Anonymous Authentication and Pseudonym-Renewal for VANET in NDN

Muktadir Chowdhury
University of Memphis
mrchwdhr@memphis.edu

Ashlesh Gawande
University of Memphis
agawande@memphis.edu

Lan Wang
University of Memphis
lanwang@memphis.edu

ABSTRACT

Secure deployment of a vehicular network depends on the network's trust establishment and privacy-preserving capability. In this paper, we propose a scheme for anonymous pseudonym-renewal and pseudonymous authentication for vehicular ad-hoc networks over a data-centric Internet architecture called Named Data networking (NDN). We incorporated our design in a traffic information sharing demo application and deployed it on Raspberry Pi-based miniature cars for evaluation.

CCS CONCEPTS

• **Security and privacy → Pseudonymity, anonymity and untraceability**; **Mobile and wireless security**; • **Networks →** *Naming and addressing*;

KEYWORDS

NDN, VANET, authentication, privacy

ACM Reference format:
Muktadir Chowdhury, Ashlesh Gawande, and Lan Wang. 2017. Anonymous Authentication and Pseudonym-Renewal for VANET in NDN. In *Proceedings of ICN '17, Berlin, Germany, September 26–28, 2017,* 2 pages.
https://doi.org/10.1145/3125719.3132111

1 MOTIVATION

A Vehicular Ad-hoc Network (VANET) is a decentralized and self-organized network of vehicles that communicate among themselves. In such a network, vehicles may exchange information about real-time traffic and vehicular information, e.g. speed, acceleration, and emergency braking. However, a vehicular network is distributed and mobile in nature and suffers from intermittent connectivity, which make it difficult to deploy on the traditional point-to-point IP architecture.

1.1 Why NDN?

Keeping in mind the characteristics of VANET, we choose Named Data Networking (NDN) [6] as the underlying network. NDN is different from IP in that it does not require the consumers to set up a connection before requesting data. The consumers send out a request, containing name of the data, and whoever has the data will respond to that request. Security is built into the NDN architecture as each data packet is signed by a producer and carries the meta information about the signature such as the key locator [4]. A consumer can retrieve the data from anywhere and verify its provenance.

1.2 Privacy and Authentication

A vehicle is identified by a name in NDN and the data produced by the vehicle may indicate that name through its data name and key name. Consequently having a static name for a vehicle can divulge sensitive information about a vehicle. For example, an eavesdropper can capture the data packets and generate profiles of routes for vehicles. This information can be used for various criminal activities.

On the other hand, false information from a mischievous vehicle can disrupt the network and have hazardous effect. Therefore, the network should also establish trust among vehicles to prevent the dissemination of false information.

In our previous work [2], we proposed a trust model and a preliminary pseudonym renewal scheme. In this work, we flesh out the design to anonymously renew pseudonyms, which conforms to our trust model, and integrate it into our demo application.

2 RELATED WORK

Petit et al. [5] provided a survey encompassing various aspects of pseudonyms. They divided the pseudonym issuance schemes into two categories: third-party issuance and self issuance. Teja et al. [3] proposed an anonymous authentication framework for the interactions between an electric vehicle and a charging station. Their framework also provides anonymity revocation in case of misbehavior by a vehicle. Pseudonymous authentication can be approached in different ways [1], such as public-key cryptography, group-based signature, symmetric-key, and identity-based cryptography.

All the above designs are in the IP domain, while our work is in the context of NDN. Our pseudonym issuance scheme combines self insurance and third-party issuance, and our pseudonymous authentication uses public-key cryptography.

3 PSEUDONYM CHANGING SCHEME

Our NDN based VANET is composed of three entities: vehicle, manufacturer, and a root organization. We have adopted the security trust model and naming of the entities from our previous work [2]. To prevent tracking of vehicle, we use pseudonyms instead of the real name of the vehicle. A vehicle's overall pseudonym consists of two components: the vehicle's pseudonym and the manufacturer's pseudonym. We also proposed a preliminary version of anonymous

ICN '17, September 26–28, 2017, Berlin, Germany
© 2017 Association for Computing Machinery.
ACM ISBN 978-1-4503-5122-5/17/09…$15.00
https://doi.org/10.1145/3125719.3132111

pseudonym renewal method [2] that uses a Certificate Issuing Proxy (CIP). We describe a refined version of the protocol 1 in this paper.

(1) All the proxies listen for Interests at /autondn/CIP/request-key prefix. The vehicle broadcasts an Interest i_1 with the name /autondn/CIP/request-key to retrieve the key of a proxy.
(2) The nearby proxies will respond with data d_1 named /autondn/CIP/request-key/<CIP-name> that contains their key.
(3) When the first proxy's Data d_1 containing its key arrives, the vehicle sends the Certificate Requesting Interest i_2 to that proxy. The vehicle verifies the data using the trust model for CIP data (CIP's public key is signed by root organization). The vehicle then generates a random pseudonym based on its VID (Vehicle Identification) and appends it to a manufacturer's pseudonym to create the vehicle's pseudonym. It also generates a new key K_3 for the pseudonym. Afterwards, the vehicle encrypts its VID, one of the vehicle's current public keys K_2, and the new public key K_3 using the manufacturer's public key K_0. Moreover, it encrypts the manufacturer's name using the CIP's key K_1. Next, it sends i_2 to the CIP with the Interest name /<CIP-name>/E_{K_1}(<manufacturer-name>)/E_{K_0}(<VID>, K_2, K_3).
(4) When the CIP receives i_2, it decrypts the component that follows <CIP-name> and determines the manufacturer's name. CIP cannot decrypt the components after manufacturer's name as they are encrypted using K_0, which ensures that CIP cannot obtain the VID and other sensitive information. Next, CIP constructs and sends a new Interest i_3, signed with K_1, with the Interest name /<manufacturer name>/key-issuance/E_{K_0}(<VID>, K_2, K_3).
(5) After receiving i_3, the manufacturer checks that the Interest is signed by one of the authorized proxies and then extracts the VID, K_2, and K_3. The manufacturer verifies the VID and creates a certificate for the new key K_3. The data d_3 contains the new certificate, one of the manufacturer's new pseudonyms and the corresponding certificate. It is encrypted using K_2 preventing CIP or any eavesdropper from obtaining the information.
(6) When the CIP receives the data packet d_3, it constructs d_2 by changing its name to match i_2, re-signs the data, and forwards it to the vehicle which will be able to decrypt the data and store the certificate and other information. The manufacturer's future pseudonym and certificate will be used by the vehicle the next time it generates a pseudonym.

4 DEMO SCENARIO AND SETUP

We implemented the trust model, and pseudonym renewal protocol and integrated them in a prototype road information sharing application (AutoNDN). Vehicles request for the status of the next road in their route, and at the same time broadcast the status of the road they are currently on. We will demonstrate the system on Raspberry Pi based miniature cars running on a track. Our demo scenario in Figure 2 includes (1) vehicles sending road information, (2) other vehicles receiving and validating the information according to the trust schema, (3) changing pseudonyms, (4) publishing data under new pseudonyms, and (5) refilling pseudonyms.

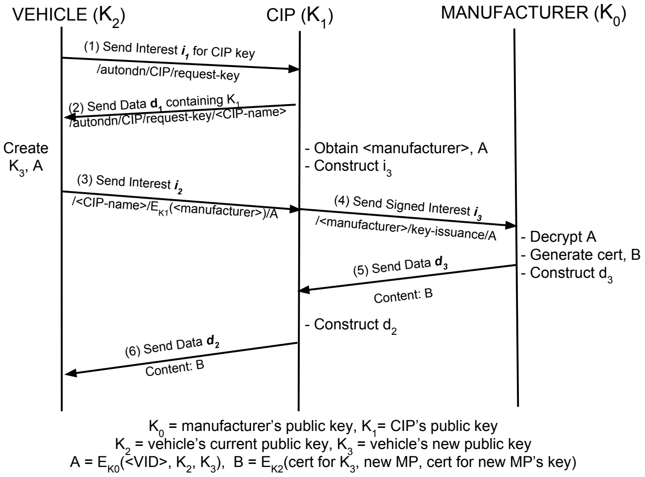
VEHICLE (K_2)
CIP (K_1)
MANUFACTURER (K_0)
(1) Send Interest i_1 for CIP key
/autondn/CIP/request-key
(2) Send Data d_1 containing K_1
/autondn/CIP/request-key/<CIP-name>
Create K_3, A
- Obtain <manufacturer>, A
- Construct i_3
(3) Send Interest i_2
/<CIP-name>/E_{K1}(<manufacturer>)/A
(4) Send Signed Interest i_3
/<manufacturer>/key-issuance/A
- Decrypt A
- Generate cert, B
- Construct d_3
(5) Send Data d_3
Content: B
- Construct d_2
(6) Send Data d_2
Content: B
K_0 = manufacturer's public key, K_1= CIP's public key
K_2 = vehicle's current public key, K_3 = vehicle's new public key
A = E_{K0}(<VID>, K_2, K_3), B = E_{K2}(cert for K_3, new MP, cert for new MP's key)

Figure 1: Obtaining Certificates from Manufacturer and Proxies

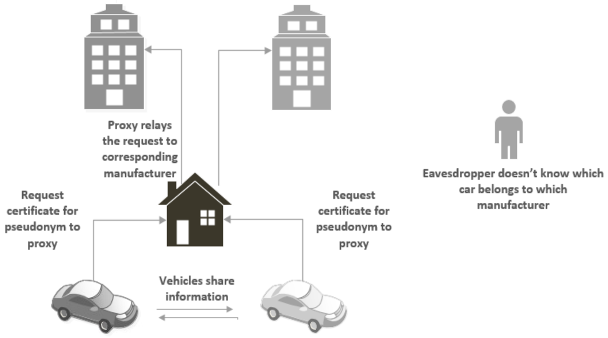
Proxy relays the request to corresponding manufacturer
Request certificate for pseudonym to proxy
Request certificate for pseudonym to proxy
Eavesdropper doesn't know which car belongs to which manufacturer
Vehicles share information

Figure 2: Demonstration Scenario: Interaction between proxy, vehicle, and manufacturer

ACKNOWLEDGMENT

The authors gratefully acknowledge the financial support of the FedEx Institute of Technology in conducting this research.

REFERENCES

[1] Subir Biswas, Md. Mahbubul Haque, and Jelena V Misic. 2010. Privacy and Anonymity in VANETs: A Contemporary Study. *Ad Hoc & Sensor Wireless Networks* 10, 2-3 (2010), 177–192.
[2] Muktadir Chowdhury, Ashlesh Gawande, and Lan Wang. 2017. Secure Information Sharing among Autonomous Vehicles in NDN. *2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI)* 00 (2017), 15–26. DOI: http://dx.doi.org/doi.ieeecomputersociety.org/
[3] Vishnu Teja Kilari, Satyajayant Misra, and Guoliang Xue. 2016. Revocable anonymity based authentication for vehicle to grid (V2G) communications. In *Smart Grid Communications (SmartGridComm), 2016 IEEE International Conference on.* IEEE, 351–356.
[4] NDN Project Team. 2014. NDN Packet Format Specification 0.1.1 documentation. Online: http://named-data.net/doc/NDN-TLV/current/. (2014).
[5] Jonathan Petit, Florian Schaub, Michael Feiri, and Frank Kargl. 2015. Pseudonym schemes in vehicular networks: A survey. *IEEE communications surveys & tutorials* 17, 1 (2015), 228–255.
[6] L. Zhang, A. Afanasyev, J. Burke, V. Jacobson, k. claffy, P. Crowley, C. Papadopoulos, L. Wang, and B. Zhang. 2014. Named Data Networking. *ACM SIGCOMM Computer Communication Review (CCR)* 44, 3 (Jul 2014), 66–73.