A Study on Efficient Authentication Method for V2V Communication

Zhang Ke Monica

A Study on Efficient Authentication Method for V2V Communication

Content

1. VANET (VEHICULAR AD-HOC NETWORK)

In the ever-changing Internet age, Internet are not limited to linking humans together. With the concept of the Internet of Things brought out, VANET, vehicular ad-hoc network, as a major branch of the Internet of Things is gradually emerging and has aroused the attention of scientific research institutions and automobile manufacturers.

Development and Security Problems in VANET

Information security problems hidden in the VANET are concerned by people. The IEEE 1609.2 standard provides a reference for the vehicle manufactures in information security designation for VANET, but there are still some details in IEEE 1609.2 standard can be optimized.

2. Cryptology Background Knowledge

Digital Signature

X.509 format Digital Certification

3. System Designation

A Study on Efficient Authentication Method for V2V Communication

Using NS-3 to simulate communication system

By utilizing NS-3 simulator to construct a ad-hoc network, importing OpenSSL to support cryptology algorithms, I perform simulations both on the improved system and the system applying original IEEE1609.2 standard.

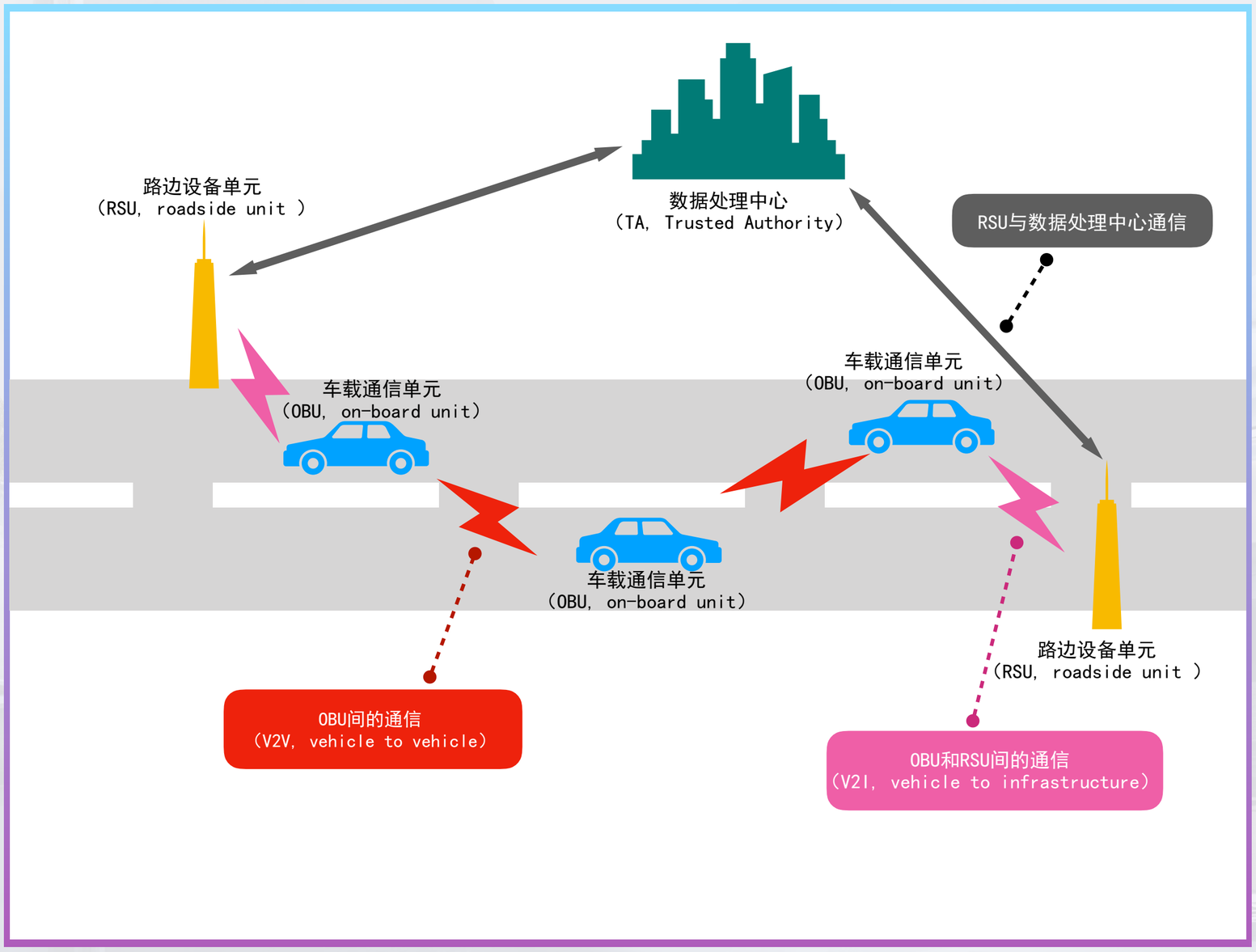
Simulations

4. Results and Analysis

1. VANET

A Study on Efficient Authentication Method for V2V Communication

1. VANET
Structure of VANET



VANET is consisted of 3 entities:

OBU, On-Board Unit

RSU, Roadside Unit

TA, Trusted Authority

Communications in VANET:

V2V, vehicle to vehicle communication

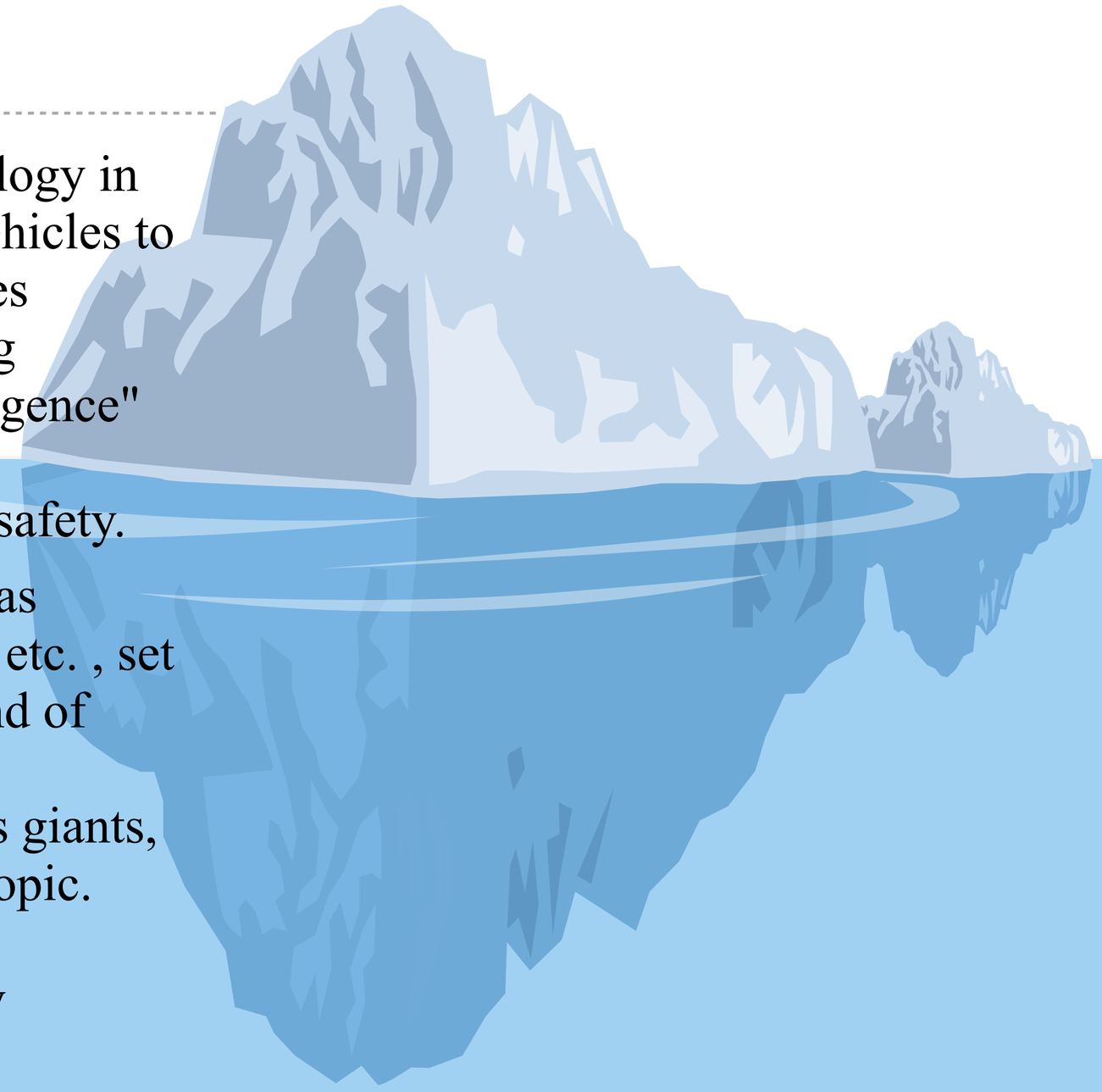
V2I, vehicle to infrastructure communication

communication between RSU and TA

Development

VANET is the most promising technology in mobile Ad Hoc network. It enables vehicles to exchange information, and summarizes remote information by interconnecting vehicles, thereby enhances the "intelligence" of vehicles, and achieves the goal of improving road traffic efficiency and safety.

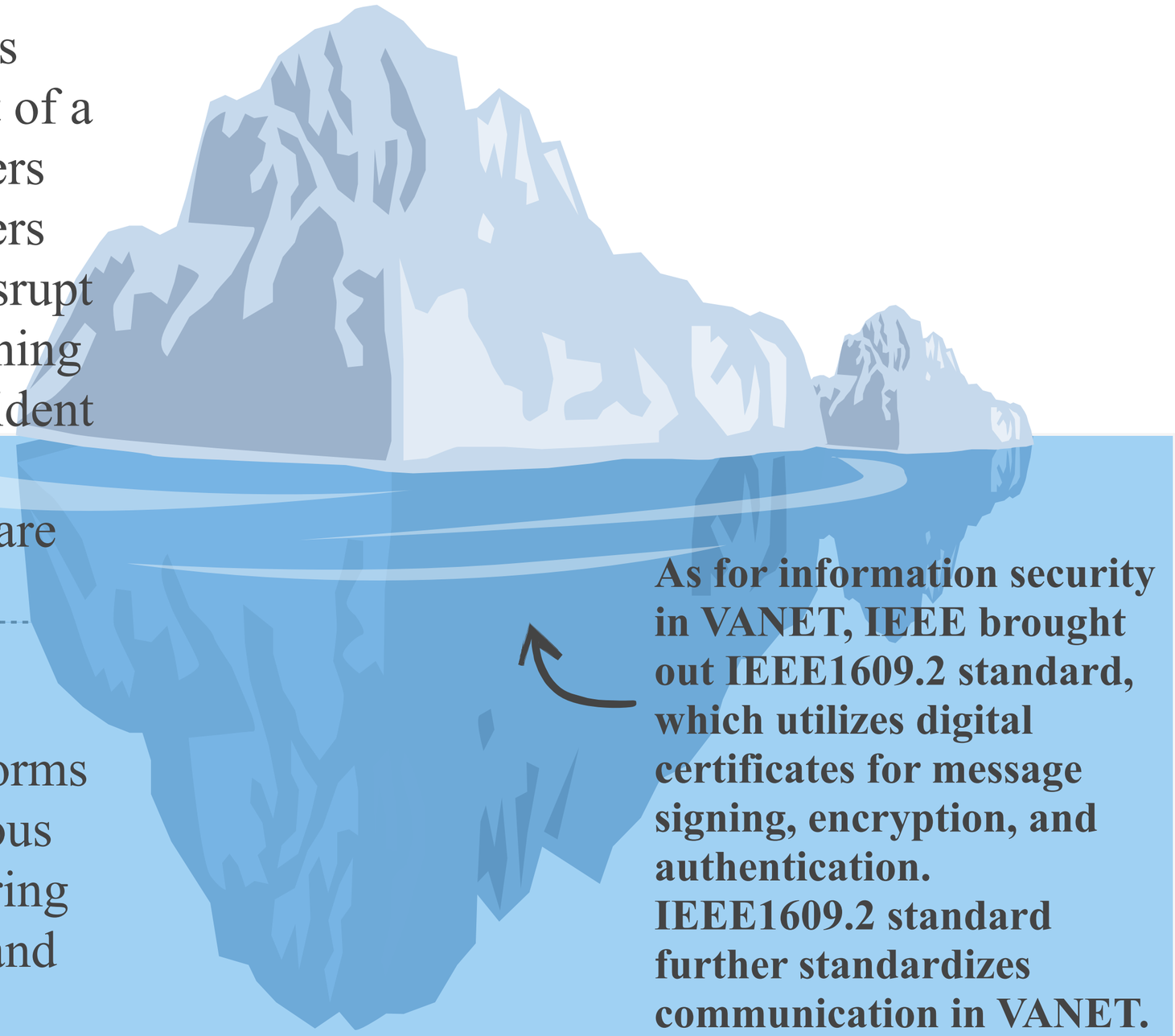
Numbers of famous companies, such as Google, Alibaba, Baidu, Tencent and etc. , set up their VANET teams to join the trend of developing this frontier technique.
With the promotion of these industry's giants, VANET immediately becomes a hot topic.
Economic benefits of the business opportunities in VANET are gradually emerging.



1. VANET

Development and Security Problems in VANET

During the communication, attackers may modify the information content of a data package to mislead data receivers about the source of message; attackers may also create fake messages to disrupt the traffic. In the process of establishing VANET, the need for reproduce accident scene and the importance of tracing correct time sequence for accidents are also increasing.



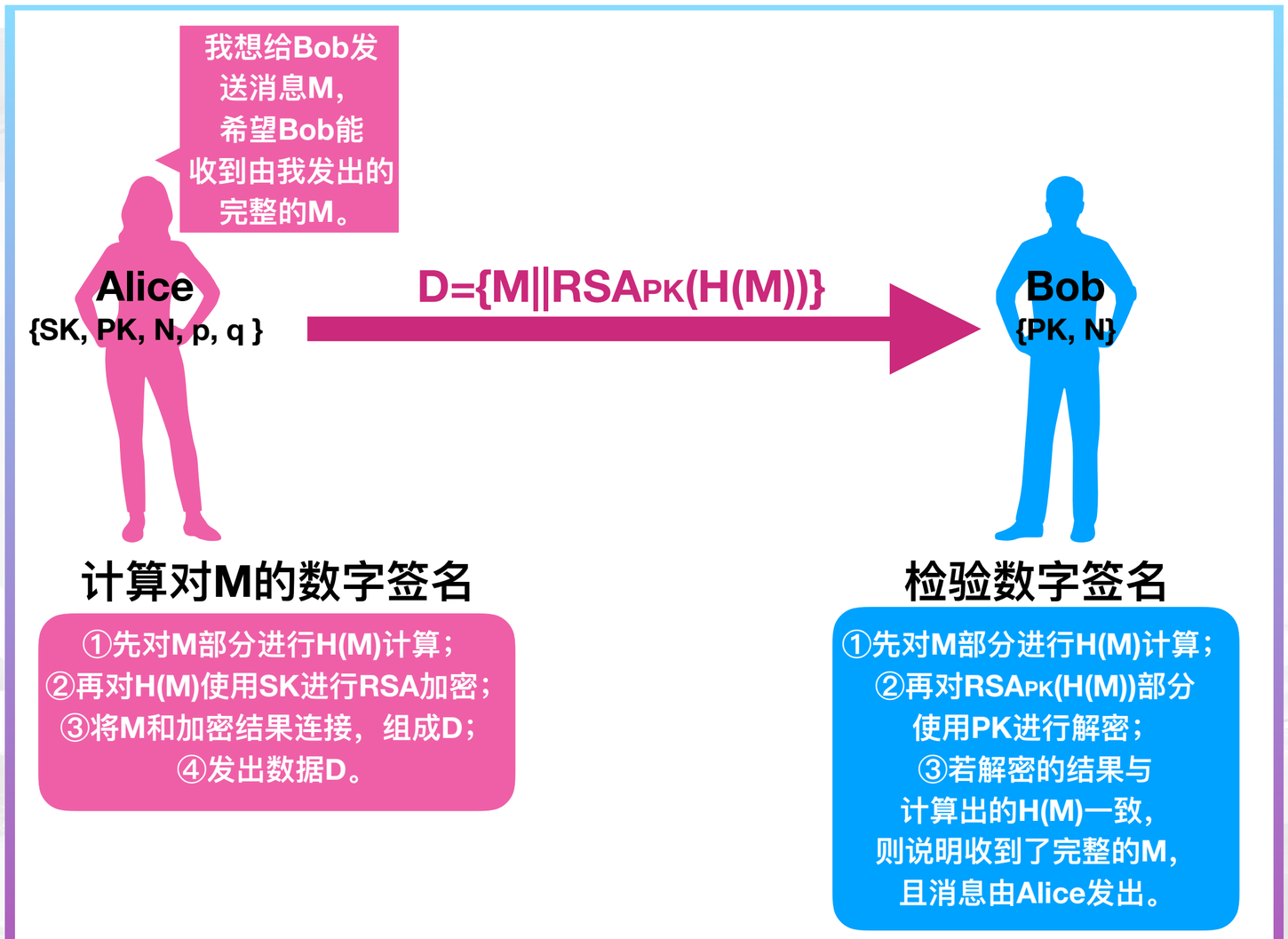
Security Issues

Since the V2V communication performs in wireless network, false or erroneous traffic injection and message tampering may pose a threat to the credibility and security of the VANET.

As for information security in VANET, IEEE brought out IEEE1609.2 standard, which utilizes digital certificates for message signing, encryption, and authentication. IEEE1609.2 standard further standardizes communication in VANET.

2. Cryptology Background Knowledge

2. Cryptology Background Knowledge
Digital signature



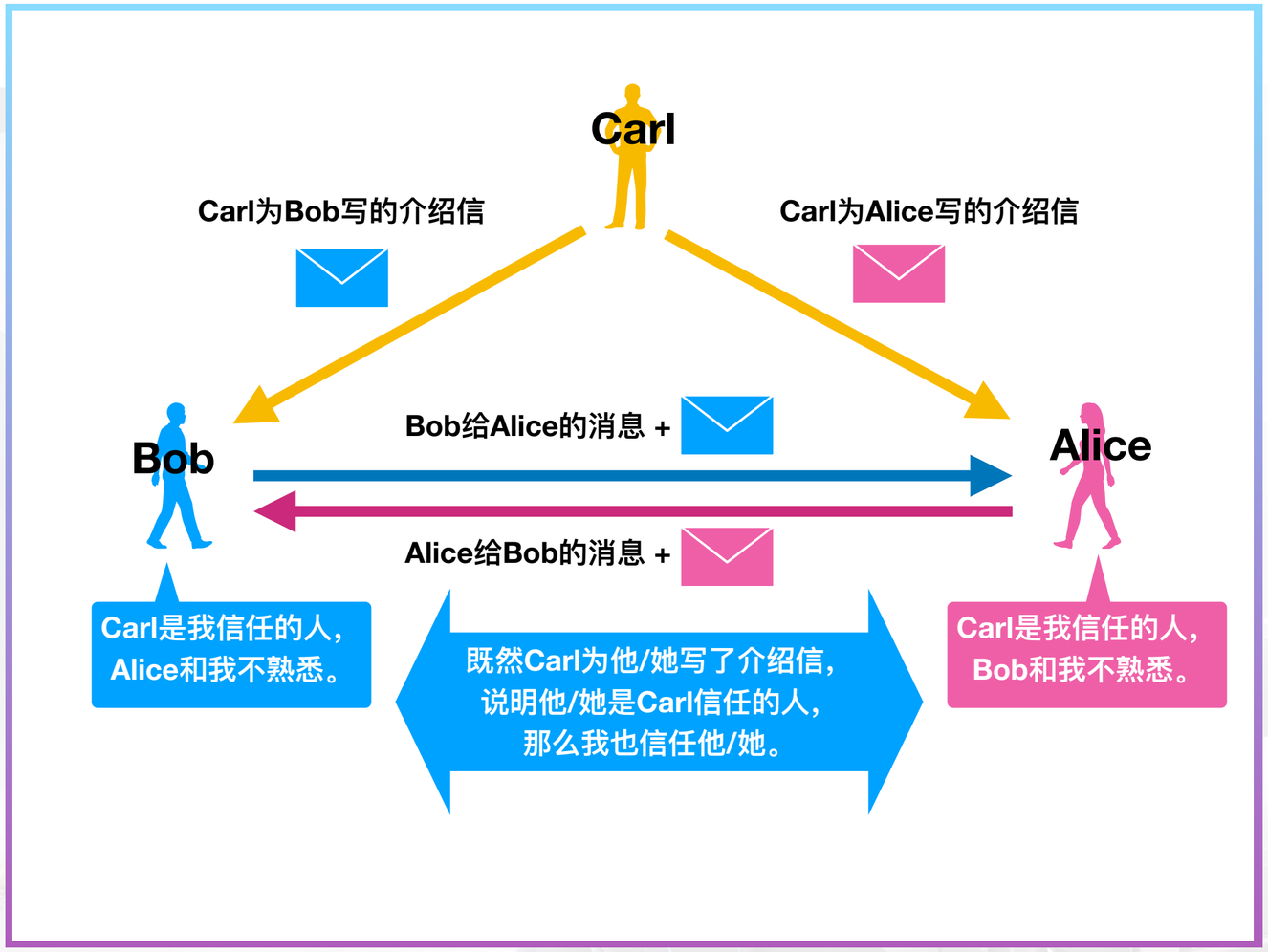
RSA

1. Randomly choose 2 distinct prime number p and q;
2. Compute N *and* $\varphi(N)$. $N = p \times q$, $\varphi(N) = (p - 1) \times (q - 1)$, $\varphi(N)$ is the Euler totient function of N;
3. Generate a random number e as the private key, where $1 < e < \varphi(N)$ *and* $\gcd(e, \varphi(N)) = 1$;
4. Compute the public key d , where $d \cdot e \equiv 1 \bmod \varphi(N)$;
5. Use M to present the original data, and use C to present the encrypted data. Relationship between M and C is:

$$C \equiv M^e \bmod N, \quad M \equiv C^d \bmod N.$$

2. Cryptology Background Knowledge

X.509 format digital certification



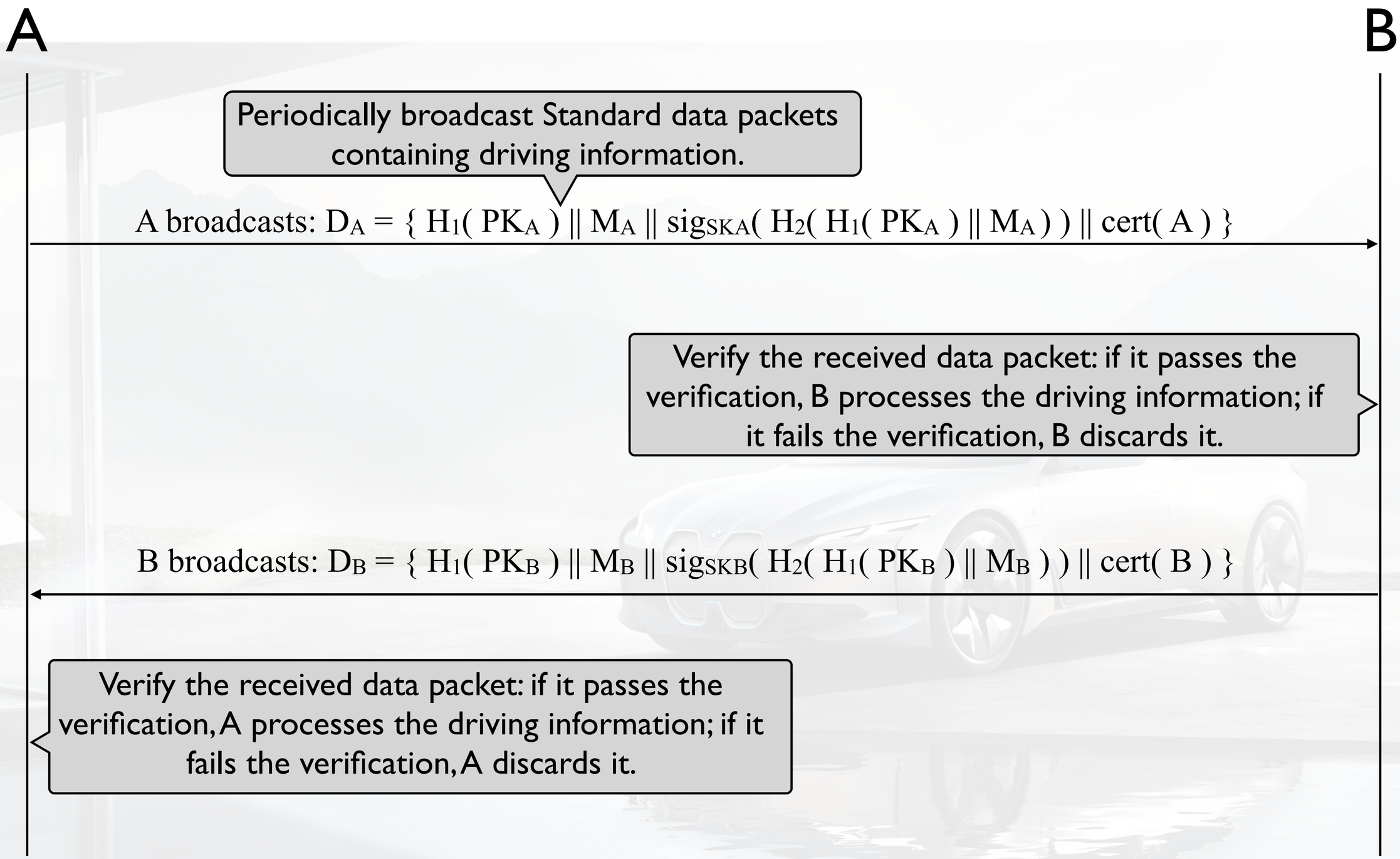
消息密文 $Enc_{pubb}(M)$	签名 $Sig_{priva}(H(Enc_{privb}(M)))$	数字证书

CA is trusted by entities on Internet, and the entity carries with digital certification signed by trusted CA is regarded as trusted by data receiver.

3. System Designation

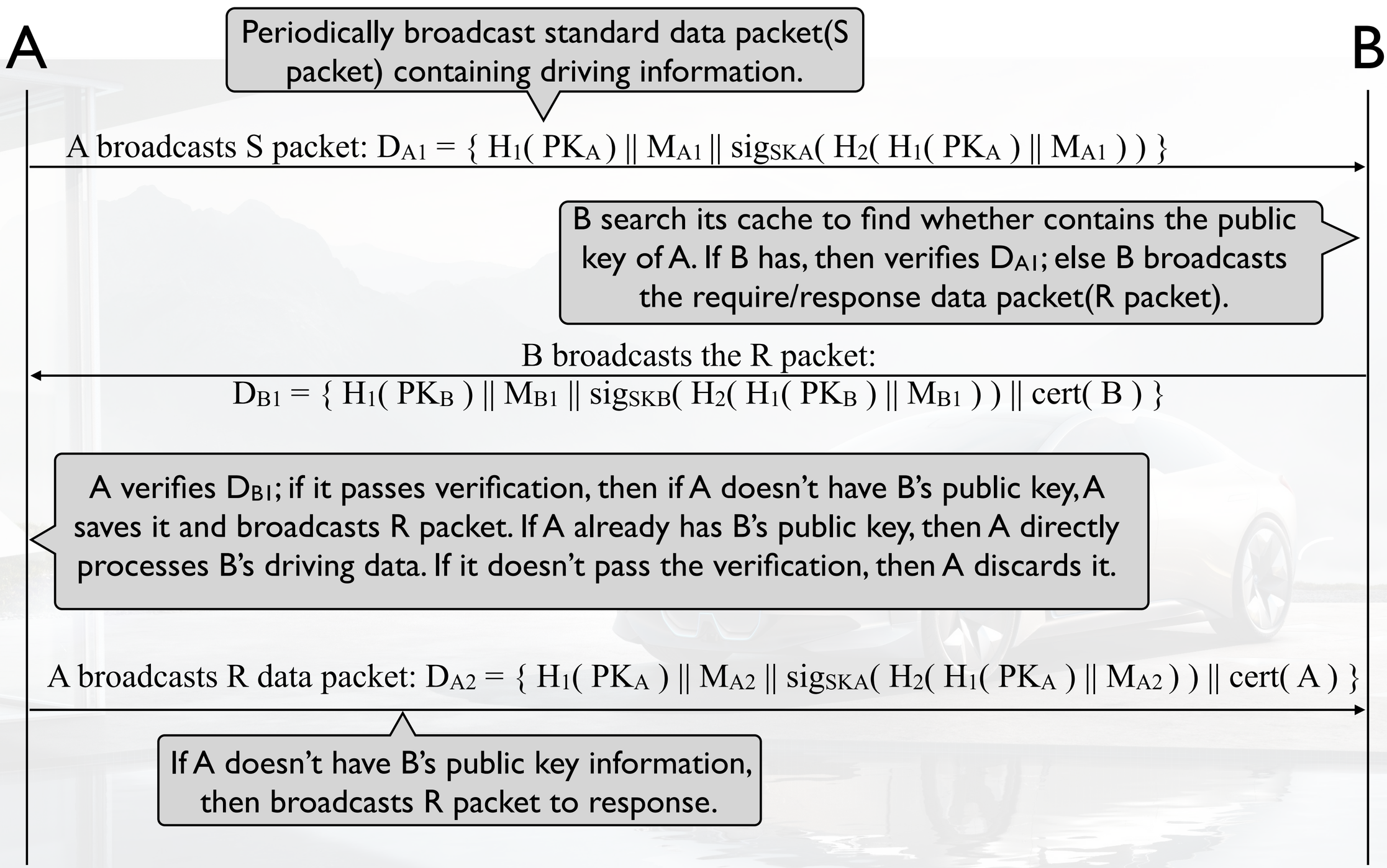
A Study on Efficient Authentication Method for V2V Communication

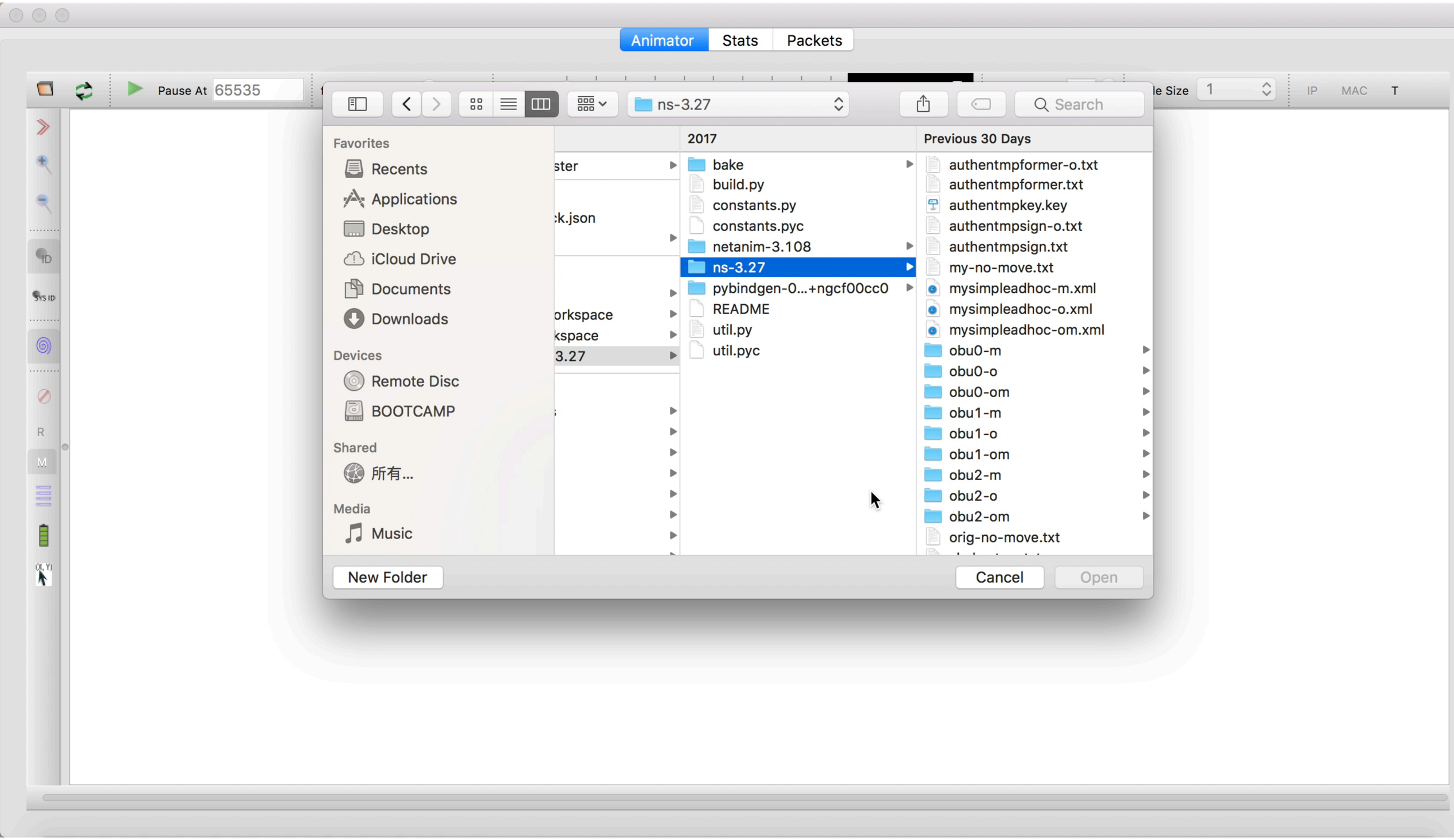
3. System Designation
IEEE 1609.2 Standard



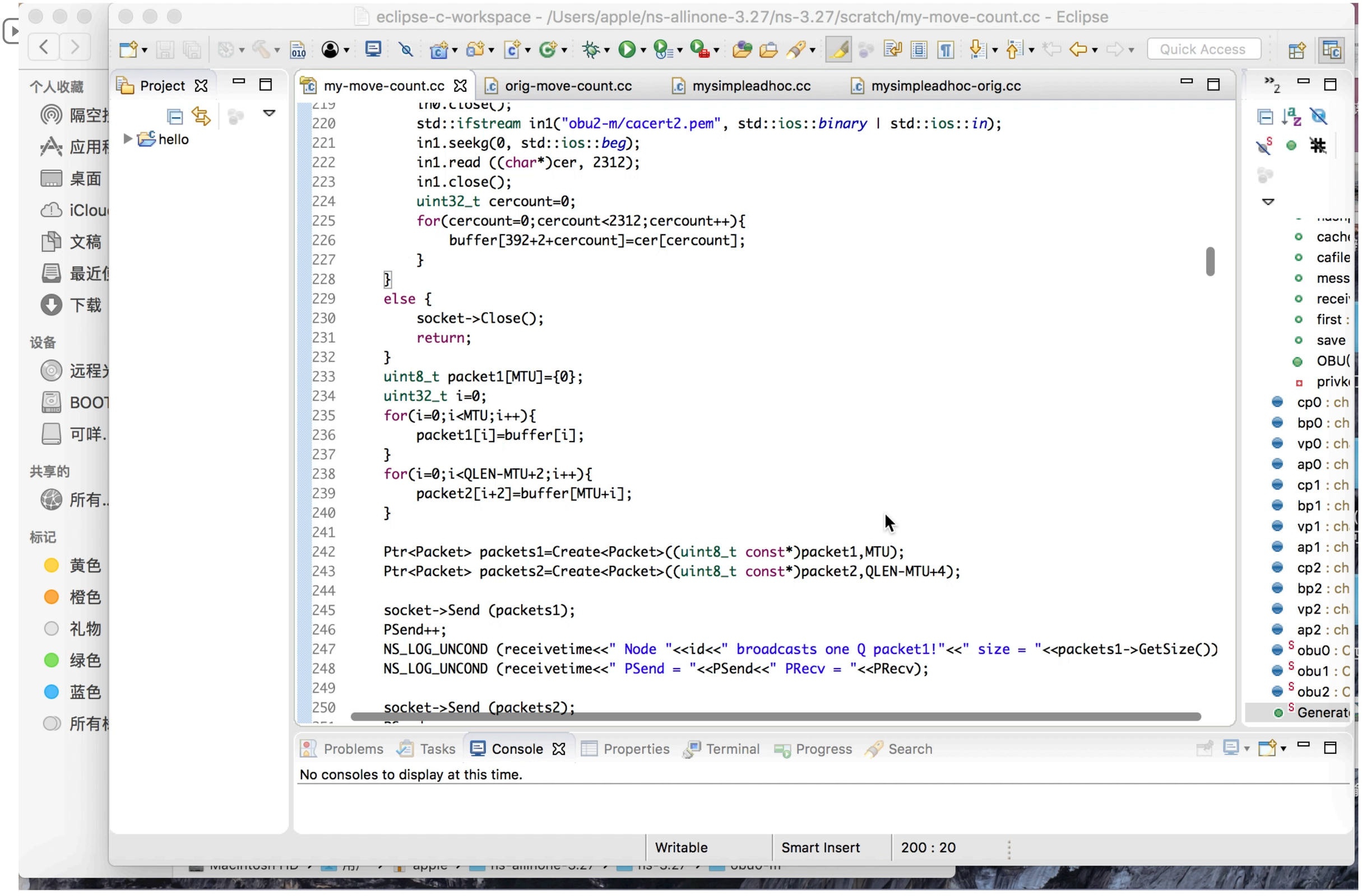
3. System Designation

A Study on Efficient Authentication Method for V2V Communication





A Study on Efficient Authentication Method for V2V Communication


eclipse-c-workspace - /Users/apple/ns-allinone-3.27/ns-3.27/scratch/my-move-count.cc - Eclipse
Quick Access
Project
hello
my-move-count.cc
orig-move-count.cc
mysimpleadhoc.cc
mysimpleadhoc-orig.cc
std::ifstream in1("obu2-m/cacert2.pem", std::ios::binary | std::ios::in);
in1.seekg(0, std::ios::beg);
in1.read ((char*)cer, 2312);
in1.close();
uint32_t cercount=0;
for(cercount=0;cercount<2312;cercount++){
buffer[392+2+cercount]=cer[cercount];
}
}
else {
socket->Close();
return;
}
uint8_t packet1[MTU]={0};
uint32_t i=0;
for(i=0;i<MTU;i++){
packet1[i]=buffer[i];
}
for(i=0;i<QLEN-MTU+2;i++){
packet2[i+2]=buffer[MTU+i];
}
Ptr<Packet> packets1=Create<Packet>((uint8_t const*)packet1,MTU);
Ptr<Packet> packets2=Create<Packet>((uint8_t const*)packet2,QLEN-MTU+4);
socket->Send (packets1);
PSend++;
NS_LOG_UNCOND (receivetime<<" Node "<<id<<" broadcasts one Q packet1!"<<" size = "<<packets1->GetSize())
NS_LOG_UNCOND (receivetime<<" PSend = "<<PSend<<" PRecv = "<<PRecv);
socket->Send (packets2);
Problems
Tasks
Console
Properties
Terminal
Progress
Search
No consoles to display at this time.
Writable
Smart Insert
200 : 20
cp0 : ch
bp0 : ch
vp0 : ch
ap0 : ch
cp1 : ch
bp1 : ch
vp1 : ch
ap1 : ch
cp2 : ch
bp2 : ch
vp2 : ch
ap2 : ch
obu0 : C
obu1 : C
obu2 : C

4. Results and Analysis

4. Results and Analysis

Time consuming

S packets

（发送方，接收方）	传输距离（m）	发送时间（10^{-9}s）	接收时间（10^{-9}s）	间隔时间（10^{-9}s）	平均时长（10^{-9}s）
(OBU0,OBU1)	7.71	1000000000.0	1003848023.0	3848023.0	3848023.0
		5000000000.0	5003848023.0	3848023.0	
		9000000000.0	9003848023.0	3848023.0	
(OBU1,OBU0)		2000000000.0	2003848023.0	3848023.0	
		6000000000.0	6003848023.0	3848023.0	
		1000000000.0	11003848023.0	3848023.0	
(OBU1,OBU2)	5.0	2000000000.0	2003848016.0	3848016.0	3848016.0
		6000000000.0	6003848016.0	3848016.0	
		1000000000.0	10003848016.0	3848016.0	
(OBU2,OBU1)		3000000000.0	3003848016.0	3848016.0	
		7000000000.0	7003848016.0	3848016.0	
		11000000000.0	11003848016.0	3848016.0	
(OBU2,OBU0)	11.18	3000000000.0	3003848037.0	3848037.0	3848037.0
		7000000000.0	7003848037.0	3848037.0	
		11000000000.0	11003848037.0	3848037.0	
(OBU0,OBU2)		1000000000.0	1003848037.0	3848037.0	
		5000000000.0	5003848037.0	3848037.0	
		9000000000.0	9003848037.0	3848037.0	

R packets

（发送方，接收方）	传输距离	发送时间（10^{-9}s）	接收时间（10^{-9}s）	间隔时间（10^{-9}s）	平均时长（10^{-9}s）
(OBU0,OBU1)	7.71	1000000000.0	1023510023.0	23510023.0	31140055.6
		3023450023.0	3059804134.0	36354111.0	
		8211050357.0	8234480380.0	23430023.0	
(OBU1,OBU0)		2000000000.0	2023450023.0	23450023.0	
		2023510023.0	2070420108.0	46910085.0	
		6190318272.0	6224134341.0	33186069.0	
(OBU1,OBU2)	5.0	2000000000.0	2023450016.0	23450016.0	31674665.0
		2023510023.0	2070420101.0	46910078.0	
		3059874085.0	3093930133.0	34056048.0	
(OBU2,OBU1)		2023510037.0	2059874085.0	36363748.0	
		3000000000.0	3023410016.0	23410016.0	
		4093930133.0	4119788217.0	25858084.0	
(OBU2,OBU0)	11.18	3000000000.0	3023410037.0	23410037.0	25570730.4
		4093930133.0	4119788196.0	25858063.0	
		6142938256.0	6166168293.0	23230037.0	
(OBU0,OBU2)		1000000000.0	1023510037.0	23510037.0	
		3023450023.0	3059804148.0	36354125.0	
		7224134341.0	7245196424.0	21062083.0	

4. Results and Analysis

Time consuming

Comprehensive Analysis

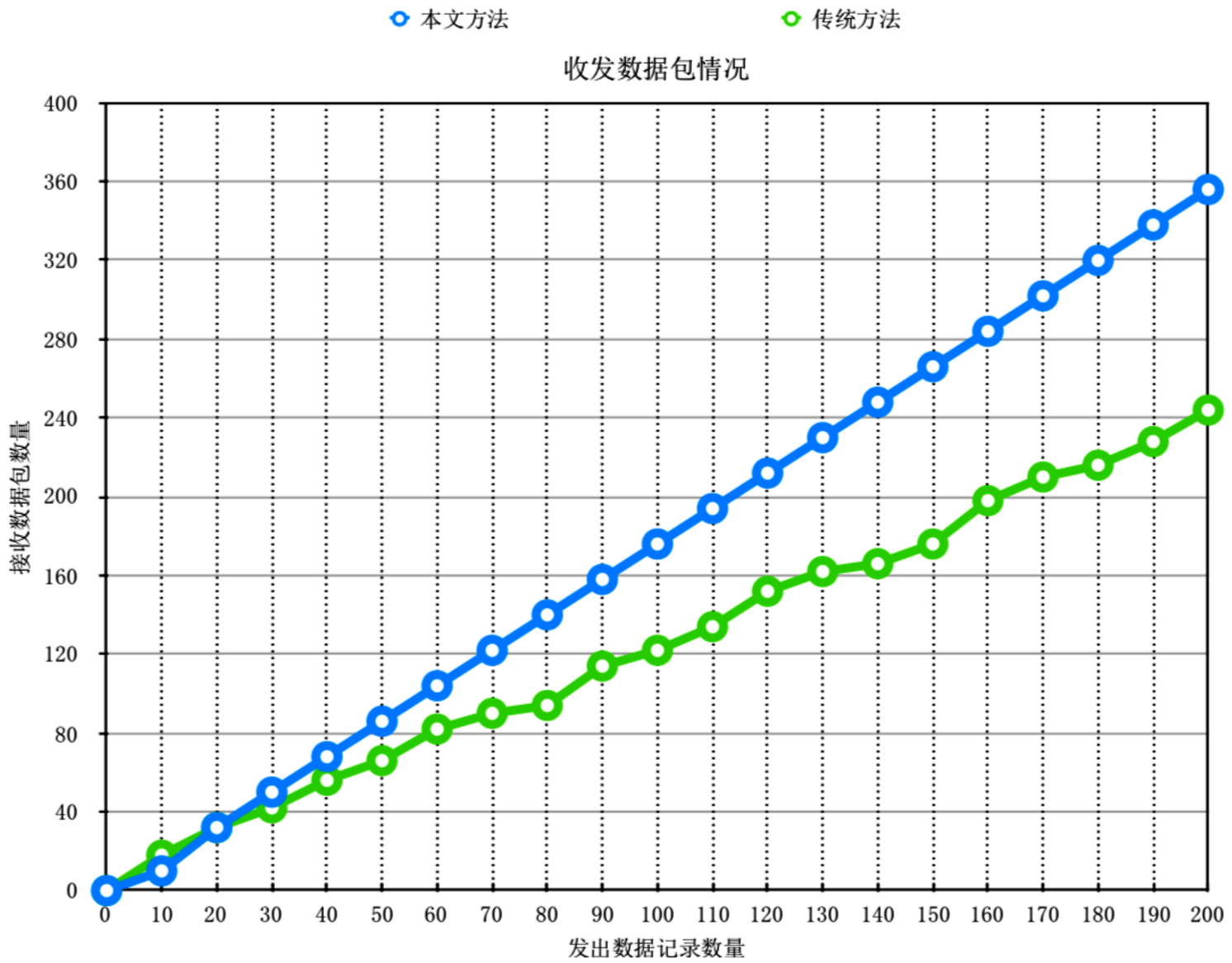
数据收发平均时长	OBU0 与 OBU1 之间	OBU0 与 OBU2 之间	OBU1 与 OBU2 之间
标准数据包（10^{-9}s）	3848023.0	3848037.0	3848016.0
传统数据包（10^{-9}s）	31140055.6	25570730.4	31674665.0
$\frac{\text{传统数据收发时长}}{\text{标准数据收发时长}}$	8.09	6.65	8.23

4. Results and Analysis

Efficiency

收发数据包总数

发出数据记录总数	本文方法	传统方法
0	0	0
10	10	18
20	32	32
30	50	42
40	68	56
50	86	66
60	104	82
70	122	90
80	140	94
90	158	114
100	176	122
110	194	134
120	212	152
130	230	162
140	248	166
150	266	176
160	284	198
170	302	210
180	320	216
190	338	228
200	356	244

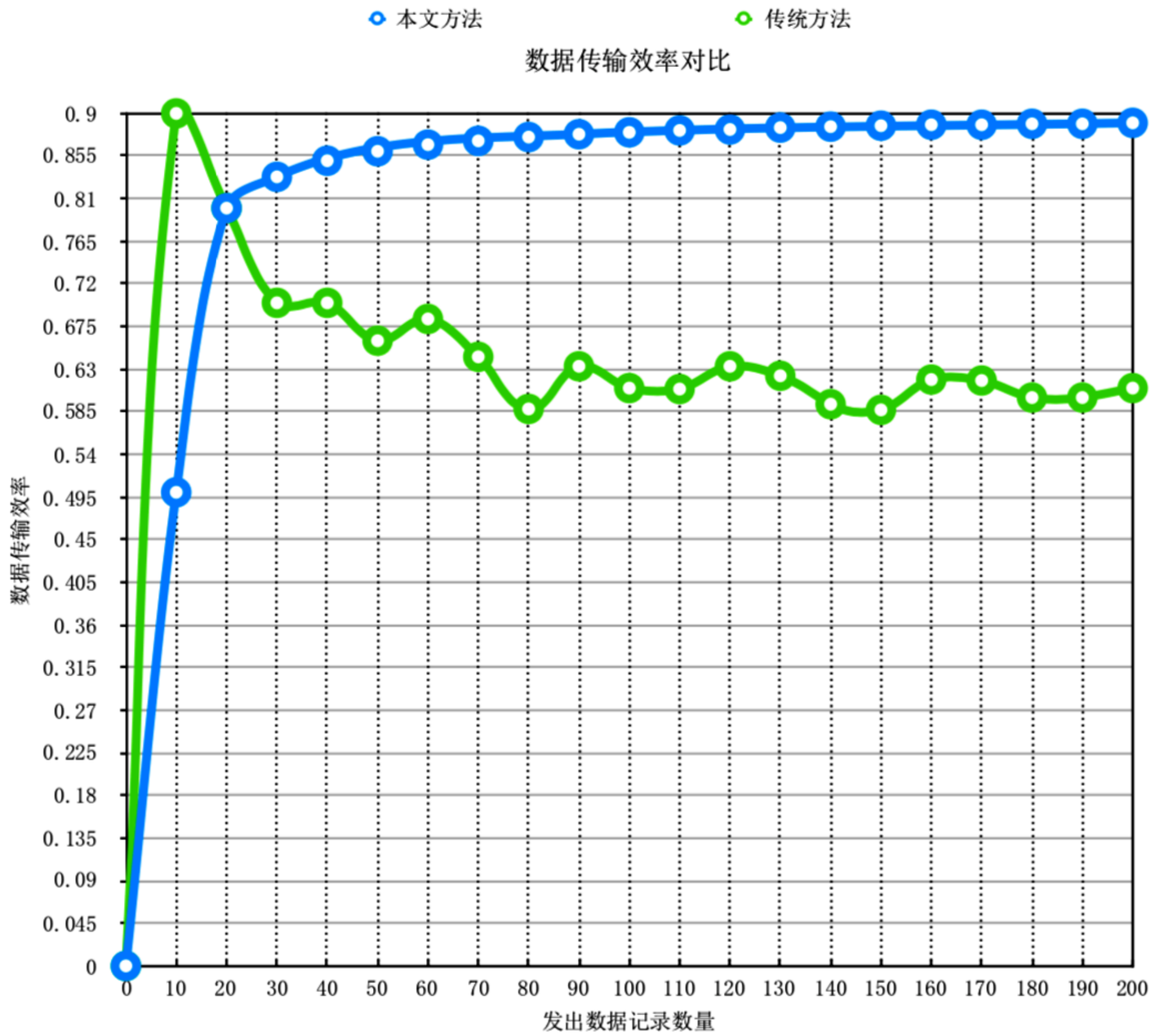


4. Results and Analysis

Efficiency

数据传输效率

发出数据记录总数	本文方法	传统方法
0	0	0
10	0.5	0.9
20	0.8	0.8
30	0.833	0.7
40	0.85	0.7
50	0.86	0.66
60	0.867	0.683
70	0.871	0.643
80	0.875	0.588
90	0.878	0.633
100	0.88	0.61
110	0.882	0.609
120	0.883	0.633
130	0.885	0.623
140	0.886	0.593
150	0.887	0.587
160	0.888	0.619
170	0.888	0.618
180	0.889	0.6
190	0.889	0.6
200	0.89	0.61



4. Results and Analysis
Conclusion

save more than 80% of the transmission time

increase the efficiency of data transmission by 45%

It can be seen that the method proposed in this paper improves the communication speed and stability of communication while ensuring the data security of communication. The new method is more conducive to the transmission of important data in V2V. By using the method proposed in this paper, traffic data loss in the VANET will be alleviated, and V2V communication in the reliable VANET will bring greater convenience to people. It will also provide tremendous assistance to the traffic management department and the government in traffic management and accident recovery.

Q&A

A Study on Efficient Authentication Method for V2V Communication

Zhang Ke Monica

A Study on Efficient Authentication Method for V2V Communication