SECURE VANET VIA NAMED DATA NETWORKING

HKU COMP4801 (FYP) Interim Report

Designing a new security protocol for privacy preserving identity verification in V-NDN
(Vehicular ad-hoc network via Named Data Network)
24 JAN 2015

Cheuk Yiu So
Edw1n@hku.hk  |  UID: 2012530095
Summary

Vehicular Ad-hoc NETwork (VANET) is a type of infrastructure-less network mainly for inter vehicle communication through wireless medium. Named Data Networking (NDN) is a data-oriented networking model. It provides a good networking model for communication between vehicles since most of the VANET applications relies on sharing information between vehicles.

On named-data.net, there is a specification for Named Data Networking (Named Data Networking: Motivation & Details - Named Data Networking (NDN)). The protocol overview specifies that Named Data Networking protocol aims to replace IP on the networking layer. There is also a “VANET via Named Data Networking” (Giulio Grassi, 2014) publication on named-data.net. It contains a NDN protocol for effective communication between vehicles through vehicle to vehicle (V2V) communication by utilizing the nature of wireless communication protocol, which is broadcasting to reduce the amount of packet need to be resend by nodes.

Currently, a protocol has been designed for sharing information with other vehicles which located within a specific area in a specific time range. In the next stage, the protocol will be tested in a NS-3 simulator. Result from the simulator will be used for optimizing the design of the protocol.

In addition, there is also a protocol being designed for privacy preserving identity verification by utilizing the packet structure of NDN. The protocol utilized the pseudo identity scheme to achieve privacy preserving and trusted party to sign the certificate. The protocol will be running in a simulator to conduct performance analysis and look for room for improvement.

It can be expected a report and a publication will be written for describing the protocol in the end of the project.
## Contents

Summary ......................................................................................................................... 1  
Contents .......................................................................................................................... 2 
Introduction .................................................................................................................... 3 
Background ..................................................................................................................... 4 
Purpose ............................................................................................................................ 5 
Previous work in the field ............................................................................................... 5 
Current Design of Geographical based encryption (Data Fusion) ................................... 6 
  Design Example ............................................................................................................. 6 
  Comment ......................................................................................................................... 7 
Current Design of Privacy preserving identity verification ........................................... 7 
  Privacy preserving .......................................................................................................... 8 
  Identity verification ......................................................................................................... 8 
  Delivering PKC ................................................................................................................ 9 
  Marinating the neighbor table ....................................................................................... 9 
Current status .................................................................................................................. 9 
Results ............................................................................................................................. 10 
References ...................................................................................................................... 10 
Table of Figures .............................................................................................................. 10
Introduction

Vehicular Ad-hoc NETwork (VANET) is a type of wireless network mainly for inter-vehicle communication. Named Data Networking (NDN) has been selected to be the next generation Internet architecture and NDN is suitable for VANET applications as most of them rely on sharing and distributing information with other vehicles.

The project will study how NDN can be used in VANET and a new protocol with privacy-preserving identity verification for VANET with NDN will be designed. In the end, a new protocol, a publication and a report will be delivered.

The development of implementing NDN with VANET in the world is still at an early stage. With the new protocol, vehicle can share information with each other without worrying the driver’s privacy being exposed to 3rd party. Meanwhile, the message sender (the driver or the on broad unit) identity will still be properly authenticated. This can help developing better VANET application as the protocol has provided a way to share information safely run on application and developer need not to design additional mechanism to protect sender’s privacy and verifying sender’s identity.
In Figure 1, NDN will replace IP packets by Content chunks. Routing will not be determined by IP address; instead, it will be decided by the content tag. And the strategy layer will decide how the content chunks will be delivered to the next hop.

Named Data Networking (NDN) is a kind of data-oriented networking model. It provides a good networking model for communication between vehicles since most of the VANET applications rely on sharing information between vehicles.

There are several application domains on VANET, from spreading information with single hops to spreading information to multi hops within various distances. Examples are electronic brake lights, platooning and traffic information systems.

VANET applications are usually required to share information with other vehicles through distribution. An example is road safety application, which is a kind of traffic information system that shares traffic information with other vehicles nearby. The traditional IP networking model focuses on unicast (one to one) communication. Therefore, IP will introduce a significant overhead on VANET application as the source node has to maintain the connection between the client nodes.
With NDN, the sender node is no longer required to maintain the connection between the client nodes as each node can be turned into a relay node to help distribute data. The sender node just needs to make sure the data has been sent out to the nearby node and will respond to requests when additional data is needed.

### Purpose

Vehicular Ad-hoc NETwork (VANET) and Named Data Network (NDN) are regarded as two next generation networks. VANET aims at enhancing road safety while NDN aims at replacing the traditional IP network. Researchers start combining them to utilize their advantages.

The purpose of the project is to develop a protocol for VANET through an NDN network model with privacy preserving identity verification. For example, the message sender must be properly authenticated while the privacy of the driver must be properly preserved. Attackers should not be able to trace a driver’s travelling route by analyzing multiple packets sent by the vehicles.

### Previous work in the field

On named-data.net, there is a specification for Named Data Networking. (Named Data Networking: Motivation & Details - Named Data Networking (NDN)) The protocol overview specified that Named Data Networking protocol is aim as replacing IP on the networking layer. It has also mentioned how data packets are being signed to provide source identification. However, this might not be suitable for privacy-preserving identity verification as each packet has to be signed by using a private key. The identity of the sender will be revealed if the signer’s certification contains the personal information of the sender.
There is also a “VANET via Named Data Networking” (Giulio Grassi, 2014) publication on named-data.net. It contains a NDN protocol for effective communication between vehicles through vehicle to vehicle (V2V) communication. The design of this protocol aims as making data packets spread quickly and effectively. However, it also includes the GPS location of the sender. As a result, the sender’s location and the driving route can be traced easily if the sender keep on sending information out.

Current Design of Geographical based encryption (Data Fusion)

Currently, a protocol has been designed for sharing information with other vehicles located within a specific area in a specific time range. For example, the sender can decide sharing information with vehicles which are located within about 50 meters radius from the sender at 2015-10-11 12:32:37.

To achieve this, an encryption algorithm is required to encrypt the data. Since NDN is a network model which is similar to multicast, a new key distributing method has been developed to make good use of this property. Every vehicle will contain a GPS unit to record their GPS location. Each row in the record table will contain the GPS location and the timestamp. The format of the location value is WGS 84.

The property of WGS84 is that the more decimal places are given in the value, the more accurate the location will be. In other words, considering using this property as a key for encryption to restrict decoder in a specific area. On the other hand, the fewer decimal places are used as the key, the larger the area will be.

Design Example

The sender will send out the packet with the following data:

1. The timestamp of the information generated, for example, “2015-10-11 12:32”
2. The accuracy of the location value for the key (how many decimal places), for example, “1”.
3. The encrypted information.
4. The id of the vehicle.
5. The hashed value of the key.

The example above will create a specified area with size 11km north-south and 8.5km east-west. Only vehicles located in the same specified area of the sender at the moment 2015-10-11 12:32 will know the exact key for decryption. Receivers can retrieve the key from their record tables by using the timestamp provided in the packet and truncating the location by the accuracy specified in the packet and use it as a decryption key.

The hashed value of the key provides a mechanism for receivers to check whether they have the correct key to decrypt the message. This enables the receiver to put the computing resource on the decrypting packet which is targeted at him so that less resource will be wasted on trying to decrypt messages which are not for the receiver. Since a hashed value cannot be reversed to the original value, attackers cannot retrieve the key simply by analyzing the hashed value.

Comment

Although this design enables privacy preserving identity verification by knowing who is sending the packet (The Id of the vehicle), where exactly the driver is located is not known. This design has several restrictions.

First, the size of the specified area is restricted by the design of WGS 84. As a result, the scale of the size of the area is divided by 10. For example, with 1 decimal place, the accuracy in latitude is 11km; with 2 decimal place, the accuracy in latitude is 1.1km. Senders cannot decide the accuracy in latitude to be 5km.

Second, this protocol cannot be used in areas with no GPS signals, for example, inside a tunnel or an area with large, thick clouds which may filter out the GPS signal.

Additional works have to be done to further improve the protocol and test it within the NS3 simulator.
Current Design of Privacy preserving identity verification

A new protocol has been designed to utilize the properties of Named-data networking to reduce the overhead for authenticating the sender identity with asymmetric encryption system.

There will be a trusted third party responsible for issuing public key certificates (PKC). The public key of the trusted party will be pre-configured in every vehicle.

Privacy preserving

To achieve identity preserving, each vehicle will create a new identity after a certain period. To create its new identity, the sender will do the following actions:

1. First, generate a new pair of public key and private key.
2. Using the trusted party’s public key to encrypt new public key and the traceable id of the vehicle recognized by the trusted party
3. Next, send the encrypted content in the previous step to the trust party to request a new public key certificate.

The process of requesting a new certificate can be done using the road side unit which connected to the trust party or through other medium like cellular data network.

The trusted party will keep a table which tracing what certificate has been issued to vehicle. When there is a need to trace a sender’s identity, a request can be made to the trust party by providing the public key digest of the sender.

Identity verification

To achieve identity verification, the protocol will utilize the “KeyLocator” field which specified in the NDN specification. This means when the sender sends out a message, the certificate and the public key will not be included in the message. Instead, the certificate and the public key will be located in another data packet and will be fetched by the receiver when needed.

When a node receives a packet, it will verify the sender’s identity. It will first lookup the value in the KeyLocator field in the SignatureInfo field of the data packet. Then it will
Delivering PKC

To deliver its own PKC, there are three scenarios:

A. It is the first time the sender using its new identity
   When the sender sends out the first data packet after renewing its own identity, it will first send
   out its own public key certificate, then the data packet next.

B. A certain amount of new neighbors appeared
   When some new vehicles appeared near the sender, it will send out the PKC first and send out
   the message after. In VANET application, vehicle will keep on sending out data packet. A neighbor
   table can be maintained based on listening on packet sent by other vehicles.

C. An interest packet arrived
   When an interest packet related to the sender’s PKC arrived, the sender will send out its own PKC.
   Intermediate node will also send out PKC when there is a matched entry in its CS.

Marinating the neighbor table

The neighbor table can be maintained in the following way:

1. Through listening on “/vanet/*”
2. Each neighbor has a time to live (TTL) value
3. If not new packet from neighbor after certain period, remove it from the table

Current status

At the moment, a prototype of the new protocol has been developed. The design has been reviewed
by the supervisor to make sure that it meets all the design criteria safely. Next, the protocol will be
tested in a NS-3 simulator. Result from the simulator will be used for optimizing the design of the
protocol. In the end, a report and a publication will be written for describing the protocol.
Results

The current design of the protocol has the properties to fulfill part of the purpose of the project. Simulation will be done on next stage. It can be expected the protocol will able to deliver information safely and effectively inside the simulator.

References


Table of Figures

Figure 1 - Internet and NDN Hourglass Architectures, from (Named Data Networking: Motivation & Details - Named Data Networking (NDN))........................................................................................................................................................................... 4