n, j! = i\}$:

E(Resp#'$_{tp}$, Sign#'$_{Root}$, $K_{RSUi,\ RSUj}$), MAC(E(...), $K_{RSUi,\ RSUj}$)

$RSU_i \rightarrow v_1$: $E(Resp\#_{tp}, Sign\#_{Root}, PK_{v1})$

Phase 5. Each of $\{RSU_j\}$ stores the tuple, (GK_{set}, $GK_{set}P$, $\{R_j\}$, $\{v_i\}$, TP_{map}, ETime, ΔT), in the storage until the ETime is expired. $\{RSU_j\}$ sends a notification to $\{v_i\}$, if the vehicles is moving in their transmission ranges.

Each $RSU_i \rightarrow$ a subset of $\{v_i\}$:

Notify# (the RSU set is ready for your trip), Sign (Notify#, SK_{RSUi}), $Cert_{RSUi}$

$\{RSU_j\}$ as head avatars assist the scattered vehicles in aggregating a VGK within their transmission ranges. Suppose that one of $\{RSU_j\}$, R_x, has a few of the vehicles $\{v_y | y \in 1\text{-}j, n > j\}$ within its transmission range, exactly as a cluster. The members in $\{v_y\}$ are arranged in a sequence, when v_j always moves behind v_{j-1}. Figure 4 depicts a localized key agreement process among R_x and $\{v_y\}$, with the following steps:

1. R_x replies a message, Resp& to $\{v_y\}$ as a subset of the vehicles, when v_i in $\{v_y\}$ sends Req# to R_x.

$R_x \rightarrow$ broadcast: Resp&($\{v_y\}$, ETime, $GK_{set}P$), Sign (Resp&, SK_{Rx}), $Cert_x$.

2. One member (v_1) generates a key pair, k_{v1} and $k_{v1}P$, and then broadcasts $k_{v1}P$ to other members. When another member (v_2) receives the key, then multiplies it with its private key, denoted as $k_{v2}k_{v1}P$. To avoid a broadcast storm, v_1 as the most front of members in the road broadcasts first, and other members delay a little time to broadcast. Eventually, each member performs the same product, $K_{v1}K_{v2}...K_{vy}P$.

3. Each member filters out its private key from the product, and unicasts the extracted result to R_x, for example, v_1 sends the $K_{v2}...K_{vy}P$ to R_x. Members can unicast confidentially the result to R_x, using the public key, $GK_{set}P$.

4. R_x receives a product from one member, and then generates a response by multiplying with the key, GK_{set} in the storage. For example, R_x constructs the product, GK_{set} K_{v2}, ..., $K_{vy}P$, for v_1, then unicasts it to v_1. Consequently, R_x and $\{v_y\}$ share a group key, denoted as vgk_x ($= GK_{set} \prod_{i=1}^{x} K_i P$), in the localized group.

5. This step is optional. $\{R_x\}$ can determine whether to share the VGK to the $\{v_i\}$ in the localized groups. R_x sends confidentially the VGK to its members by encrypting with the vgk_x.

The vehicles will share a VGK, if completing all steps of the five phases. Each of the vehicles shares securely data with the others, when the data are encrypted by the VGK. If the last step of the fifth phase is excluded, head avatars will have the extra encryption/decryption overheads. The secure group communication without the last step from v_i to the others is detailed as follows:

$v_i \rightarrow R_i$:

Stream#(v_1, Multimedia, Tstamp), MAC(Stream#, vgk_i), or

E(Stream#(v_1, Multimedia, Tstamp), vgk_i), MAC(E(...), vgk_i)

$R_i \rightarrow \{R_j | j \in 1\text{-}n, j! = i\}$:

Stream#, MAC(Stream#, VGK), or E(Stream#, VGK), MAC(E(...), VGK)

$R_j \rightarrow \{v_j\}$:

Stream#, MAC(Stream#, vgk_j), or E(Stream#, vgk_j), MAC(E(...), vgk_j), where each vehicle in $\{v_j\}$ is moving within the transmission range of R_j.

5. Security and delay analyses

Attackers could generate incorrect propagation of information based on fake traffic events to influence traffic conditions, even paralyze the vehicle network. In addition, group communication including sensitive data in the private group will provoke adversary's interest. This section analyzes the security issues for the delay propagation and group communication.

5.1. Security of the propagation of traffic-related information

A Warn# message with the signature and warrant/certificate of a vehicle source can achieve the identity and data authentication, after verifying using the public key. Each of the vehicles in the propagation procedure can trust the sensitive data of the two preceding senders as their GPS positions and speeds, after verifying successfully their signatures.

In the only V2V mode, attackers without the valid key pair issued by the trusted third party cannot create or forward an incorrect warning message. A compromised vehicle could go through a wrong warning propagation and try to modify a warning propagation. If a compromised vehicle fixed in a location creates a wrong propagation to attack the network, it is most probably without success. The detection range of event-based sensors is smaller than the transmission range of 802.11p in vehicles, and therefore the neighboring vehicles can easily find no event happening in its neighborhood. Already compromised vehicle does not modify easily the propagation, since the propagation is signed by its two preceding senders and the vehicle source is found in the propagation path. The compromised vehicle could conspire with them to fabricate an incorrect warning; however, the adversaries could be found with a high probability by their valid neighbor vehicles.

As the network supports the V2I mode, the trusted RSUs service as guards may accuse a compromised vehicle that creates or forwards incorrect Warn# message. If the number of accusations against a suspected vehicle achieves a threshold, the certificate of the vehicle will be expired and added in the certificate revocation list

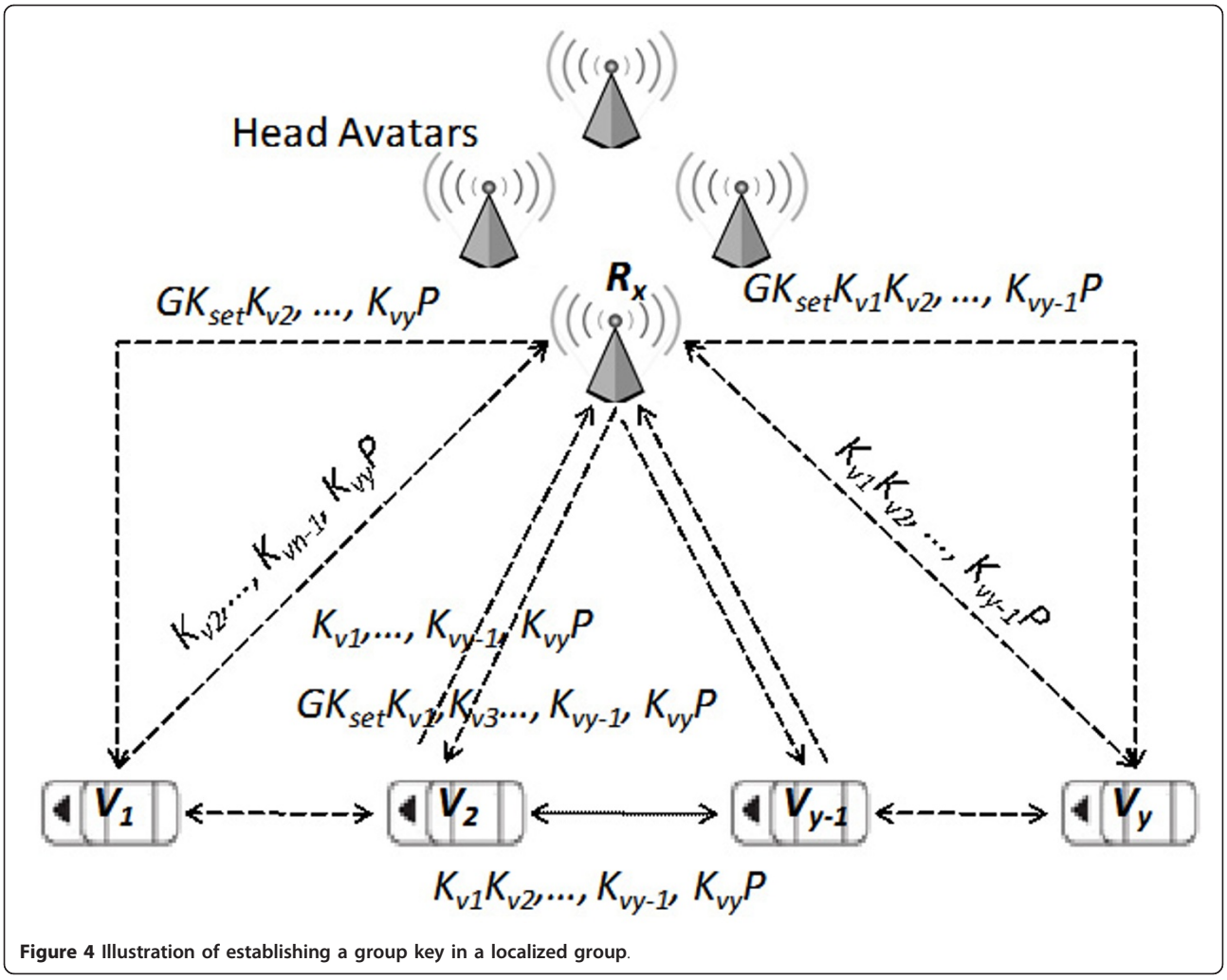

Figure 4 Illustration of establishing a group key in a localized group.

(CRL) by the trusted party. If a trusted vehicle accuses a suspect vehicle, the accusation will be verified by a number of its neighboring RSUs. If the accusation is correct, then the RSUs will report the result to the trusted third party through its management servers.

A replay attack could be generated, while the two neighboring vehicles in a propagation path collude to propagate repetitively a warning message. The vehicle receiving the replay message can check whether the warning is expired or not according to the timestamp given by the vehicle source. Three timestamps are attached in a Warn# message: one is attached by the source, and the others are attached by collusive vehicles. The difference in time between the two previous timestamps of the Warn# is represented as the actual elapsed time of the event happening. The vehicle can determine whether the event happening is expired or not, when each event type has a stable reparation period announced by the government responsible for the traffic event. Consequently, the propagation of a traffic-related message reaches the security degrees consisting of source non-repudiation, data integrity, the prevention of replication attacks, and delay effect.

5.2. Propagation delay

We illustrate two cases for the propagation delay scheme using the architecture presented in Figure 2. The IEEE 802.11p operates under 5.9 GHz and supports speed up to 190 km/h with a normal transmission range of 300 m. The vehicles move on the highway (HH) and rural roads (RR), individually corresponding to two examples. Table 2 shows the delay time of propagations for the examples. Suppose that R_T is 300 m in Equation (1), the other values of v_{i+1} , v_{i+2}, and v_{i+3} are given in the table. The GPS_i, GPS_{i+1}, GPS_{i+2}, and GPS_{i+2} are set to (24.164477, 120.670084), (24.164492, 120.671157), (24.164676, 120.671841), and (24.164935, 120.672254).

The derived unit of GPS is latitude and longitude, (x, y), and the derived unit of Speed (Sp) is Kilometer per hour (Km/h), same as that of $v$limit. To calculate

Table 2 Illustration of the delay propagation with v_i, v_{i+1}, v_{i+2}, and v_{i+3} in Figure 2

	*v*limit	Sp_{i+1}	Sp_{i+2}	Sp_{i+3}	$\Delta dpj_{i+1\to i+2}$	$\Delta dpj_{i+1\to i+3}$	0.5α	$Delay_{i+2}$	$Delay_{i+3}$
HH	110	95	105	70	64.15	103.03	6/12	4.24/8.47	3.75/1.82
RR	60	45	15	50	64.15	103.03	6/12	1.94/3.88	2.62/5.26

GPS (*x*, *y*) in GoogleMap [20], *Sp* (km/h), *v*limit (km/h), and delay (s)

the projection distance, v_{i+2} and v_{i+3} first gain their projection positions over the vector from v_i to v_{i+1} . Second, each of them calculates the straight distance from Sp_{i+1} to itself. For example, v_{i+2} calculates the distance using Equation (3) as follows:

$$\Delta dpj = 2 \times \arcsin\left(\sqrt{\sin^2(a') + \cos(x_{i+1}) \times \cos(x_{i+2}) \times \sin^2(b')}\right) \times \text{EarthRadius}, \quad (3)$$

where a' is set to $(x_{i+1} - x_{i+2})/2$, b' is set to $(y_{i+1} - y_{i+2})/2$, and EarthRadius is set to 63, 78, 137 m.

Vehicle v_{i+2} and v_{i+3} moving within the transmission range of v_{i+1} have the projection distance, 64.15 (m) and 103.03 (m) over the vector from v_i to v_{i+1} . In the HH, v_{i+2} moves more faster than v_{i+1} , and v_{i+3} moves slower than v_{i+1} . Vehicle v_{i+3} must propagate the traffic-related information faster than the propagation of v_{i+2} . Basically, v_{i+2} will listen and gain the propagation from v_{i+3} , then be able to stop its propagation to avoid broadcast storms. In the RR, v_{i+2} moves slowly and v_{i+3} moves fast toward v_{i+1} . Vehicle v_{i+2} must propagate the traffic-related information faster than the propagation of v_{i+3} . The vehicle v_{i+3} will decide not to propagate for collision avoidance, after waiting a period as the delay time of v_{i+2}.

5.3. Security of V2I group communication

Vehicles and RSU can authenticate each other through the asymmetric cryptography. RSUs are maintained by the servers on the Internet, and the servers are supported with the trusted third party. If an invalid RSU was recorded in the CRL, then servers will eliminate it from the establishment procedure of virtual groups. An attacker without the servers' support masquerades difficultly itself as a valid RSU to attend the head avatars of any virtual group.

Group communication is designed for the groups of friends driving vehicles to travel together; hence, any of vehicles always holds their total identities. It is impossible that an outside attacker joins easily and successfully their trip in the V2I mode. During the period of applying for a new virtual group, to deliver the Req# from a vehicle to the Root through a RSU can achieve data integrity, source authentication, and non-repudiation of transmission. If the RSU uses a secret key shared with the Root to encrypt their operations with a MAC code, then delivering Req# or Resp# between them will achieve data confidentiality and integrity. In addition, any two BSUs communicate securely each other using a secret key or their public keys. In this case, the communication achieves data confidentiality and integrity.

A compromised vehicle cannot apply for the same virtual group by sending the same set of the vehicles' identities and the travel path to a valid RSU, unless it belongs to one of them. In other words, any two sets of the VGK and the key materials (GK_{set}, $GK_{\text{set}}P$) determined by the Root (i.e., a server with the trusted third party) cannot be same, only if the values of the parameters, tp, ΔT, $\{R_j\}$, $\{v_i\}$, and Tstamp are the same in two different applications.

To perform the key agreement protocol for a localized group, the members exchange their ECDH-based public keys and send particular products to the BSU, individually. The delivery of the products is secure using the $GK_{\text{set}}P$ to prevent the middle attack. Group communication in a localized group can achieve data confidentiality and integrity, when the members adopt the localized group key to encrypt their communication.

5.4. Security of V2V group communication

The V2V group communication can be implemented, following the conditions: no connection gap among the traveling vehicles, and enough THs moving at steady speeds. The vehicles are divided into different one-hop physical groups. The delivery of a Req@ from one TH to its neighboring members achieves data integrity, source authentication, and non-repudiation, since the TH's signature was appended to the request. Each TH cooperates with its one-hop members in key agreement to gain a common key gk_x. Since THs move on the roadway in an order, they can cooperate to get a common key, GGK, after an exchange of ECDH products to make a round trip from the head TH to the tail TH and back again. Both of the key agreements are safe unless attackers solve the elliptic curve discrete logarithm problem. The confidentiality and integrity of data sharing among the vehicle in a physical or global group can be reached.

An attacker without a valid certificate cannot become a TH. Any compromised vehicle with a valid certificate cannot easily join a traveling group, since the vehicles know each other. A compromised vehicle could disguise itself as one of the vehicles by broadcasting a beacon with the compromised identity, and therefore, the two vehicles with the same identity move together at the beginning. The adversary can successfully perform the

key agreement in its physical group, before the key agreement process of GGK. To avoid the expansion of damage into other physical groups, THs must append their identities to the products during the agreement period of GGK, as detailed in Section 4.2. For example, TH_k forwards its product to the next TH, and the product is defined as follows:

$$TH_k \rightarrow TH_{K+1} : < \prod_{i=1}^{k} gk_i' P, \{M\}_{TH1}, \{M\}_{TH2}, \cdots, \{M\}_{THk} >$$

The compromised vehicle can easily be detected, while each TH knows which vehicles are moving within which of physical groups.

6. Performance evaluation

In this study, each vehicle conserves a key pair to encryption/decrypt data at the VANET initialization. In addition, various public key cryptographies were applied to the initialization process. Some participants establish a session key using their public key cryptography, and therefore hash and session key operations are adopted to consume few overheads and to improve the encryption/decryption performance. Vehicle exploits a hash function such as HMAC-160 or RIPEMD-160 to verify the integrity of data communication in our evaluation. Each vehicular computer in our experimental environment is implemented using a Linux platform PC with a 2.4 GHz CPU, 1 GB of memory as hardware and supporting the GNU C/C++ library, which will have enough capability to implement Elliptic Curve and RSA cryptographies. This study evaluated the eclipsed time of propagating traffic-related packets, the key synchronization time in the global and virtual groups, and the delay results of comparing our schemes with GDH [5], and GSIS [16].

The delay propagation scheme, denoted as DelayProp, compared with a natural propagation, denoted as NatureProp. Vehicles always flood immediately while receiving a propagation message in the NatureProp. Figure 5 shows the propagation with a message loss ratio in the DelayProp smaller than that in the NatureProp. We also compared the experimental results, while DeplayProp is designed with various average numbers of neighboring nodes of each vehicle. All DelayProps with Equation (1) reached a small ratio in the packet loss estimation, even if the network size was increasing, such a ratio of approximately 1%. The value of α as the number of neighbors of a vehicle increases, the delay time increases. Since the width of a road is limited with few lanes, the average number of neighboring vehicles was set to 6, 12, 18, or 24 in the evaluation. Consequently, the network size had a little impact for the proposed scheme. The "DelayProp with 18" and "DelayProp with 24" have a high value of neighbor-based vehicle density, and therefore only few vehicles participate the propagation process, and most of them always listen the propagation from its rear neighboring nodes after waiting an individual time. Figure 6 depicts the propagation delay time of the four DelayProp with various numbers of neighboring nodes. The environment area of the VANET in "DelayProp with 6" is max in the four propagations; hence, it has more delay than the others. The percentage of the area, that any of the four propagations are covered with, is always larger than 93%.

The proposed key agreement scheme is compared with the group-based GDH and GSIS schemes. The GDH and GSIS established a group-based secret key and a group-based public key individually. Both of them adopted DH with exponential operations. We evaluated the proposed scheme with a 160-bit group key for *gk*, *vgk*, GGK, and VGK, and the others were implemented with a 1024-bit key. The group communication adopted the seven or eight members in each physical or localized group, and the total number of vehicles in a VANET is 65 nodes. Figure 7 depicts the comparison of the average delay time of the three key agreement schemes without GSIS, since the procedure of its group-based signature was initialized in the offline phase. The key agreement in a virtual group obtained the aid of the valid RSUs, thus the delay time was very low. A global group without RSUs in VANETs had a large delay, when the traffic load was increasing. The global group had a small delay before the traffic load was 65, while vehicle heads always helped exchanging ECDH-based products.

Figure 8 depicts the comparison among four schemes for secure group communication. After finishing the key agreement protocols, members in a group shared a secret key. The network using GSIS to data transmission performed the verification of the group-based signature replacing the encryption and decryption operations. The communication architectures of Virtual Group-160 and GSIS supported the aid of fixed RSUs. For this reason, their average delay was inclining to a stable status. However, the consumption overhead of verifying a signature was larger than encryption or decryption operations. The average transmission delays of GSIS and Virtual Group-160 were tending to 60 and 25 ms, individually. The others built secure communication in the only V2V mode, so that the delays of data transmission were serious, as the traffic load increases.

7. Conclusions

This research paper discusses the security issues for two communication scenarios in vehicle network, the propagation of traffic-related messages, and the group-based communication scenarios. The security issues of the

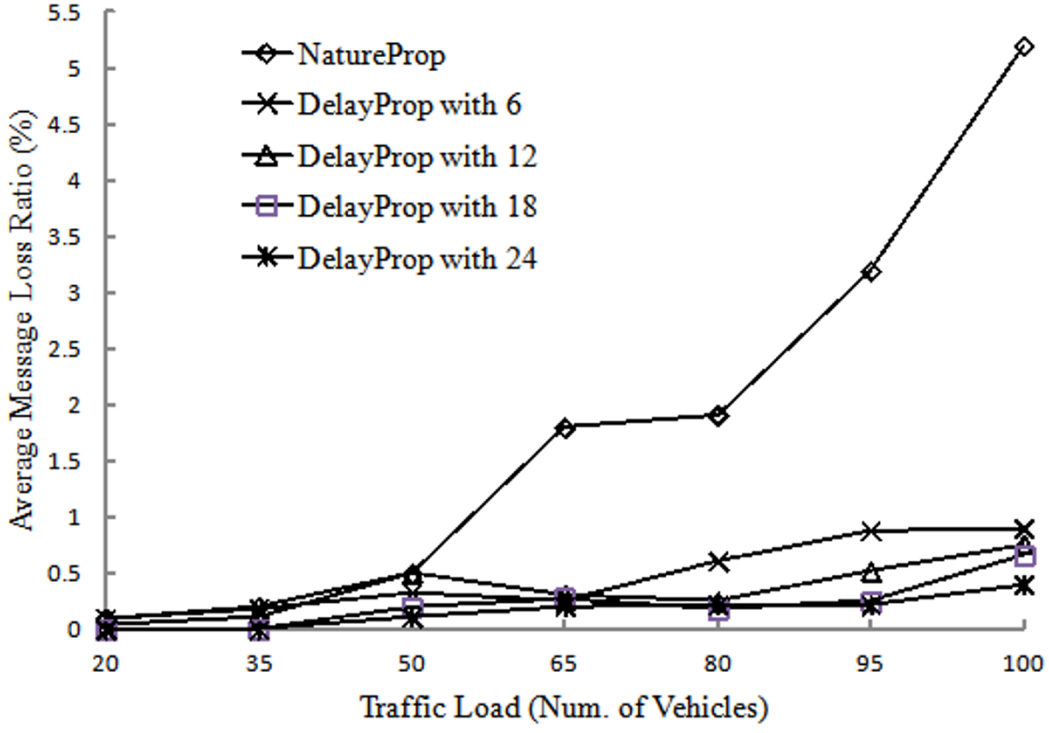

Figure 5 Impact of traffic load on message loss ratio for the propagation of traffic-related information.

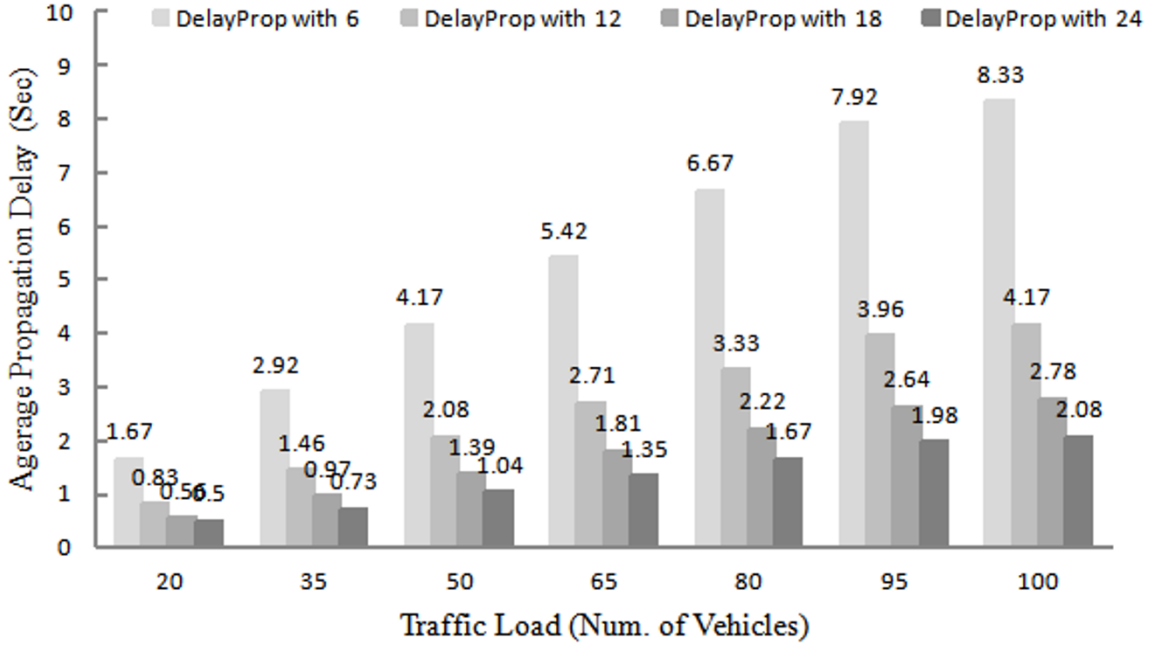

Figure 6 Comparison of the propagation delay of DelayProp with various the average number of neighboring nodes.

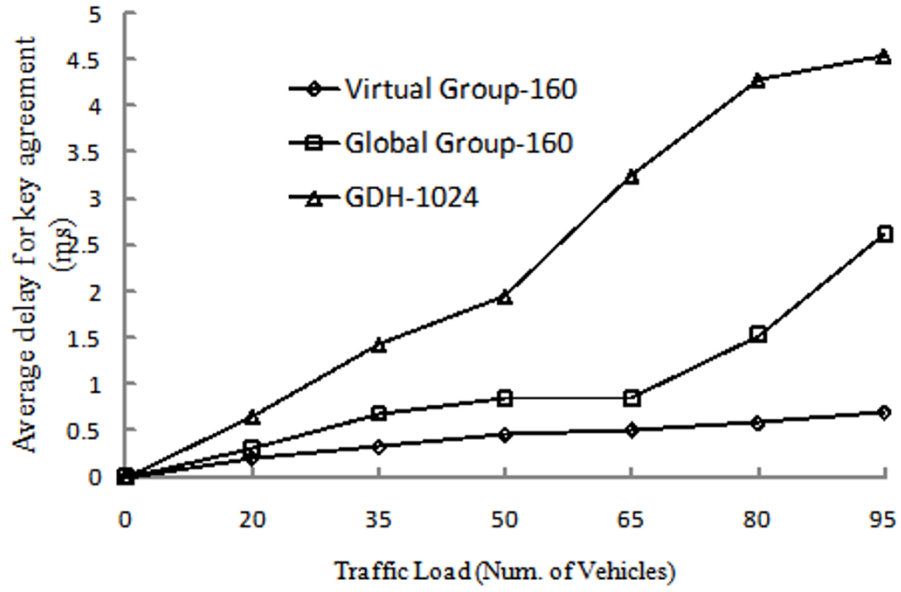

Figure 7 Comparison of the average delay of three key agreement schemes.

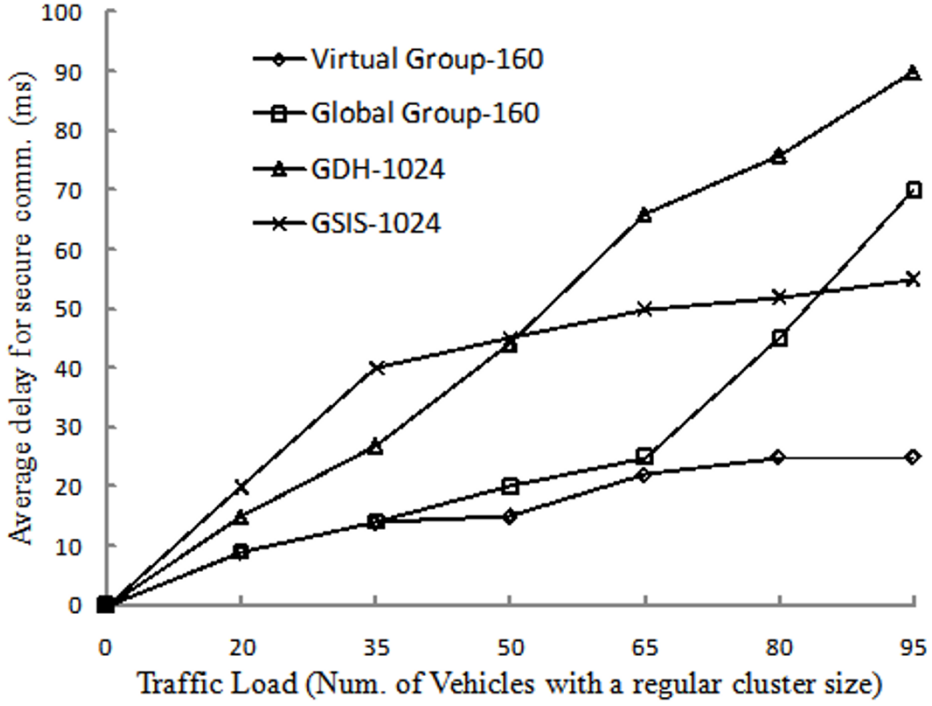

Figure 8 Comparison of the average delay of the four schemes for secure transmission from one source to all members in a group.

delay propagation achieved authentication and non-replication. The propagation delay mechanism avoids problems of communication collision and broadcast storms, but increases the propagation delay. Our simulation results indicated that the scheme improved the performance of the data flooding. The delay time (seconds) is acceptable, since to deal with traffic-related events such as a car accident needs a lot of time (minutes or hours).

Secure group communication scenarios can be implemented in the V2I and V2V modes. In the V2I mode, BSUs strengthen the security of group communication. The key agreement process in a localized group is easily accomplished with the head avatars in the virtual group. In addition, the vehicles distributed in different localized groups can perform secure group communication by the aid of their localized group keys and a VGK, issued by the third party. The establishment of group key for secure V2V group communication can easily be accomplished because of the security features of the ECDH-based key agreement protocol. The elliptic curve group key with a small size still has the same security strength with RSA and DH. The V2V group communication with the aid of the position-based routing consumes less time in the establishment of a secret key among THs in a global group.

In general, key management for secure group communication is a challenge in ad hoc networks. The group key management in the proposed schemes is easily to be solved. According to the scenario of group communication, groups of friends traveling together can easily gain identities of all vehicles. For this reason, it is impossible that a new vehicle can join to the group during the period of traveling. However, a member could leave the traveling group in the real world. In order to reduce the complexity of rebuilding group keys, heads in the V2I or V2V group cannot distribute the virtual or global group key (VGK or GGK) to their members. If one member leaves from a physical or localized group, then the head should re-build the *gk* or *vgk* key. In case that one of head avatars was not available, then the vehicles will need to re-apply for a virtual group to avoid attacks. Alternatively, if one of THs leaves, then the members belonging to the TH must re-organized physical groups, and the GGK will be re-builded. The vehicles in the other physical groups not belonging to the TH still keep the original status.

Acknowledgements
This work was supported by National Science Council (NSC), Taiwan, under research grants no. NSC100-2221-E-126-001- and NSC100-2221-E-126-006-.

Author details
[1]Department of Computer Science and Information Engineering, Providence University, Taichung, Taiwan [2]Department of Information Management, China University of Technology, HsinChu, Taiwan [3]Institute of Computer Science and Information Engineering, National Ilan University, Yilan, Taiwan

Competing interests
The authors declare that they have no competing interests.

Received: 1 July 2011 Accepted: 10 November 2011
Published: 10 November 2011

References

1. V Kapoor, VS Abraham, R Singh, Elliptic curve cryptography. Ubiquity **9**(20), 1–8 (2008)
2. W Haodong, S Bo, L Quan, Elliptic curve cryptography-based access control in sensor networks. Int J Security Netw. **1**(3), 127–137 (2006). doi:10.1504/IJSN.2006.011772
3. T Kavitha, SJS Priya, D Sridharan, Design of deterministic key pre distribution using number theory, in *3rd International Conference on Electronics Computer Technology (ICECT 2011)*. **5**, 134–137 (July 2011)
4. X Lin, X Sun, P-H Ho, X Shen, GSIS: a secure and privacy-preserving protocol for vehicular communications. IEEE Trans Veh Technol. **56**(6), 3442–3456 (2007)
5. Y Amir, Y Kim, C Nita-Rotaru, G Tsudik, On the performance of group key agreement protocols, in *Processing of the 22nd IEEE International Conference on Distributed Computing Systems* (June 2002)
6. E Bresson, O Chevassut, A Essiari, D Pointcheval, Mutual authentication and group key agreement for low-power mobile devices. in *5th IFIP-TC6 International Conference on Mobile and Wireless Communications Networks* 241–250 (2003)
7. C Becker, U Wille, Communication complexity of group key distribution. in *Proceedings of 5th ACM Conference on Computer and Communication Security*, 1–6 (1998)
8. J Nikodem, M Nikodem, Secure and scalable communication in vehicle ad hoc network. Lecture Notes in Computer Science. **4739/2007**, 1167–1174 (2007)
9. Z Lei, W Qianhong, A Solanas, J Domingo-Ferrer, A scalable robust authentication protocol for secure vehicular communications. IEEE Trans Veh Technol. **59**(4), 1606–1617 (2010)
10. I Broustis, M Faloutsos, Routing in vehicular networks: feasibility, modeling, and security. Int J Veh Technol 8 (2008). Article ID 267513
11. H Wu, R Fujimoto, R Guensler, M Hunter, MDDV: a mobility-centric data dissemination algorithm for vehicular networks. in *Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks, (VANET '04)*, 47–56
12. C Lochert, H Hartenstein, J Tian, H Fußler, D Hermann, M Mauve, A routing strategy for vehicular ad hoc networks in city environments, in *Proceedings of the IEEE Intelligent Vehicles Symposium (IV '03)*, Columbus, Ohio, USA, 156–161 (June 2003)
13. M El Zarki, S Mehrotra, G Tsudik, N Venkatasubramanian, Security issues in a future vehicular network, in *Proceedings of the European Wireless Conference (EuroWireless'02)*, Florence, Italy (February 2002)
14. D Boneh, M Franklin, Identity-based encryption from the weil pairing, in *Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology*, Lecture Notes in Computer Science Santa Barbara, CA, USA, 213–229 (2001)
15. C Tang, DO Wu, An efficient mobile authentication scheme for wireless networks. IEEE Trans Wirel Commun. **7**(4), 1408–1416 (2008)
16. H-K Choi, I-H Kim, J-C Yoo, Secure and efficient protocol for vehicular ad hoc network with privacy preservation. EURASIP J Wirel Commun Netw 15 (2011). Article ID 716794
17. A Khalique, K Singh, S Sood, Implementation of elliptic curve digital signature algorithm. Int J Comput Appl. **2**(2), 21–27 (2010)
18. D Jiang, V Taliwal, A Meier, W Holfelder, R Herrtwich, Design of 5.9 GHz DSRC-based vehicular safety communication. IEEE Trans Wirel Commun. **13**(5), 36–43 (2006)
19. C Laurendeau, M Barbeau, Probabilistic localization and tracking of malicious insiders using hyperbolic position bounding in vehicular networks. EURASIP J Wirel Commun Netw 13 (2009). Article ID 128679
20. GoogleMap APIs http://code.google.com/intl/zh-TW/apis/maps/index.html

doi:10.1186/1687-1499-2011-167
Cite this article as: Hsieh *et al.*: **Secure protocols for data propagation and group communication in vehicular networks.** *EURASIP Journal on Wireless Communications and Networking* 2011 **2011**:167.