Overview of extra-vehicular communication

Felix Myhsok, Holger Kinkelin*, Filip Rezabek*
*Chair of Network Architectures and Services, Department of Informatics
Technical University of Munich, Germany
Email: felix.myhsok@tum.de, kinkelin@net.in.tum.de, frezabek@net.in.tum.de

***Abstract*—Extra-vehicular communication is the key element of connected mobility. Therefor the identification of vehicles and the ability to authenticated information from vehicles need to be accomplished while preserving high privacy standards.**

In this paper an architecture for vehicle-to-everything communications is presented at the example of the European ETSI C-ITS standard. A public key infrastructure is thereby the commonly trusted approach to secure communications without compromising the entities privacy.

***Index Terms*—vehicle-to-everything communications, V2X, etsi c-its, public-key-infrastructure, PKI**

1. Introduction

The future of connected mobility and transport is based on extra-vehicular communications. By giving vehicles the ability to communicate and exchange information with their surroundings, improvements at mobility and road traffic can be achieved. Areas of improvement are mainly road-safety, efficiency and environmental pollution [1]. The concept of vehicles communicating with their environment is summarized in the term *vehicle-to-everything (V2X)* (also car-to-everything (C2X)) communication. V2X combines multiple communication applications such as *vehicle-to-vehicle (V2V)*, *vehicle-to-Infrastructure (V2I)*, and *vehicle-to-pedestrians (V2P)*. In each of them, a vehicle communicates with a surrounding entity using a data connection to share and collect information about the environment. This information can then be used to improve the decision-making process of the driver or in an autonomous concept of the vehicle itself. Some use cases as described by [2] are:

- emergency brake lights
- emergency warnings
- collision/intersection warnings
- road work warnings
- lane change assistance
- traffic light optimized speed
- cooperative automated cruise control

1.1. Communication architecture

In this section, we will describe the communication scheme of V2X followed by an overview of the transmission technology.

To equip a vehicle with V2X communication capabilities, it requires an explicit communication interface as part

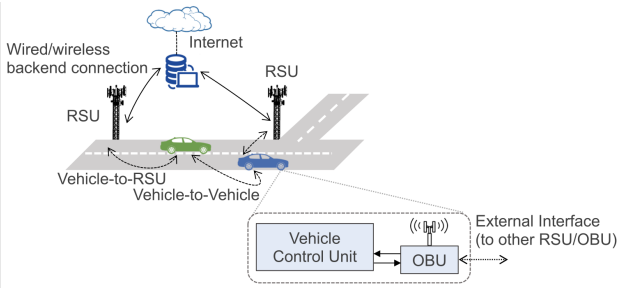

Figure 1: V2X Communication Scheme [3]

of its hardware. This external interface, called *on-board unit (OBU)*, connects intra-vehicular computing units to the outside world. Communication partners for OBUs are in most scenarios other OBUs (V2V communication) or infrastructure at the roadside, referred to as *roadside units (RSU)*(V2I communication). A graphic representation of the general communication scheme can be found in Figure 1. RSUs, like traffic lights or construction sites, can also serve as a gateway to other communication infrastructure. Thus communication partners are not necessarily located aside of the road, for example like databases or authorities. In this paper, these various communication partners like OBUs and RSUs, are referred to as other entities. [3]

In the currently existing concepts, there are two different approaches concerning the underlying technology for wireless transmissions: WiFi-based or cellular-based networks. Both approaches are briefly outlined in the following Sections 1.1.1 and 1.1.2. In Chapter 2 and 4, we focus on the WiFi-based approach of the European ETSI C-ITS standard.

1.1.1. WiFi-based communication. In this approach, the technology used to establish wireless communication is based on WiFi - more specific, on the IEEE 802.11p standard [4]. Communications via WiFi are often summarized under the term *Dedicated Short Range Communication (DSRC)*. The entities in the network communicate over a wireless adhoc network using the 5.9 GHz frequency. Therefore, every entity has an antenna to send, receive, or forward messages. Since the signal range of WiFi is usually limited to a few hundred meters, connections between two entities are mostly of shorter duration and the vehicle is not always connected to the network. Since the WiFi-technology is widely known and used, there are already different standards for V2X communications in production using this technology. The most most popular are:

doi: 10.2313/NET-2020-11-1_15

- ETSI Cooperative Intelligent Transport Systems (C-ITS) standard in Europe [5]
- Wireless Access for Vehicular Environment (WAVE) standard in the United States [6]
- ITS Connect standard in Japan (operates on the 700MHz band) [7]

1.1.2. Cellular-based communication. In cellular vehicle to everything (C-V2X) communications the network connection is established using Long Term Evolution (LTE) (3GPP Release 12) or 5G (Release 16) cellular networks. In this architecture, the vehicle communicates in most cases with base stations which provide a high ground coverage. Additionally, through the LTE-PC5 interface (also LTE-Sidelink) entities have the ability to communicate directly without using a base station [6].

This paper is structured as follows: Chapter 2 explains security challenges in V2X communications. In Chapter 3 the general concept of a public key infrastructure is summarized briefly before in Chapter 4 the concrete public key infrastructure used in the ETSI C-ITS standard explained and compared to the US WAVE standard.

2. Security challenges

In this chapter we outline the most important security challenges and threats for V2X communications. However the focus of this paper is on not authenticated messages and tracking of vehicles.

By establishing V2X communications, a vehicle relies not only on information obtained by itself (e.g. through sensors at the vehicle) but also on information generated by others. If this received information does not correspond to the reality it can cause severe damage to the driver, the vehicle or others. For example if the vehicle receives false information and as a result initiates an emergency breaking, this could lead to collisions and traffic jams. The source of this false information can either be from a malfunctioning entity in the network or a malicious entity. We consider an entity, which tries manipulate other entities by sending false information, as an attacker. In this paper we focus on malicious attacks.

Attack scenarios, like the ones described in [3], can be clustered in three categories by analyzing the underling attack strategy.

2.1. Denial of Service Attacks on the communication channel

The basic principle of *denial-of-service (DoS)* attacks, is to overload the receiving entity with more messages than it can process. Due to the lack of resources, important data can then be lost or not processed in time. These attacks can happen on different layers like simple physical frequency jamming or by acting as a router in an ad hoc network and dropping packets, as in a JellyFish Attack. They can also be spread over multiple nodes (distributed DoS [DDoS]) to increase the number of messages send and to bypass security measures. [8] DoS attacks are mostly geographically limited. For this reason, they only affect a limited amount of entities. There are existing techniques and concepts how to reduce impact of DoS attacks, which are explained in the further reading [9].

2.2. Insertion of not Authenticated Packets

If entities are not identifiable, attackers can take on any appearance they want. Thus they can send faked messages to manipulate other entities without being detected. This makes proper responses and prosecution of attackers more difficult. It also leads to multiple attack scenarios, which are explained in the following.

In **sybil attacks**, one attacker has more than one identity. Thus, he is able to send bogus information, e.g. about the traffic situation, to other entities. It can also be used to boost the trustworthiness of malicious entities or lower it for legitimate entities to increase the impact of false information. [3] [8]

Message replay attacks are used to reveal conditions or services at the receiving end. In general, an attacker records a valid message but resends it to a different time or location. For example, the attacker records the message send by a vehicle when it accesses a restricted area, for instance, a parking deck. Without security measures, an attacker could then just transmit this message again to gain access to this parking deck. [3] [8]

By using **false data injection attacks**, attackers can send bogus data to other entities to influence their behaviour. Thereby, the attacker simply alters the real-world situation. E.g. he transmits that he is 20 meters away when he is actually 200 meters away. Using this method, an attacker could affect e.g. the road traffic or trigger emergency brakes. [3] [8]

It is possible to counter these attacks with adding a unique identity to every entity in the network to sanction them for false behaviour. Furthermore it needs to be possible to authenticate if an entity belongs to the identity it is using. This can be achieved through cryptographic scheme with digital signatures as shown in Chapter 4. This, however, comes at the cost of privacy since tracking is possible. Nevertheless, authenticated messages do not provide complete security. Despite authentication, valid messages can be replayed by attackers or false information can be transmitted in an authenticated message if the entity is compromised. [3] [8]

2.3. Tracking of Vehicles

In a V2X communications architecture, privacy protection must be a vital part. In this paper we focus on privacy issues caused by identification of entities based on sent messages. Attackers can track the digital signatures broadcasted in messages. Other tracking methods like radio fingerprinting or mobile phone tracking are out of scope. [8]

Due to missing privacy protection, **identity revealing attacks** can be facilitated, where attackers are able to identify the vehicle driver. It allows the attackers to gather personal information about the driver (e.g. personal activities) which can lead to personal profiling. [8]

Another attack which can be prevented through privacy measures is the **location tracking** of a vehicle. This attack tracks movements and current position of the vehicle and can, for example, be used in combination with identity revealing to track a person's movements. [8]

doi: 10.2313/NET-2020-11-1_15

3. Background: General architecture of a PKI

This chapter provides background information for a better understanding of a public key infrastructure and asymmetric encryption schemes.

A *public key infrastructures (PKI)* main purpose is to give every participant a digital identity and ensure the authenticity of it.

Therefore, a PKI delivers certificates for every entity based on a signing process with asymmetric keys and digital signatures. Every entity owns a unique pair of keys, which consist of a public key and a private key. The public key is accessible for everyone while the private key is kept secret by the owning entity. A *certification authority (CA)* serves as a trusted third party and issues certificates to all participants in the network. Certificates Certificate bind the identity of a participant to the key that belongs to the participant. To prove authenticity and validity of the certificate, the issuing CA signs the certificate using its own private key. [10]

To ensure that the CA is trustworthy, the CA also owns a certificate. This certificate is created and signed by another CA. Through this process certificate chains are build up. Every chain has its root in one common *Root Certification Authority (RCA)*. A RCA is an anchor that needs to be trusted by everyone in the certificate chain. [10]

When two entities are now communicating, the sender signs (encrypt) the data with his private key. The receiving entity can then use the public key from the sender's certificate to decrypt the message. This allows the recipient to verify the identity of the sender. Since the public and private key is a unique combination, only the certificate corresponding participant can successfully sign the data with its private key. Furthermore, the recipient can verify whether the certificate of the sender is valid by analyzing the certificate of the issuing authority. [10]

If a participant e.g. behaves incorrectly or the private key of the participant is compromised, the participant needs to be excluded from the PKI. Therefore his certificate gets revoked. The mostly used approach therefore is a *Certificate Revocation List (CRL)*. This CRL contains all revoked certificates and allows to check if a specific certificate is revoked. Revocation of certificates is also a task of a CA. [10]

4. The PKI in the C-ITS standard

A PKI can solve attack scenarios caused by unauthorized entities by giving every entity a unique identification. Furthermore, the PKI which is used for V2X, was also specifically designed to protect privacy to encounter tracking of vehicles. [11] In this section, we briefly explain the functionality of the PKI proposed in the C-ITS standard and the used certificates. Some aspects are fairly similar to the approaches proposed in the WAVE standard and some differences are outlined in Section 4.3.

In the V2X context the PKI main goals are to issue valid certificates to every entity, to minimize the abuse of issued certificates and to exclude malicious entities of the network. Therefor the private key needs to be securely

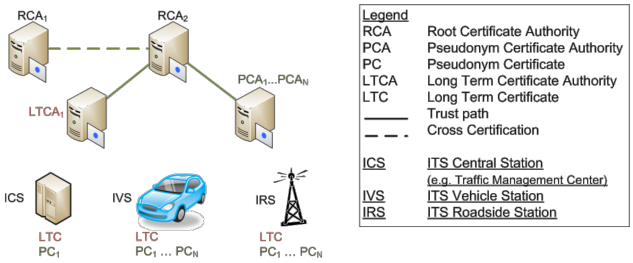

Figure 2: General PKI Structure [11]

stored inside the vehicle and the certificate is appended to every outgoing message. [11]

4.1. The PKI of the C-ITS

This section explains the PKI which was created by the *Car 2 Car Communication Consortium (C2C-CC)* [11] and got adopted by the European ETSI C-ITS standard for V2X communications.

4.1.1. Structure. We describe the structure of the PKI from top down, explaining functionality and components layer by layer. The structure described in the following is corresponding to the one given in Figure 2.

At the highest level of the PKI proposed by the C2C-CC is the RCA. Its main task is to control and manage the CAs on the layer below. Therefore the RCA issues certificates for the underlying CAs with a long validity. If there are multiple RCAs it is possible that they cross-sign their certificates to increase their trust level. Cross certification is only possible between RCAs and not between other CAs on the lower layer. Below the RCA, there are two kinds of Sub-CAs, *Long-Term Certification Authorities (LTCA)* (also Enrolment Authorities) and *Pseudonym Certification Authorities (PCA)*(also Authorization Authority). [11]

Entities need to have a long term identity to identify and authenticate them inside the PKI. Therefor every entity owns unique a *Long-Term Certificate (LTC)* (also Enrolment Credentials) which gets issued to the entity by a LTCA. To prevent tracking and traceability of entities, LTCs are not used for communication between two entities. Instead entities use pseudonyms identities which can not be mapped to the LTC. These pseudonymous identities are realized through *pseudonymous certificates (PC)*(also Authorization Tickets) which disguise the individual identifiers of the entity, such as MAC-Address and the network layer identifier. These PCs (usually distributed in a set) get issued to the entity by PCAs. In contrast to LTCs, PCs are short-lived, which means their validity is limited to a couple of minutes to a few hours. If a single PC is used to often it enables tracking again, since the identifiers of the PC can be tracked. Therefor an entity stores a large amount of valid PCs inside the vehicle. As a result PCs need to be exchanged and renewed often. [11]

The last layer of the PKI hirarchy are the actual entities. Each of them owns as described one LTC and multiple PCs. [11]

4.1.2. Issuing & renewing of Certificates. This section briefly explains how the issuing of certificates is handled in the PKI and how they are renewed.

doi: 10.2313/NET-2020-11-1_15

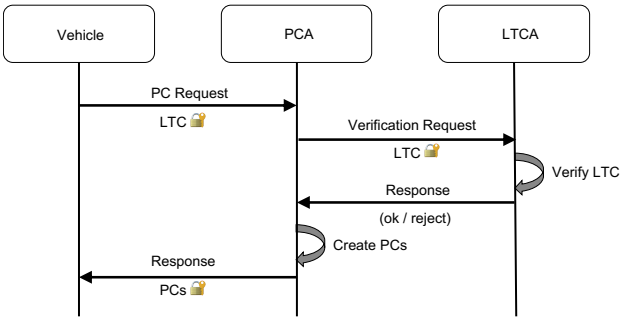

Figure 3: Issuing PCs Flowchart

The first LTC of an entity could be installed by the manufacturer. Since the LTC is valid for longer periods of time, it is not renewed very often. When a LTC needs to be renewed, the entity sends its LTC (encryped with the public key of the LTCA) to the LTCA and receives in a response the new LTC. [12]

The lifetime of PCs and thereby the number of renewing operations is based on three major factors: the number of PCs an entity uses silmultaneously, the lifetime of one PC (e.g. 10min or 1h) combined with the decision if they can be reused and how many usable PCs an entity has to store. In the C-ITS standard these parameters are not further specified yet and left up to the manufacturer. [12]

Since PCs need to be renewed often than LTCs, this process must be more flexible. The process of issuing PCs to an entity, which is described in the following, is also shown in Figure 3.

To get a new set of PCs, an entity sends a request to a PCA. This request includes the LTC (encrypted with the public key of the LTCA), the ID of the corresponding LTCA, public keys and the current position. The for this region responsible PCA, sends a request to the LTCA stated in the entity's request with the received LTC. By analyzing the LTC, the LTCA then permits the PCA to issue new PCs if the entity is a valid part of the network. The PCA generates a set of PCs which are encrypted, using the received public keys, and sends these new PCs back to the original entity. [11] [12]

4.1.3. Revocation. If an entity gets identified as malicious or defect, it is the responsibility of the PKI to ensure the reported entity gets excluded from the network. The detection of the malicious entities is not part of this paper.

To exclude entities, the PKI implements a Certification Revocation List. The CRL contains the LTCs of the reported entities and is collectively managed by the LTCAs. When an entity is reported, the LTCA, in collaboration with the PCA, identifies the LTC of this entity and adds it to the CRL. When the malicious entity requests new PCs, the LTCA compares the given LTC with the CRL and is able to reject the request if the entity is reported. If an entity does not have valid PCs, it is not trusted in the network communication and therefore excluded. [11] [12]

By using this approach, an entity can send valid and authenticated messages until it runs out of valid cached PCs. Without valid PCs the messages send by the entity are not authenticated and discarded at the receiving end. This can cause problems, depending on the specific design of the PCs and the renewing process, because there could be a significant amount of time between detecting a compromised entity (adding the LTC to the CRL) and excluding this entity from the network (entity runs out of PCs). In this period of time the entity could cause severe damage in the network. [11] [12]

TABLE 1: Certificate types in the PKI [14]

Name	Quantity	Size	Lifetime
RCA Certificates	20	126 Byte	up to 15 years
LTCA Certificates	up to 1000	126 Byte	up to 15 years
PCA Certificates	up to 2000	126 Byte	up to 5 years
LTC	1	125 Byte	up to 10 years
PC	1500/Year	124 Byte	up to 1 years

In a situation where a CA is compromised, for example, if the private key got exposed, all the certificates issued by this CA needs to be revoked. Otherwise an attacker could produce valid certificates for malicious entities, which can not be detected by the PKI. [13]

To revoke all certificates issued by a CA, CRLs are also put to use. The PKI administrator appends the certificate of the compromised CA to a CRL. This CRL only contains revoked CAs and gets actively distributed to all PKI participants. When a certificate, issued by the compromised CA, gets checked by an entity through the certificate chain, the entity compares the certificate of the CA with the distributed CRL and is able to verify if it is valid. This expensive process only needs to be executed rarely due to the fact that compromised CAs occurs seldom. [13]

4.2. Certificates

In this section, we explain general design ideas and possible options for certificates. The exact definition of the certificates is not part of this paper.

4.2.1. Format & Types. For the PKI in the V2X network, multiple types of certificates are needed. According to the specifications made by the ETSI C-ITS standard [14], there are five different types of certificates which are listed in the Table 1 along with some estimations of the amount stored in an entity, the size of one certificate and the lifetime, defined by the C2C-CC in [11]. All certificates follow the same structure based on the ExplicitCertificate defined in the IEEE standard 1609.2 clause 6.4.6 [15]. The technical differences of each certificate are defined in [16].

4.2.2. Cryptographic algorithms. The cryptographic algorithms used in the certificates and the V2X communications are also vitally important to ensure secure communications.

In the C-ITS standard Elliptic Curve Digital Signature Algorithms (ECDSA) are intended for signing data [16].

For sending encrypted data, the Elliptic Curve Integrated Encryption Scheme (ECIES) is specified by the the IEEE standard 1609.2 [15].

Both use one of the elliptic curves NIST P-256 (specified in FIPS 186-4) or brainpoolP256r1 (specified in RFC 5639) [15].

doi: 10.2313/NET-2020-11-1_15

4.3. Comparision with the WAVE standard

In the following, we point out major differences of the European C-ITS and the US WAVE standard. We especially focus on the key-generation and the revocation process. A more detailed comparison between the different standards can be found in [6].

In comparison to the European standard, The WAVE standard distributes tasks among several smaller independent authorities as in contrast to the three authorities (RCA, LTCA, PCA) in the European standard. As a result, power is widely distributed in the system and abuse is more difficult. This ensures no one has enough information to do harm or breach the privacy of entities. [17]

Furthermore, the WAVE standard uses a new cryptographic construct for the key generation, called *butterfly key expansion*. The basic principle behind it, is that the entity generates one key pair and sends the public key (also public seed) along with one expansion function to the certificate issuing authority. The authority can now apply the received function to the public key to generate multiple public keys which are used to create certificates. The entity also uses an expansion function on the private key to generate multiple private keys. These separately generated public and private keys fit together to an asymmetric key pair and can be used for signing and encryption. [18] Using this approach, the number of messages send between the entity and the issuing authority is drastically reduced as shown in [19].

As a result, a different revocation process has been established. This is explained in detail in [18]. In summary, multiple authorities cooperate to identify the LTC. Furthermore, it is possible to revoke the PCs of the revoked entity, based on the seed value used for the certificate generation. This poses a major difference to the C-ITS approach.

5. Conclusion and further work

V2X communications is a promising concept to improve our daily mobility on many levels and we are getting closer to a connected mobility every day. The European WLAN based ETSI C-ITS standard gives manufacturers and developers a fundamental structure of how communications should be established but leaves some aspects up to the manufacturer. We outlined that the concept of a PKI with LTCs and PCs seems suitable for establishing trust and validate messages in a V2X network. It should be emphasized that privacy has been an important design goal from the beginning. Concerning the revocation process, new concepts as in the WAVE standard show efficient techniques, which could be part of a future adaption. Since mobility is not limited to specific regions in the long run, the different standards should be compatible on a basic level without major adjustments at the entity.

References

[1] U. D. of Transportation, "How connected vehicles work," https://www.its.dot.gov/factsheets/pdf/connected_vehicles_work.pdf, [Online; accessed 11-June-2020].

[2] G. Pocovi, M. Lauridsen, B. Soret, K. I. Pedersen, and P. Mogensen, "Automation for on-road vehicles: Use cases and requirements for radio design," in *2015 IEEE 82nd Vehicular Technology Conference (VTC2015-Fall)*, 2015, pp. 1–5.

[3] M. Hasan, S. Mohan, T. Shimizu, and H. Lu, "Securing vehicle-to-everything (v2x) communication platforms," *IEEE Transactions on Intelligent Vehicles*, pp. 1–1, 2020.

[4] I. of Electrical and E. Engineers, "Ieee standard for information technology—telecommunications and information exchange between systems local and metropolitan area networks—specific requirements - part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications," *IEEE Std 802.11-2016 (Revision of IEEE Std 802.11-2012)*, pp. 1–3534, 2016.

[5] A. Festag, "Cooperative intelligent transport systems standards in europe," *IEEE Communications Magazine*, vol. 52, no. 12, pp. 166–172, 2014.

[6] T. Yoshizawa and B. Preneel, "Survey of security aspect of v2x standards and related issues," in *2019 IEEE Conference on Standards for Communications and Networking (CSCN)*, 2019, pp. 1–5.

[7] ARIB, "700 MHz Band Intelligent Transport Systems," Association of Radio Industries and Businesses, Standard ARIB STD-T109, 2013.

[8] A. Ghosal and M. Conti, "Security issues and challenges in v2x: A survey," *Computer Networks*, vol. 169, p. 107093, 2020.

[9] I. Aad, J. Hubaux, and E. W. Knightly, "Impact of denial of service attacks on ad hoc networks," *IEEE/ACM Transactions on Networking*, vol. 16, no. 4, pp. 791–802, 2008.

[10] J. Weise, "Public key infrastructure overview," *Sun BluePrints OnLine, August*, 2001.

[11] N. Bißmeyer, H. Stbing, E. Schoch, S. Gtz, and B. Lonc, "A generic public key infrastructure for securing car-to-x communication," in *18th World Congress on Intelligent Transport Systems featuring ITS America's annual meeting and exposition 2011*, 10 2011.

[12] J. P. Monteuuis, B. Hammi, E. Salles, H. Labiod, R. Blancher, E. Abalea, and B. Lonc, "Securing pki requests for c-its systems," in *2017 26th International Conference on Computer Communication and Networks (ICCCN)*, 2017, pp. 1–8.

[13] Working Group 2, Task Force 1, "Draft report on european security mechanism," C-Roads, Tech. Rep., 2019.

[14] ETSI, "Intelligent transport systems (its); security; its communications security architecture and security management," European Telecommunications Standards Institute, Standard TS 102 940, 2018.

[15] IEEE, "Ieee standard for wireless access in vehicular environments–security services for applications and management messages," *IEEE Std 1609.2-2016 (Revision of IEEE Std 1609.2-2013)*, pp. 1–240, 2016.

[16] ETSI, "Intelligent transport systems (its); security; security header and certificate formats," European Telecommunications Standards Institute, Standard TS 103 097, 2017.

[17] W. Whyte, A. Weimerskirch, V. Kumar, and T. Hehn, "A security credential management system for v2v communications," in *2013 IEEE Vehicular Networking Conference*, 2013, pp. 1–8.

[18] B. Brecht, D. Therriault, A. Weimerskirch, W. Whyte, V. Kumar, T. Hehn, and R. Goudy, "A security credential management system for v2x communications," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 12, pp. 3850–3871, 2018.

[19] B. Hammi, J. P. Monteuuis, H. Labiod, R. Khatoun, and A. Serhrouchni, "Using butterfly keys: A performance study of pseudonym certificates requests in c-its," in *2017 1st Cyber Security in Networking Conference (CSNet)*, 2017, pp. 1–6.