TSINGHUA SCIENCE AND TECHNOLOGY
ISSN 1007-0214 02/13 pp 377–388
DOI: 10.26599 / TST.2018.9010016
Volume 23, Number 4, August 2018

Meet-Cloud for Secure and Accurate Distribution of Negative Messages in Vehicular Ad hoc Network

Baohua Huang, Xiaolu Cheng, Caixia Huang*, and Wei Cheng

Abstract: Keeping Vehicular Ad hoc Network (VANET) from attacks requires secure and efficient distribution of information about bad entities. Negative messages are pieces of information that define the negative attributes of vehicles. By formally defining the negative message, we observe that accuracy is essential for its efficient distribution. We formally define the coverage percentage and accurate coverage percentage to describe the availability and distribution efficiency of negative message. These two metrics can jointly evaluate the performance of a distribution method. To obtain both high coverage percentage and high accurate coverage percentage, we propose meet-cloud, a scheme based on meet-table and cloud computing to securely and accurately distribute negative messages in VANET. A meet-table in a Road Side Unit (RSU) records the vehicles it encounters. All meet-tables are sent to cloud service to aggregate a global meet-table. The algorithm for distributing and redistributing negative messages are designed. Security analysis shows that meet-cloud is secure against fake and holding on to negative message attacks. Simulations and analysis demonstrate that meet-cloud is secure under denial of service and fake meet-table attacks. The simulation results also justify that meet-cloud outperforms the RSU broadcast and epidemic model.

Key words: negative message; accurate coverage percentage; meet-table; VANET; cloud computing

1 Introduction

Similar to the existing information systems, information management is the foundation of Vehicular Ad hoc Network (VANET) and has been extensively studied[1]. As the most significant and attractive VANET application is to improve the safety of transportation[2], the management of information related to safety should be paid more attention.

The traditional information related to safety includes speed limit, work zone notification, curve warning, and accident information. With the development of VANET, dangerous and untrustworthy vehicle identification information can also play an important role in safety. We call this type of information negative messages, as they are used to describe the negative attributes of a vehicle. Negative messages include dangerous drivers, untrustworthy certificates, and black lists, but are not limited to these messages.

Comparing with other information in VANET, a negative message features two significant properties: (1) it describes a definite vehicle, that is, the objective vehicle; and (2) it is cared by the vehicles that may encounter the objective vehicle. Accordingly, a negative message needs not to be distributed to all vehicles in the VANET. Instead, the negative message should be distributed to a subset of

- Baohua Huang is with the School of Computer and Electronic Information, Guangxi University, Nanning 530004, China. E-mail: bhhuang66@gxu.edu.cn.
- Xiaolu Cheng and Wei Cheng are with the Department of Computer Science, Virginia Commonwealth University, Richmond, VA 23220, USA. E-mail: chengx3@vcu.edu; wcheng3@vcu.edu.
- Caixia Huang is with the School of Computer Engineering and Applied Mathematics, Changsha University, Changsha 410003, China. E-mail: ken5cs@foxmail.com.

* To whom correspondence should be addressed.
Manuscript received: 2017-07-28; accepted: 2017-09-14

vehicles that may encounter the objective vehicle.

Although information management in the VANET has been extensively studied[1], and a few works have focused on distributing Certificate Revocation List (CRL) in the VANET[3, 4], no work elucidates the concept of negative messages to the best of our knowledge. In Ref. [3], the Vehicle Infrastructure Integration (VII) tries to distribute CRL to vehicles through Road Side Unit (RSU) broadcast. This method requires a large number of RSU and high cost. In Ref. [4], Haas et al. attempted to propagate CRL in an epidemic fashion. The epidemic method can distribute CRL to all vehicles with a less number of RSU and less time, but it requires large storage and communication capacity in the VANET.

In our previous work[5], we propose meet-table to optimize CRL propagation in the VANET. As human movements follow simple reproducible patterns[6] and the trajectories of vehicles are part of human movements, the trajectories of vehicles are certainly reproducible. In other words, a vehicle may encounter RSUs and other vehicles in a certain set every day. Therefore, with the help of meet-table, we can efficiently distribute a vehicle's negative message through the encountered RSUs and vehicles.

In Ref. [7], we also proposed the concept of negative message and a scheme based on meet-table and cloud computing to distribute negative messages in the VANET. In the proposed scheme, every RSU or vehicle features a meet-table that records the vehicles encountering it. All the RSUs' meet-tables are sent to the cloud for storage and aggregation. The cloud service uses NoSQL database to manipulate the meet-table and negative messages in a highly scalable and efficient manner[8].

In this paper, we integrate previous works and extend the definitions, algorithms, analysis, and simulations. Our major contributions include the followings:

(1) We add the concept of negative message document to extend the concept of negative message for describing negative attributes such as CRL, and discuss the effect of performance.

(2) We describe and analyze the scheme, algorithms, and data structures in detail.

(3) We present simulation results, including the results of message delay simulation, fake meet-table attack simulation, and Denial of Service (DoS) attack simulation.

2 Negative Message and Evaluation of Its Distribution Method

A negative message describes the negative attributes of a particular vehicle, that is, the objective vehicle. A negative message must be distributed to the vehicles that may encounter the objective vehicle. The general information management scheme attempts to distribute all messages to all the vehicles. Thus, a number of unnecessary distributions are present. Therefore, these schemes are inefficient for distributing negative messages.

We define the set of vehicles and RSUs in the VANET as follows.

$$V = \{v_i | 0 \leqslant i \leqslant n_V\} \tag{1}$$

$$U = \{u_i | 0 \leqslant i \leqslant n_U\} \tag{2}$$

V represents the set of all vehicles in the VANET. n_V refers to the number of vehicles in V. U denotes the set of all RSUs, and n_U corresponds to the number of RSUs in U.

2.1 Negative message and negative message document

A negative message uniquely binds to an objective vehicle. As the negative message is unusable for all vehicles in the VANET, it features a set of vehicles that may care about it.

Definition 1: A negative message is a negative description of a vehicle. Formally, a negative message is defined as follows:

$$m \stackrel{\text{def}}{=} < o, d, C > \tag{3}$$

where m is the negative message, and it is a 3-tuple consisted by o, d, and C; o denotes the objective vehicle of m; d is the data in the message describing o; and C is a set of vehicles that concern the message m.

The negative messages are often generated by authority. The authority generally compiles several negative messages and signs them as a whole document. We call this type of document as a negative message document, or a negative document in short.

Definition 2: A negative message document is a set of negative messages with a signature. Formally, a negative message document is described as follows:

$$D \stackrel{\text{def}}{=} < M, a > \tag{4}$$

$$M = \{m_i | 0 \leqslant i \leqslant n_M\} \tag{5}$$

where D is the negative message document, M is the set of negative messages, a is the authority, and n_M is the number of elements in M.

Given the presence of various objective vehicles in a negative message document, efficiently distributing negative message document becomes more complicated and challenging than distributing negative messages

separately.

2.2 Evaluation criteria

The general message dissemination methods in the VANET attempt to distribute data to all the vehicles. These methods aim to achieve a high percentage of vehicles possessing a message, that is, the possessing percentage.

Definition 3: The possessing percentage is the percent of vehicles possessing a message in all vehicles. Formally, the possessing percentage is described as follows:

$$r = \frac{|B|}{|V|} = \frac{|B|}{n_V} \tag{6}$$

where B is the set of vehicles possessing the negative message, and V is the set of all vehicles in the VANET.

The existing methods, which attempt to obtain a high possessing percentage, are not very efficient and suitable for negative messages. For example, broadcasting CRL in a nationwide VANET is not only infeasible but also unnecessary[5].

In the VANET, we should process the negative message m in a way that: (1) we can push m to all vehicles as soon as possible; (2) every vehicle can achieve m with high availability. To correctly evaluate the method processing negative messages, we define the coverage percentage and accurate coverage percentage as follows.

Definition 4: The coverage percentage of a negative message is the percent of vehicles possessing the message in vehicles concerning the message. Formally, the coverage percentage is presented as follows:

$$r_c = \frac{|B \cap C|}{|C|} = \frac{\sum_{b \in B} \begin{cases} 1, & b \in C; \\ 0, & b \notin C \end{cases}}{|C|} \tag{7}$$

Definition 5: The accurate coverage percentage of a negative message is the percent of vehicles concerning the message in vehicles possessing the message. Formally, the accurate coverage percentage is computed according to the following:

$$r_{ac} = \frac{|B \cap C|}{|B|} = \frac{\sum_{b \in B} \begin{cases} 1, & b \in C; \\ 0, & b \notin C \end{cases}}{|B|} \tag{8}$$

where C is a set of vehicles that concern the message. The coverage percentage of a negative message represents the availability of the message, and the accurate coverage percentage of the message represents the efficiency of the distribution method.

Based on the definitions of coverage percentage and accurate coverage percentage of a negative message, we can obtain the evaluation criteria for evaluating the negative message distribution method.

Evaluation-Criterion 1: A good negative message distribution method should possess both high coverage percentage and high accurate coverage percentage.

A distribution method may feature a high possessing percentage but a low coverage percentage and accurate coverage percentage, as the possessed messages may not accurately cover the vehicles that really care the message.

3 Meet-Cloud

According to Evaluation-Criterion 1, an ideal model of distributing the negative message m in a VANET is to make C, the set of vehicles concerning m, equal to B, which is the set of vehicles possessing m. In this model, $r_c = r_{ac} = 100\%$. Thus, this model is the most available and efficient. The general methods of disseminating information in the VANET attempt to broadcast m to all the vehicles in V; their coverage percentage $r_c \to 100\%$, but their accurate coverage percentage $r_{ac} \to 0\%$. These methods are inapplicable in negative message distribution. We propose the meet-cloud, a scheme for distributing negative messages in a VANET based on the meet-table and cloud computing, to solve the problem.

3.1 Definition of meet-table and global meet-table

To make C equal to B, we must locate the vehicles in C. Consequently, we propose the meet-table in an RSU or a vehicle to record the vehicles that pass the RSU or the vehicle. Formally, as the meet-table of w, an RSU or a vehicle, can be defined as follows:

$$T_w = \{p_i | 0 \leqslant i \leqslant n_{T_w}\} \tag{9}$$

$$p_i \stackrel{\text{def}}{=} < v, t, c > \tag{10}$$

$$T = \{T_i | 0 \leqslant i \leqslant n_U\} \tag{11}$$

where T_w is the meet-table generated by w; n_{T_w} is the number of elements in T_w; p_i is the i-th recorder in T_w, and it is a 3-tuple consisting of v, t, and c; v is a vehicle that passed w c times by time t. T is the set of all meet-tables in the RSUs.

The meet-tables are distributed in the RSUs. We need to construct a global meet-table for negative message distribution. Thus, meet-tables must be aggregated to a global form. Formally, the global meet-table can be defined as follows:

$$G = \{g_i | 0 \leqslant i \leqslant n_G\} \tag{12}$$

$$g_i \overset{\text{def}}{=} < v, U_i > \tag{13}$$

where G is the global meet-table; n_G is the number of elements in G. g_i is the i-th recorder of G, and it's a 2-tuple. v is the vehicle that passed all the RSUs in U_i.

The algorithm for aggregate meet-tables T to global meet-table G is presented in Algorithm 1.

In a large VANET, the size of G may be huge, and its recorders feature variable lengths; thus, G should be processed with the NoSQL database[9] in a cloud computing environment. We, therefore, propose a meet-cloud to use the meet-table and cloud computing technology.

3.2 Deployment of meet-cloud

With the help of meet-table and cloud computing, we can efficiently distribute negative messages in a VANET. The deployment of components in meet-cloud is shown in Fig. 1.

In the meet-cloud, a cloud service runs on the Internet to process the global meet-table and to distribute negative messages. The meet-cloud utilizes high scalability and virtualization of cloud computing[10, 11] and NoSQL database to serve global meet-table processing and negative messages distribution.

RSUs are built at the roadsides. The RSUs are also connected to the Internet through wired or wireless communication channels, e.g., 5G[12]. Every RSU records the vehicles passing it in its meet-table.

The meet-table of an RSU can be sent to the cloud service in a planned schedule. When an RSU receives a negative message from the cloud service, it broadcasts the message to the vehicles passing it.

Algorithm 1: Alg-Aggregate

Input: T, V, U
Output: G

```
G = φ ;
foreach v ∈ V do
    U_v = φ ;
    foreach T_u ∈ T do
        foreach p ∈ T_u do
            if p.v == v then
                U_v = U_v ∪ {u} ;
            end
        end
    end
    g =< v, U_v > ;
    G = G ∪ g ;
end
```

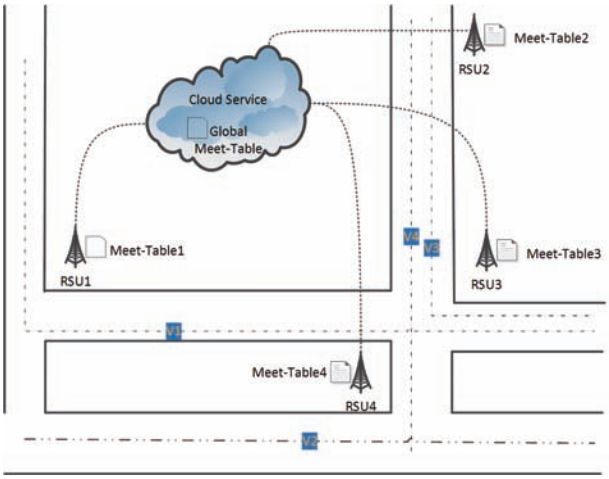


Fig. 1 Deployment of meet-cloud.

A vehicle travels along its ways. When a vehicle passes an RSU on the roadside, it can be recorded by the RSU. At the same time, the vehicle accepts the messages broadcasted by the RSU. If this vehicle encounters other vehicles, it can record them into its meet-table and broadcast the messages obtained from the RSUs it passed by.

3.3 Architecture and principle of meet-cloud

The principle of meet-cloud shown in Fig. 1 can be illustrated with the architecture shown in Fig. 2.

In the meet-cloud shown in Fig. 2,

$$V = \{v_1, v_2, v_3, v_4\} \tag{14}$$

$$U = \{u_1, u_2, u_3, u_4\} \tag{15}$$

$$T_{u_1} = \{< v_1, ... >\} \tag{16}$$

$$T_{u_2} = \{< v_3, ... >, < v_4, ... >\} \tag{17}$$

$$T_{u_3} = \{< v_1, ... >, < v_3, ... >, < v_4, ... >\} \tag{18}$$

$$T_{u_4} = \{< v_2, ... >\} \tag{19}$$

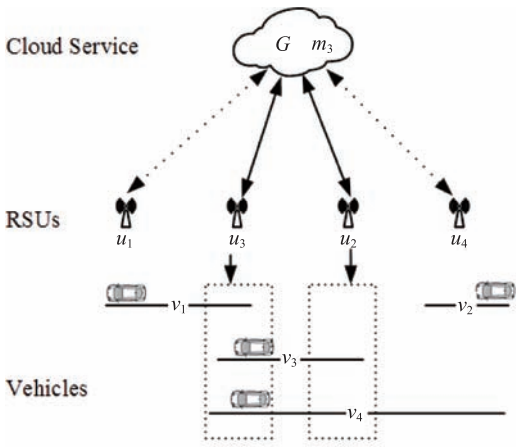


Fig. 2 Architecture of meet-cloud.

$$G = \{< v_1, \{u_1, u_3\} >, < v_2, \{u_4\} >, < v_3, \{u_2, u_3\} >, < v_4, \{u_2, u_3, u_4\} >\} \quad (20)$$

$$m_3 \stackrel{\text{def}}{=} < v_3, d, \{v_1, v_4\} > \quad (21)$$

Thus, when m_3 is sent to the cloud service for distribution, it can find $< u_3, \{u_2, u_3\} >$ from G, and it can send m_3 to u_2 and u_3 for broadcasting. u_1 and u_4 need not to broadcast m_3 at all. Therefore, v_1 and v_4 will receive m_3, but v_2 will not.

In a VANET, if we know C, which is the set of vehicles that care the negative message m, we can accurately distribute m to vehicles in C. Vehicles in C include those that may encounter the objective vehicle of m. According to the reproducible movement patterns of humans[6], we can assume that the vehicles passing by the same RSU may encounter each other. Thus, we can record the vehicles passing an RSU or a vehicle with meet-table. For the negative message m, if $\exists p_i \in T_w,\ p_i.v = m.o$, then m should be distributed through w.

3.4 Negative message distribution algorithm

A negative message describes a negative attribute of its objective vehicle. A negative message is often distributed by an authorized entity. For example, a CRL is a typical negative message issued by a Certificate Authority (CA). In the proposed meet-cloud, the algorithm for distributing negative messages is presented in Algorithm 2.

Alg-Distribute is invoked by the entity that wants to distribute the message m, and executed by the cloud service, RSUs, and vehicles in an asynchronous and distributed model.

Algorithm 2: Alg-Distribute

Input: G, m
Output: m to u, v where $u \in U, v \in V$

```
U_m = φ ;
foreach g_i ∈ G do
    if g_i.v = m.o then
        U_m = g_i.U_i ;
        break ;
    end
end
if U_m ≠ φ then
    foreach u ∈ U_m do
        push m to u ;
        foreach v, which is passing u do
            u broadcasts m to v ;
            foreach vv, which comes across v do
                v broadcasts m to vv ;
            end
        end
    end
end
```

3.5 Negative message redistribution algorithm

When the RSU u encounters a vehicle v that it never encountered before, the RSU must redistribute the negative messages of the vehicle to maintain high coverage percentage and accurate coverage percentage of the messages. The negative message redistribution algorithm is presented in Algorithm 3.

Alg-Redistribute is invoked by RSUs and executed by RSUs and vehicles in an asynchronous and distributed model. Every RSU executes its own Alg-Redistribute procedure. The cloud service provides the interface for querying negative messages of a vehicle.

4 Performance and Security Analysis

The meet-cloud utilizes the meet-table and cloud computing to securely and accurately distribute negative messages in a VANET. After describing all details of our design, we now compare it with other methods to evaluate its performance and analyze its security. In the next section, we present the simulation results.

4.1 Performance analysis

Two typical methods, the RSU broadcast[3] and epidemic model[4], are generally used in a VANET to distribute

Algorithm 3: Alg-ReDistribute

Input: v, T_u
Output: messages of v to vehicles passing u

```
p = null ;
foreach p_i ∈ T_u do
    if p_i.v = v then
        p = p_i ;
        break ;
    end
end
if p ≠ null then
    p =< v, current_time, 1 > ;
    T_u = T_u ∪ {p} ;
    query m, m.o = v from the Cloud Service ;
    if m ≠ φ then
        foreach vv, which comes across u do
            broadcasts m to vv ;
            foreach vvv, which comes across vv do
                vv broadcasts m to vvv ;
            end
        end
    end
end
```

negative messages. We, therefore, compare our design with these methods in terms of complexity and coverage.

4.1.1 Complexity

We define several average quantities in a VANET.

The average number of RSUs that a vehicle may encounter is computed as follows:

$$\bar{n_u} = \frac{\sum_{u \in U} n_{T_u}}{n_V} \tag{22}$$

The average number of vehicles that an RSU may encounter is as follows:

$$\bar{n_v} = \frac{\sum_{u \in U} n_{T_u}}{n_U} \tag{23}$$

Then, we can calculate complexities of the meet-table, RSU broadcast, and epidemic model. The results are shown in Table 1.

From Table 1, we can observe the following:

(1) Meet-cloud can reduce communications from the core to the RSU and the RSU to a vehicle as $\bar{n_u}$ is smaller than n_U.

(2) Meet-cloud can reduce communications between vehicles, as $\bar{n_u}$ and $\bar{n_v}$ are smaller than n_V.

(3) Meet-cloud can reduce vehicle storage as $\bar{n_u}$ and $\bar{n_v}$ are smaller than n_V in a large VANET.

4.1.2 Message coverage metric

The RSU broadcast and epidemic models attempt to distribute messages to all vehicles, but the meet-cloud strives to distribute messages to the right vehicles that really care the message. Table 2 shows the message coverage metrics of these methods in a very large VANET.

From Table 2, we can observe that the RSU broadcast and epidemic models are not highly efficient. According to Evaluation-Criterion 1 and Table 2, the meet-table is the best.

4.2 Security analysis

In this section, we provide the attack model and analyze the security of the meet-table. The next section discusses the simulation results of fake meet-table attack and DoS attack.

4.2.1 Attack model

In the proposed scheme, we assume that the authorized entity, cloud Service, most RSUs, and most vehicles are trustworthy. Under this assumption, we can profile the major attacks that can be conducted on the scheme.

(1) Fake negative message attack. An attacker tries to distribute an untrue negative message of a target vehicle to disturb communication and operation of the victim.

(2) Holding on to negative message attack. An attacker tries to prevent the vehicles that received negative messages from the RSUs from broadcasting the negative message to other vehicles encountered.

(3) Fake meet-table attack. An attacker tries to build a fake meet-table by driving the vehicle to pass numerous RSUs that are unnecessary in a normal human travel model.

(4) DoS attack. An attacker tries to jam the broadcasting of RSUs, to block the negative messages pushed from the cloud service, to stop cloud service, and to broadcast a huge number of garbage messages.

4.2.2 Security of the scheme

From the architecture and the algorithms described above, we know that the proposed scheme follows a distributed and asynchronous model. Thus, the scheme features potential anti-attack properties. Also, utilizing the matured cloud computing technology, the cloud service becomes scale free and hard to attack.

Table 1 Complexity of distributing method.

Complexity	Meet-cloud	Epidemic	RSU broadcast
Core to RSU communication	$n_M \bar{n_u}$	N/A	$n_M n_U$
RSU to vehicle communication	$n_M \bar{n_u} \bar{n_v}$	N/A	$n_M n_U \bar{n_v}$
Vehicle to vehicle communication	$n_m \bar{n_u} \bar{n_v}$	${n_M n_V}^2$	N/A
Core storage	$n_M + n_v \bar{n_u}$	N/A	N/A
Vehicle storage	$n_M \bar{n_u} \bar{n_v}$	$n_M n_V$	$n_M n_V$
Computing	$n_U n_V$	N/A	N/A

Table 2 Message coverage metrics of distributing methods in very large VANET.

Metric	Possessing percentage (%)	Coverage percentage (%)	Accurate coverage percentage (%)
Meet-cloud	$\to 0$	$\to 100$	$\to 100$
Epidemic	$\to 100$	$\to 100$	$\to 100$
RSU broadcast	$\to 100$	$\to 0$	$\to 0$

Numerous anti-attack measurements are available for fake negative message attack. For example, cloud service can authenticate the sender; negative messages may be signed with a signature for verification in RSUs and vehicles.

If a vehicle is controlled by an attacker, it may not broadcast negative messages that are received from RSUs and other vehicles to the vehicles it encounters. This holding of negative message attack can hardly affect the propagation of negative messages in a VANET, given that compared with other uncontrolled vehicles, the number of vehicles controlled by the attacker is remarkable less.

An attacker can drive the vehicle passing RSUs to build a fake meet-table, but the process is very costly and easy to detect. This physical attack hardly occurs in a large scale. In addition, the movement pattern of the attacker's vehicle significantly differs from an ordinary human's reproducible pattern[6], and it is very easy to detect with the help of the global meet-table.

In general, DoS, especially Distributed DoS (DDoS) is hard to defeat if the opposite features adequate resources[13]. In the proposed scheme, DoS, even DDos faces difficulty in achieving its goal. If an attacker wants to jam the broadcasting of an RSU, he must be present at the RSU site. Thus, he can only attack a very limited number of RSUs. Given the matured protection technology of cloud computing, the attacker experiences difficulty in blocking the negative message pushed from the cloud service or in stopping cloud service. An attacker can broadcast a huge number of garbage messages to a limited part of a VANET and affect a limited area, but he can not affect the whole VANET, and its main part given that it is distributed, executes asynchronously, and contains numerous RSUs and vehicles.

In summary, the scheme is secure to face these four types of attacks if implemented carefully as it is distributed, executes asynchronously, includes numerous entities, and is based on cloud computing technology.

5 Simulation

We evaluate the performances of the meet-cloud and other message distribution methods via simulations. Furthermore, we evaluate the meet-cloud under DoS attacks of RSUs and fake meet-table attacks. The results are presented and analyzed in this section.

5.1 Simulation dataset

Simulation of a VANET can use the dataset of realistic traces of vehicles[14] or the generated traces based on a map[4, 15]. The realistic trace dataset of numerous vehicles is hard to obtain. The dataset used in Ref. [14] includes realistic taxi GPS traces from Shenzhen and Beijing, China and San Francisco, USA. The total number of vehicles in this dataset is about 13 000, and it contains only taxi and no other type of vehicles. In addition, the time length of this dataset reaches no more than three days.

To evaluate the performance and anti-attack ability of the proposed meet-cloud, we generate a dataset to simulate all vehicles in San Francisco, USA. The dataset is created based on the parameters shown in Table 3.

On the generated dataset, the percentages of vehicles and RSUs a vehicle met versus time are shown in Figs. 3a and 3b.

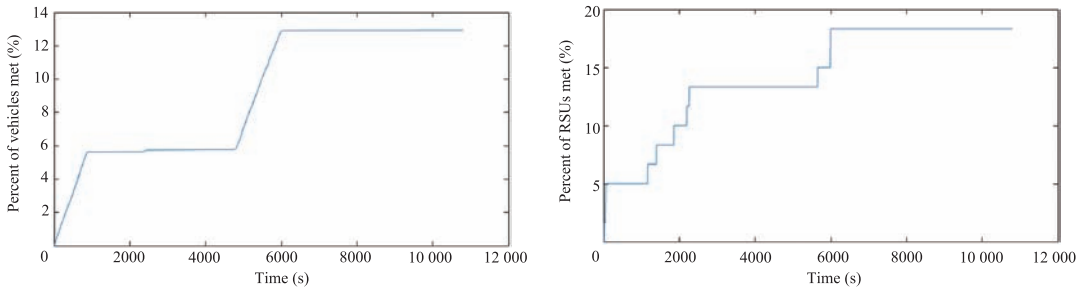
From Fig. 3, we can observe that both percentages of vehicles and RSUs met continually increase initially, but remain static after a point of time. This pattern represents the locality of vehicles' movements. Thus, the generated dataset possesses the same attribute of human movements in real daily life[14].

5.2 Performance simulations of different distribution methods

To compare the performances of the proposed meet-cloud with the RSU broadcast and epidemic models, we simulate these three methods on the generated dataset. Figure 4 shows the simulation results.

Table 3 Parameters for generating simulation dataset.

Parameter	Value	Note
Number of vehicles	471 388	Total number of vehicles in Ref. [16].
Number of RSUs	1193	Refer to the number of signalized intersections in Ref. [16].
Intersections	7200	Estimated number of intersections in Ref. [16].
Length of road	1 741 km	Total length of road in Ref. [16].
Area	121 km^2	Area - Land in Ref. [16].
Mean travel time	0.5 h	Mean Travel Time to Work in Ref. [16].
Speed	38.6 km/h	Average speed of commuter traffic speeds in Ref. [17].
maxV2I	100 m	Max communication distance of vehicle to RSU
maxV2V	10 m	Max communication distance of vehicle to vehicle



(a) Time vs. percent of vehicles met (b) Time vs. percent of RSUs met

Fig. 3 Percentage of vehicles and RSUs met on the simulation dataset.

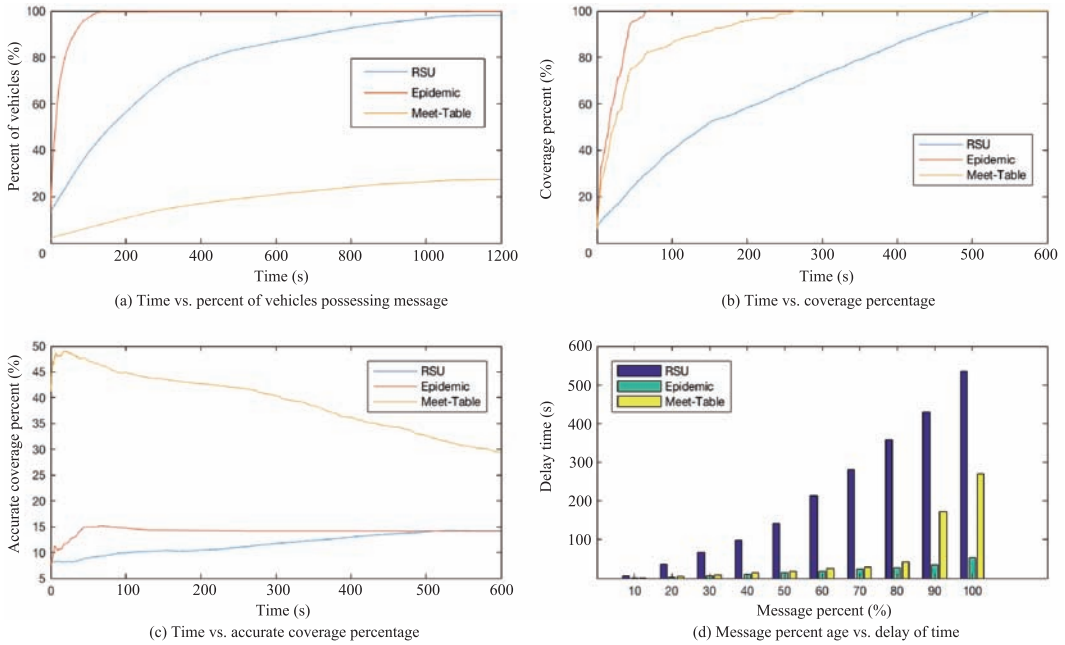
Table 4 summarizes the performance simulation results.

According to Table 4 and Evaluation-Criterion-1, as the proposed meet-cloud features both high coverage percentage and high accurate coverage percentage, and mid message delay, it is the best method for distributing negative messages in a VANET.

5.3 Fake meet-table attack simulations

To study the performance of the meet-cloud under a fake meet-table attack, we randomly add records into the meet-table of RSUs and perform simulations. Figure 5 displays the performances of different ratios of fake meet-table records.

From Fig. 5, we can observe that the fake meet-table guides the meet-cloud to act similarly to the epidemic model. The higher ratio of fake meet-table records makes meet-cloud more similar to the epidemic model. However, the fake meet-table attack can only lead to low accurate coverage percentage and not low coverage percentage. In other words, a fake meet-table attack can only affect the accuracy of negative message distribution but not the distribution range of negative message. As a result, the meet-cloud is secure under fake meet-table attacks.



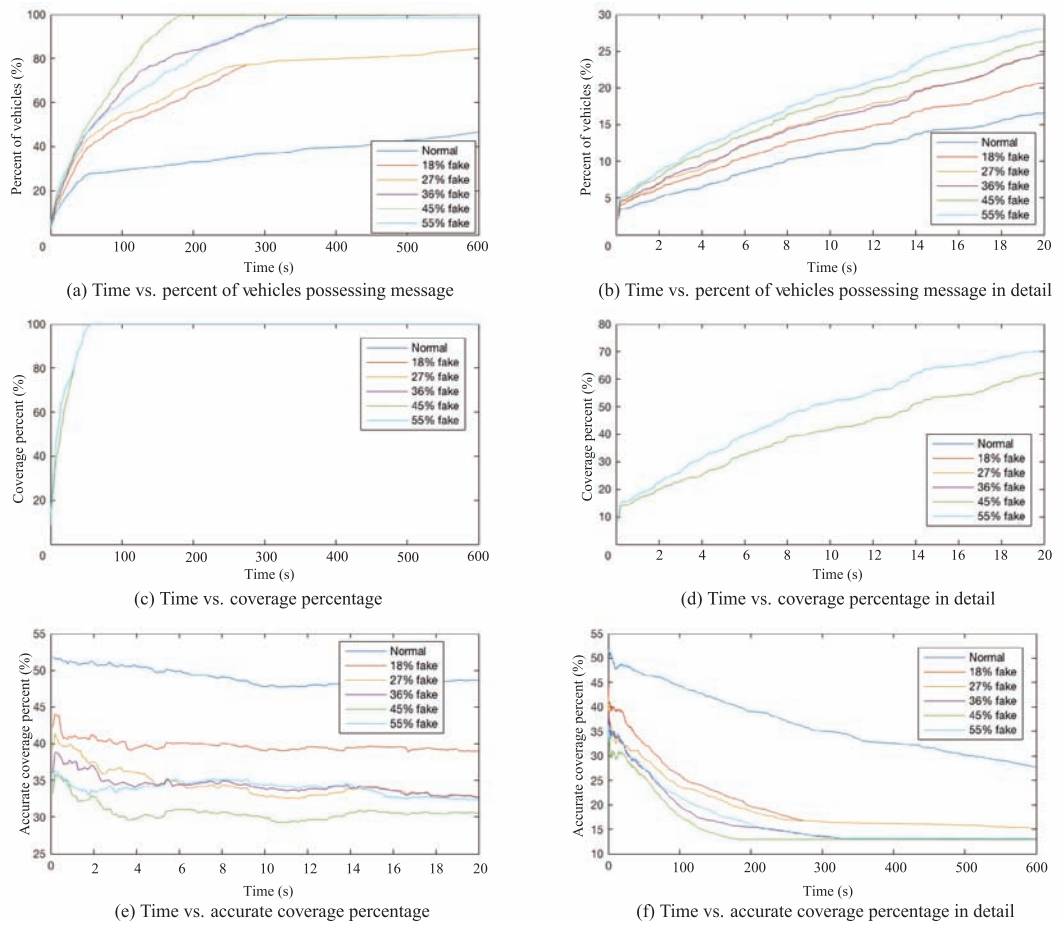
(a) Time vs. percent of vehicles possessing message (b) Time vs. coverage percentage

(c) Time vs. accurate coverage percentage (d) Message percent age vs. delay of time

Fig. 4 Performance of different distribution methods.

Table 4 Summary of performance simulation results.

Value name	Epidemic model	RSU broadcast	Meet-table based scheme
Percent of vehicles possessing message	Much high	High	Low
Coverage percentage	Much high	High	High
Accurate coverage percentage	Low	Low	High
Message delay	Low	High	Mid



(a) Time vs. percent of vehicles possessing message

(b) Time vs. percent of vehicles possessing message in detail

(c) Time vs. coverage percentage

(d) Time vs. coverage percentage in detail

(e) Time vs. accurate coverage percentage

(f) Time vs. accurate coverage percentage in detail

Fig. 5 Performance of meet-cloud under fake meet-table attack.

5.4 DoS of RSUs simulations

We randomly turn off the RSUs to simulate DoS attack of RSUs. Figure 6 illustrates the performance of the meet-cloud with different ratios of RSUs turned off.

From Fig. 6, we can observe that DoS of RSUs can not heavily affect the performance of the meet-cloud. Therefore, the proposed meet-cloud is secure in facing DoS attacks.

5.5 Discovery from attack simulation

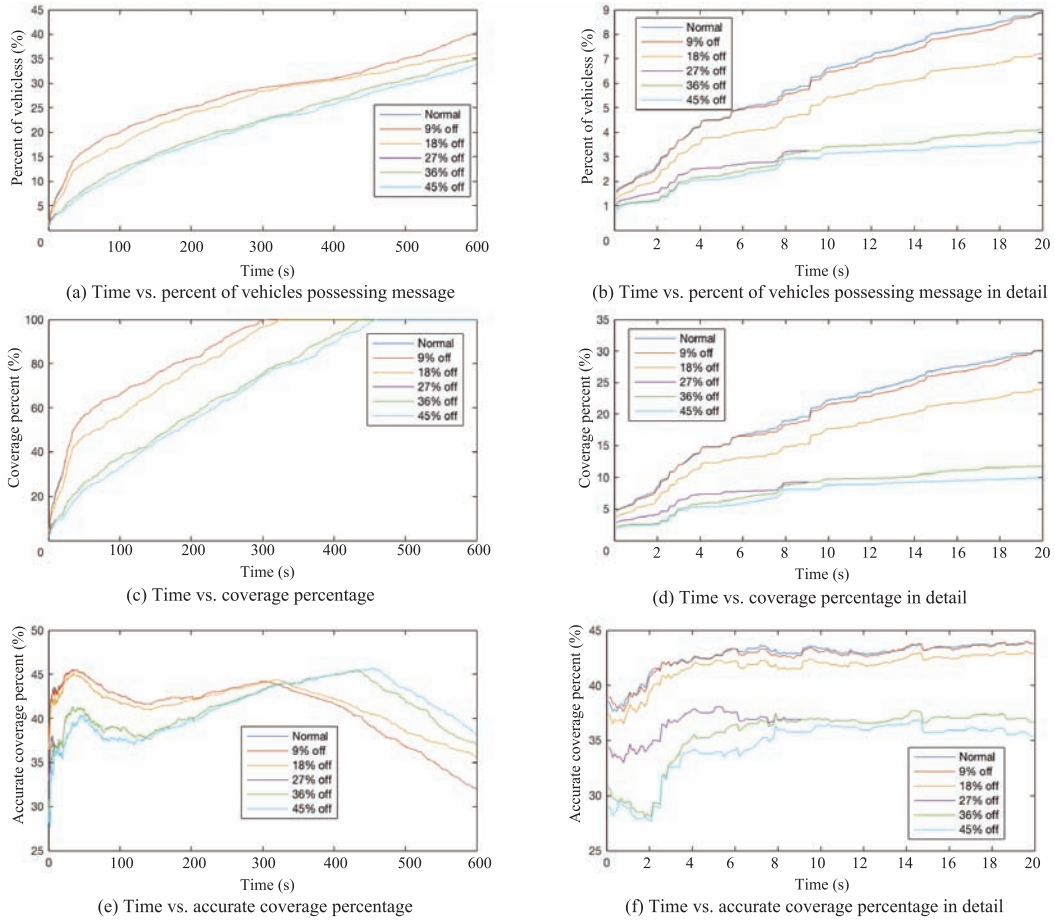
In a fake meet-table attack, we note that fake records in the meet-table may lead the meet-cloud to act like the epidemic model. In the DoS attack, we observe that turning off RSUs can not heavily affect the performance of the meet-cloud. These attributes of meet-cloud make it secure to face these attacks.

However, the proposed meet-cloud possesses attributes of both RSU broadcast and epidemic model. The meet-cloud uses the meet-table to select several RSUs as the start points of epidemic model. As a result, at a high ratio of fake meet-table records, the epidemic model attribute of the meet-cloud enhances, and the meet-cloud acts similarly to epidemic model. When the DoS of RSUs occurs, several RSUs are turned off, and the start points of the epidemic model lessen. As the epidemic model still exhibits an exponential distributing ability if only one start point is present, the epidemic model can still distribute messages around the point rapidly.

6 Related Work

Enhancing the safety of transportation is the major goal of a VANET. To achieve this goal, the VANET must gather, process, and disseminate information, such as road condition, the position of obstacles, speed limit, and road accidents[1]. With the development of a VANET, especially when self-driving cars run on the road, its security will be the key to safe transportation.

Securing a VANET requires ID authentication, message integrity, communication confidentiality, availability, and access control[18]. To satisfy these requirements, a number of solutions have been proposed. In these solutions, public key cryptography, trust



(a) Time vs. percent of vehicles possessing message

(b) Time vs. percent of vehicles possessing message in detail

(c) Time vs. coverage percentage

(d) Time vs. coverage percentage in detail

(e) Time vs. accurate coverage percentage

(f) Time vs. accurate coverage percentage in detail

Fig. 6 Performance of meet-cloud under DoS of RSUs.

management, and black list are employed. Therefore, securing a VANET requires processing messages about security in a secure and efficient manner. As elsewhere, the certificates used in a VANET must be revoked in circumstances such as the compromise or loss of a private key and illegal use of certificates[19].

The CA can issue a CRL and store it on a Lightweight Directory Access Protocol (LDAP) server for retrieval[20]. A vehicle can also use an Online Certificate Status Protocol (OCSP) to request for a CRL[21]. Instead of directly accessing the Internet, a vehicle in a VANET often accesses the Internet through an infrastructure domain. Thus, both retrieving CRL from an LDAP server and requesting CRL using OCSP are inapplicable.

VII tries to distribute CRL to vehicles through RSU broadcast[3]. This method requires a very large number of RSUs and is costly. In Ref. [4], Haas et al. attempted to propagate a CRL in an epidemic fashion. The epidemic method can distribute CRLs to all vehicles with a less number of RSUs and less time, but it requires large storage and communication capacity in the VANET.

In Ref. [6], the mobile phone users' trajectories prove that human movements follow simple reproducible patterns. According to the research results in Refs. [14, 22, 23], a VANET is a small world. In Ref. [24], a query processing algorithm that can determine the scope of each query is used to help a vehicle to avoid returning overwhelming amount results. These works give us clues to accurately distributing messages in a VANET.

Our previous work proposed the meet-table to optimize CRL propagation in a VANET[5]. Our other previous work proposed the concept of negative message and gave a scheme to distribute negative messages based on the meet-table and cloud computing[7]. Both works opted not to simulate the security of the meet-table. In the current work, we simulate fake meet-table attack and DoS attack of RSUs and analyze the simulation results.

7 Conclusion

We extend the concept of negative messages to negative message documents in a VANET, formally define the

coverage percentage and the accurate coverage percentage, and present the evaluation criteria of distribution method accordingly. Through formal analysis of the proposed meet-cloud, we observe that the meet-cloud features low communication and storage complexities in comparison with the RSU broadcast and epidemic model. The simulation results show that the meet-cloud achieves both high coverage percentage and high accurate coverage percentage and mid message delay. The simulation results of the fake meet-table attack and the DoS attack of RSUs demonstrate that meet-cloud is secure and works properly under these attacks. Therefore, the meet-cloud performs better than the RSU broadcast and epidemic model in distributing negative messages in a VANET.

Via analyzing the results under the attacks, we recognize that the meet-cloud possesses the attributes of both RSU broadcast and epidemic model. The meet-cloud uses the meet-table to select several RSUs as the start points of the epidemic model.

In our future work, we will apply fog computing[25, 26] to optimize meet-cloud, to reduce bandwidth and storage requirements of the cloud service, and to move the computing requirements from cloud to the edge.

Acknowledgment

This work was supported by the National Natural Science Foundation of China (No. 61262072).

References

[1] M. S. Kakkasageri and S. S. Manvi, Information management in vehicular ad hoc networks: A review, *J. Netw. Comput. Appl.*, vol. 39, pp. 334–350, 2014.

[2] H. Z. Zhu, M. L. Li, L. Y. Fu, G. T. Xue, Y. M. Zhu, and L. M. Ni, Impact of traffic influxes: Revealing exponential intercontact time in urban VANETs, *IEEE Trans. Parallel Distrib. Syst.*, vol. 22, no. 8, pp. 1258–1266, 2011.

[3] P. B. Farradyne, Vehicle Infrastructure Integration-VII Architecture and Functional Requirements, v1.0. 2005; http://ral.ucar.edu/project/vii.old/vii/docs/VIIArchandFuncRequirements.pdf.

[4] J. J. Haas, Y. C. Hu, and K. P. Laberteaux, Efficient certificate revocation list organization and distribution, *IEEE J. Sel. Areas Commun.*, vol. 29, no. 3, pp. 595–604, 2011.

[5] B. H. Huang, J. W. Mo, Q. Lu, and W. Cheng, Optimizing propagation network of certificate revocation in VANET with meet-table, in *Proc. 4^{th} Int. Workshop on Network Optimization and Performance Evaluation*, Zhangjiajie, China, 2016, pp. 147–154.

[6] M. C. González, C. A. Hidalgo, and A. L. Barabási, Understanding individual human mobility patterns, *Nature*, vol. 453, no. 7196, pp. 779–782, 2008.

[7] B. H. Huang and W. Cheng, Distributing negative messages in VANET based on meet-table and cloud computing, in *Proc. 12^{th} Int. Conf. on Wireless Algorithms, Systems, and Applications*, Guilin, China, 2017, pp. 653–664.

[8] R. Cattell, Scalable SQL and NoSQL data stores, *ACM SIGMOD Rec.*, vol. 39, no. 4, pp. 12–27, 2010.

[9] X. B. Tian, B. H. Huang, and M. Wu, A transparent middleware for encrypting data in MongoDB, in *Peoc. 2014 IEEE Workshop on Electronics, Computer and Applications*, Ottawa, Canada, 2014, pp. 906–909.

[10] L. Yu, H. Y. Shen, K. Sapra, L. Ye, and Z. P. Cai, CoRE: Cooperative end-to-end traffic redundancy elimination for reducing cloud bandwidth cost, *IEEE Trans. Parallel Distrib. Syst.*, vol. 28, no. 2, pp. 446–461, 2017.

[11] L. Yu and Z. P. Cai, Dynamic scaling of virtual clusters with bandwidth guarantee in cloud datacenters, in *Proc. 35^{th} Annu. IEEE Int. Conf. on Computer Communications*, San Francisco, CA, USA, 2016, pp. 1–9.

[12] E. Ndashimye, S. K. Ray, N. I. Sarkar, and J. A. Gutiérrez, Vehicle-to-infrastructure communication over multi-tier heterogeneous networks: A survey, *Comput. Netw.*, vol. 112, pp. 144–166, 2017.

[13] T. Bouali, S. M. Senouci, and H. Sedjelmaci, A distributed detection and prevention scheme from malicious nodes in vehicular networks, *Int. J. Commun. Syst.*, vol. 29, no. 10, pp. 1683–1704, 2016.

[14] J. X. Ding, J. Gao, and H. Xiong, Understanding and modelling information dissemination patterns in vehicle-to-vehicle networks, in *Proc. 23^{rd} SIGSPATIAL Int. Conf. on Advances in Geographic Information Systems*, Seattle, Washington, DC, USA, 2015, p. 41.

[15] V. Naumov, R. Baumann, and T. Gross, An evaluation of inter-vehicle ad hoc networks based on realistic vehicular traces, in *Proc. 7^{th} ACM Int. Symposium on Mobile ad Hoc Networking and Computing*, Florence, Italy, 2006, pp. 108–119.

[16] San Francisco Municipal Transportation Agency, San Francisco transportation fact sheet, 2013, https://www.sfmta.com/sites/default/files/ 2013%20SAN%20FRANCISCO%20TRANSPORTATION %20FACT%20SHEET.pdf.

[17] W. Reisman, Commute speeds have slowed down for San Francisco drivers 2011, http://archives.sfexaminer.com/sanfrancisco/commute-speeds-have-slowed-down-for-san-francisco-drivers/ Content?oid=2187521.

[18] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, VANET security surveys, *Comput. Commun.*, vol. 44, pp. 1–13, 2014.

[19] S. Chokhani, Toward a national public key infrastructure, *IEEE Commun. Mag.*, vol. 32, no. 9, pp. 70–74, 1994.

[20] Y. S. Yeh, W. S. Lai, and C. J. Cheng, Applying lightweight

directory access protocol service on session certification authority, *Computr. Netw.*, vol. 38, no. 5, pp. 675–692, 2002.

[21] T. P. Hormann, K. Wrona, and S. Holtmanns, Evaluation of certificate validation mechanisms, *Comput. Commun.*, vol. 29, no. 3, pp. 291–305, 2006.

[22] F. D. Cunha, A. C. Vianna, R. A. F. Mini, and A. A. F. Loureiro, Are vehicular networks small world?, in *Proc.* 2014 *IEEE Conf. on Computer Communications Workshops*, Toronto, Canada, 2014, pp. 195–196.

[23] H. Zhang and J. Li, Modeling and dynamical topology properties of VANET based on complex networks theory, *AIP Adv.*, vol. 5, p. 017150, 2015.

[24] X. J. Wang, L. J. Guo, C. Y. Ai, J. B. Li, and Z. P. Cai, An urban area-oriented traffic information query strategy in VANETs, in *Proc.* 8^{th} *Int. Conf. on Wireless Algorithms, Systems, and Applications*, Zhangjiajie, China, 2013, pp. 313–324.

[25] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, Fog computing and its role in the internet of things, in *Proc.* 1^{st} *Edition of the MCC Workshop on Mobile Cloud Computing*, Helsinki, Finland, 2012, pp. 13–16.

[26] V. G. Menon, Moving from vehicular cloud computing to vehicular fog computing: Issues and challenges, *Int. J. Comput. Sci. Eng.*, vol. 9, no. 2, pp. 14–18, 2017.

Baohua Huang is an associate professor and a graduate supervisor in the School of Computer and Electronic Information, Guangxi University, China. He received the PhD degree in computer science from Huazhong University of Science and Technology, China, in 2006. He is a senior member of CCF, a member of ACM and IEEE. His research interests include vehicular ad hoc network, network security, database security, etc.

Xiaolu Cheng is currently a PhD student in the Department of Computer Science, Virginia Commonwealth University, USA. She received the bachelor degree from Shandong University of Science and Technology, China, in 2013. She earned a master of Computer Science from Virginia Commonwealth University, USA, in 2016. Her research interests include vehicular network and sensor network.

Caixia Huang is an associate professor in the School of Computer Engineering and Applied mathematics, Changsha University. She received the BS and MS degree from National University of Defense Technology in 2000 and 2014, respechively. Her research interests include computer architecture, ad hoc, and sensor networking (localization, deployment and topology control, routing, etc.).

Wei Cheng is an assistant professor in the Department of Computer Science, Virginia Commonwealth University. He received the PhD degree in computer science from the George Washington University, Washington DC, in 2010. He is a member of IEEE and ACM. His research interests include localization, RFID system on road, security, and underwater networks.