

# A Paralleling Broadcast Authentication Protocol for sparse RSUs in Internet of Vehicles

Mengyuan Li, Na Ruan\*, Haojin Zhu, Jie Li, Xiang Li  
 Shanghai Jiao Tong University, China  
 \* Email: naruan@cs.sjtu.edu.cn

**Abstract**—Since the era of Internet of Vehicles (IoVs) is coming in next few years, real-time data transmission between vehicles and road-side sensor nodes has many application scenarios. However, due to different characteristics of IoVs and WSNs (Wireless Sensor Networks), real-time traffic data transmission is too complicated and slow when emergencies occurred in many RSUs-sparse (Road Side Units) areas. We build a simple integrated network model and propose a broadcast authentication protocol, namely Paralleling Broadcast Authentication Protocol (PBAP), aiming at enhance energy efficiency and providing network security in the direct communication between vehicles and WSNs. The simulation results demonstrate that the protocol can effectively extend lifetime of WSNs by improving the utilization rate of the keys and show nice properties in different channel loss ratio and different degrees of DoS attacks.

**Index Terms**—Broadcast Authentication Protocol; Internet of Vehicles; Wireless Sensor Network

## I. INTRODUCTION

### A. Background

By equipping the vehicles with Vehicle-to-Vehicle (V2V) communication, Vehicle-to-Infrastructure (V2I) communication as well as sensing capabilities, the conventional Vehicle Ad hoc Networks (VANETs) is evolving into the era of Internet of Vehicles (IoVs) [1]. In the IoVs paradigm, each vehicle is considered as a smart object equipped with a powerful multi-sensor platform, communication technologies, computation units, IP-based connectivity to the Internet and to other vehicles either directly or indirectly. IoVs are expected to provide numerous safety (e.g. crash avoidance) and non-safety applications (e.g. traffic monitoring and data collecting, accessing to the Internet, and other infotainment applications).

The academia and the industry are actively pushing the development of IoVs and making it a reality. For example, the recently defined standard IEEE 802.11p for inter-vehicular communication, designed according to the specific requirements of V2V interaction, constitutes an essential step towards this next phase. General Motors Co. has recently announced that GM will offer a car capable of piloting itself and “V2V” crash avoidance systems on a freeway by 2016. From 2012 to 2016, sponsored by the US Department of Transportation, 3,000 private cars, trucks, and buses will be allowed to communication with each other and with devices in the roadway infrastructure of northeast Ann Arbor based on 5.9 GHz Dedicated Short Range Communication (DSRC).

One of the major challenges for the real-world deployment of IoVs is the security issues. The recent successes in attacking vehicular systems [10] have demonstrated the need to design IoVs with a strong security guarantee. In IoVs, a vehicle needs to periodically broadcast its current locations, speed, and other status, to the neighboring vehicles as well as On Board Units (OBUs) will periodically broadcast data collected from other resources such as Internet and WSNs like temperature, humidity, road condition, object location and movement, sound

intensity and so on in the environment [2], [5], [6]. Such life-critical information should be ensured its authenticity and non-repudiation to achieve the fundamental security requirements.

### B. Motivation

In some natural disaster or man-made accident cases, some real-time traffic data can inform other vehicles to avoid more accidents in time [9], which requires the connections between IoVs and WSNs (Wireless Sensor Networks). Although the integrated networks of WSNs and IoVs have broad application prospects, we believe that the current data transmission routes between WSNs and IoVs needs to be optimized. In fact, the common data connections used now are based on Internet: data collected from sensor nodes is transmitted to Road Side Unit (RSU) through Internet, and then RSU broadcasts data to OBUs [10]. These indirect connections require on RSUs having strong capability and also cause a longer information delay.

However, in some cases of emergencies or RSUs-sparse areas as illustrated in Figure 1 and Figure 2, building a direct connection between OBUs and cluster-head nodes in WSNs is necessary, where cluster-head node refers to the central nodes in WSNs, which has limited resource but are densely deployed along the roadside [2], [5].

Figure 1 shows a real-time accident warning broadcasted by the cluster-head node. Since the direct connection between the cluster-head node and OBUs has shorter information delay, the cluster-head node can directly broadcast warnings to other passing vehicles as soon as nodes detect an emergency. Figure 2 shows how a landslide warning broadcasted in RSUs-sparse area, like mountain areas or rural areas. RSUs with strong capability are difficult to be deployed in high density for its investment cost and the lack of power supply. However, WSNs can be widely distributed there for its low cost and small size. Meanwhile, WSN nodes can be artificially redeployed and are flexible to be charged by exchanging batteries, which also make it suitable for this direct connection in .

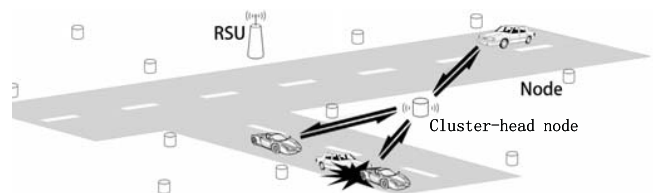


Fig. 1: out-view accident warnings

For the direct communication channel we are going to show, broadcast authentication is indispensable to provided security assurance. Although the IEEE 1609.2 standard [19] has proposed to achieve broadcast authentication by using the Elliptic

Curve Digital Signature Algorithm (ECDSA), verifying every signature using ECDSA causes high computational overhead on the standard OBU hardware, which has limited resources due to manufacturers cost constraints. A typical OBU with a 400MHz processor requires 20 milliseconds to verify one ECDSA signature while every vehicle is expected to broadcast a safety message every few hundred milliseconds and, thus verify a large number of message signatures in the case of the high density scenarios (e.g., rush hour). This makes broadcast authentication with a low generating and verification cost highly desirable towards the practical deployment of IoVs.

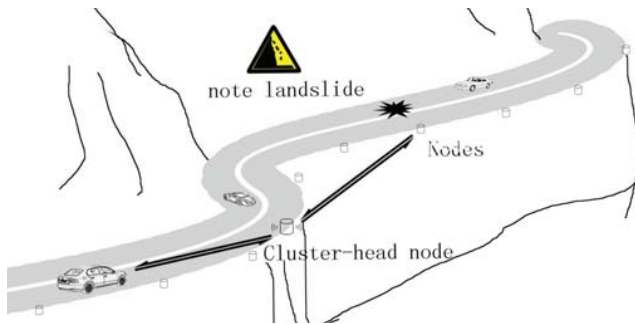


Fig. 2: landslide warnings

Thus, setting up a direct communication channel has many application scenarios, and a suitable broadcast authentication protocol is very necessary.

### C. Challenging issues

For such scenarios we described above, data transmission in the integrated network (i.e. between WSNs and IoVs) is necessary. However, a unified broadcast authentication protocol to guarantee security in the new network has not been designed yet. Indeed, the following two protocols which used in original networks does not accommodate to the new network environment.

VAST, a combination of digital signatures and TESLA++ [16], provides many important properties which are essential in IoVs, including real-time authentication, non-repudiation and prevention of DoS attacks. However, sensor nodes in WSNs are too resource-constrained in energy supply, computational capacities, memory, and broadcast frequency and range, which make VAST not applicable in the integrated network [7].

On the other hand,  $\mu$ TESLA [8] and multi-level  $\mu$ TESLA [11] are suitable for WSNs, since they have been modified in several aspects such as poor computing power to adapt to the limited resource of sensor nodes. But in the integrated network, randomly and frequently appeared communications actually require that the lifetime of high-level key chains is short enough, while is a very long time period in key management mechanism in multi-level  $\mu$ TESLA.

In addition, considering the real scenarios we described above, the high speed of passing vehicles leads to high delivery rate and demanding for short delay of package transmission. Together with the unpredictable traffic conditions and possible emergencies, these real-life cases give vast constraints on the protocol to be applied.

### D. Our work

To set a direct connection between vehicles in IoVs and cluster-head nodes in WSNs, we build a system model to meet

communication needs when emergencies happened. More importantly, our main contribution is proposing a new broadcast authentication protocol, namely Paralleling Broadcast Authentication Protocol (PBAP), to guarantee the communication security and enhance energy efficiency in this integrated network.

The advantages of our protocol are summarized as follows:

- Provide secure communication between IoVs and WSNs.
- Suitable for the resource-constrained WSNs.
- Greatly lengthen the lifetime of key chains and utility of data authentication.

In addition, we verified our protocol through reasonable network simulation and quantitative analysis.

The remainder of this paper is organized as follows. In section II, we introduce related work of the integrated networks, including network architecture and several broadcast authentication protocols based on WSNs. In section III, we list some scenario requirements and build our system model. In section IV, we present a paralleling broadcast authentication protocol which fits the integrated networks; we analyze its performance and simulation results in section V. In section VI, we draw a conclusion and discuss some future work.

## II. PRELIMINARIES

### A. Existing system model

Since people are no longer satisfied with signal information resources, many research efforts have been put in building integrated system model between IoVs and WSNs. Consequently, many strategies have been proposed in view of some special environment, for some typical examples including traffic planning, ride quality monitoring, location-aware micro-blogging and safety warning [18]–[21].

Vehicular sensor networks (VSNs) are the generic terms for those integrated networks between IoVs and WSNs. In vehicular environments, there are various wireless access methods, such as DSRC, Cellular networks, WiMAX and WLAN. The communication route in vehicular environments can be divided into two aspects: Vehicle-to-Vehicle (V2V) communications and Vehicle-to-Infrastructure (V2I) communications. V2V is more focused on information sharing between vehicles, while V2I shows the advantage of information acquisition.

However, VSNs exposes its limitations where Road Side Units are sparse. The data WSNs collected is hard to be passed to passing vehicles timely. In some emergencies, information delay in VSNs makes it unrealistic for passing vehicles to make a meaningful reaction. We believe it would be instrumental in some special scenarios to establish a direct link between cluster-head nodes in WSNs and passing vehicles. Ensuring broadcast authentication protocol powered by cluster-head nodes is an important way to achieve this goal. This paper is one of the first to explore a broadcast authentication protocol in the direct broadcast contact between vehicles and cluster-head nodes in WSNs.

### B. Multi-level $\mu$ TESLA

In this part, we introduce several related broadcast authentication protocols. TESLA++ is a flexible, extensible and efficient broadcast authentication protocol in IoVs, and it has DoS-resistant ability. But the required digital signature is poorly implemented in WSNs due to their limited computation and storage ability [16].  $\mu$ TESLA is suitable for WSNs, since it is a light-weight protocol which has fewer requirements on resources. However, its unicast-based initial parameter

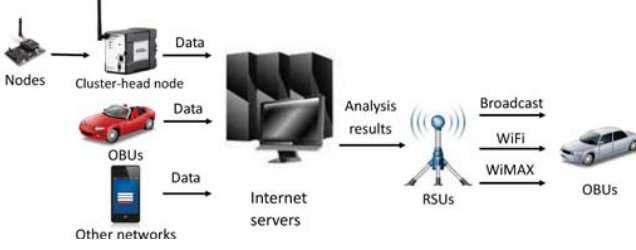


Fig. 3: Existing System Model

distribution limits its scalability and entire life cycle requires long key chain. Multi-level  $\mu$ TESLA, which is modified from  $\mu$ TESLA, is born on this basis. It shows several nice properties like low overhead, scalability to large networks, tolerance of message loss, scalability to large networks, and resistance to DoS attacks [11]. To predetermine and broadcast the initial parameters, multi-level  $\mu$ TESLA uses a multi-level key chains. The main idea of multi-level key chains is the use of Commitment Distribution Message ( $CDM_i$ ), which is composed as follows:

$$CDM_i = i|K_{i+2,0}|MAC_{K'_i}(i|K_{i+2,0})|K_{i-1}.$$

The detailed description of multi-level  $\mu$ TESLA is shown in Figure 4. Nevertheless, its advantages cannot solve all the problems and different constraints in VSNs.

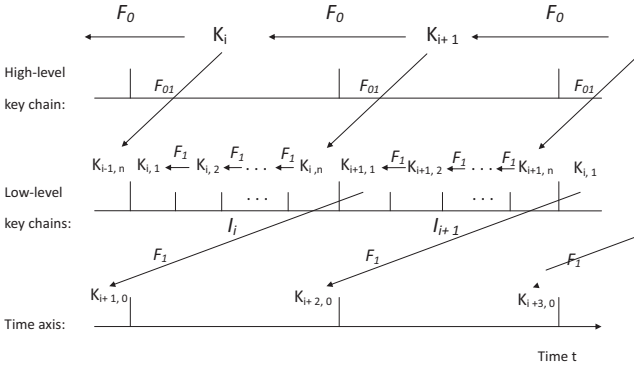


Fig. 4: usage of key chains in two levels TESLA

### III. SCENARIO REQUIREMENTS AND SYSTEM MODEL

Before presenting our protocol, we begin with building a hybrid system model for this integrated network. To achieve this, we summarize the characteristics of WSNs and IoVs to figure out the obstructions we meet and advantages we use in the designing process.

#### A. Obstructions

One obstruction is that the broadcast protocol in these integrated networks should fit the needs of high delivery rate and short delay. Since vehicles travel at speeds up to 120 kilometers per hour, the high speed makes it difficult to sustain broadcast between cluster-head nodes and vehicles. Thus a high delivery rate and short delay protocol is required.

Another obstruction is that the sensor nodes only have limited storage space and computing power, which make these

integrated networks impossible to maintain a high frequency broadcast all the time. The time interval between two disclosures of keys in WSNs is too long to satisfy high delivery rate in integrated networks. Meantime, these limits also make some existing broadcast protocols give up safety measures in authentication of broadcasting messages.

#### B. Advantages

Vehicles have high power reserves from onboard batteries as well as strong computing power and adequate storage space. Existing broadcast protocols in WSNs need to face the sensor nodes' limited power and resources. However, in these integrated networks, the broadcast receivers will be sensor nodes or vehicles. When the receivers are passing vehicles, some limits can no longer be considered.

Another advantage is the information access can be facilitated by V2V. The high speed of passing vehicles, packets loss ratio, delayed release of keys and limited broadcast distance make it impossible to guarantee vehicles can authenticate all broadcast messages. V2V can make up the problem in some ways.

Compounding matters above, a suitable broadcast authentication protocol between Distributed Sensor Networks and IoVs has a few basic requirements as follows.

(1) Ensure high delivery rate and short delay, but the key's frequent interaction cannot produce too much influence on the subsequent original system like key chain exhaustion.

(2) Ensure that vehicles can acquire an high authenticated packets ratio in a short period of time.

(3) Enhance the ability to resist DoS attacks or other attacks.

To summarize, Table 1 gives all information we mentioned before and make a comparison between WSNs and IoVs.

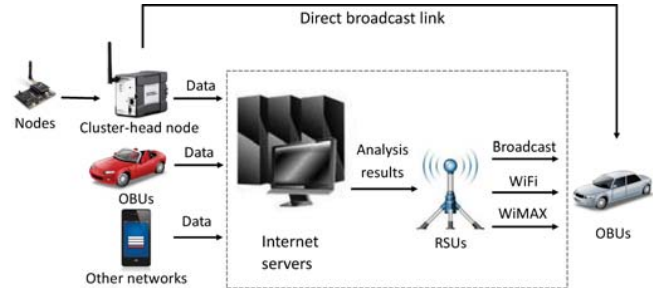


Fig. 5: Optimized system overview

#### C. System model

WSNs can gain lots of important data of IoVs, but they don't have direct connection with OBUs. Sensor nodes can be deployed among roads to detect conditions like humidity, temperature, other vehicles' location and wind speed, and they can also identify threats about roads like road icing, landslides and car accident [6] [12]. However, after gathering data from nodes, cluster-head nodes usually convey data to Internet, and then internet will convey this data to other networks [13].

Given the relatively high cost of RSUs, we believe that the direct communication between cluster-head nodes and OBUs will be necessary when the following scenarios happen.

- Vehicle in RSUs-sparse areas: one location where with-in the effective communication distance of cluster-head nodes but out of RSUs, or one location where RSU has been damaged.

- Some dangerous situations occurred and this urgent information needs to be conveyed to vehicles in time.
- When the integrated network considers it is more valuable of the whole systems to use this direct connection.

System model name	simple broadcast-based integrated system	
networks	WSNs	IoVs
member	Cluster-head nodes, sensor nodes, internet	OBUs, RSUs, internet
obstructions	Sensor nodes' limited storage space and computing power	Vehicles' high-speed
advantages	Low cost, many applications, be widely distributed	high power reserves, strong computing power and adequate storage space. V2V as another information access
main communication patterns	Sensor nodes update data to cluster-head node. Cluster-head node broadcasts instruction to nodes.	RSUs-to-OBUs communication. Vehicles-to-RSUs communication. Vehicle-to-vehicle communication.
	Cluster-head node broadcasts information to OBU directly. Cluster-head node conveys information to RSU through Internet.	

TABLE I: Basic quantities of the integrated system model

Consequently, we establish a simple integrated network system model named simple broadcast-based integrated system, which contains a directly connection between cluster-head node and OBUs and is depicted by Figure 5, Figure 6 and Table 1. In this simple model, the existing communication process can be greatly simplified, and the saved time is very meaningful when above scenarios happen.

Figure 5 gives an overview of the communication between cluster-head nodes and vehicles, and we can see multi-level connections in the dashed box are replaced by the direct broadcast link. More specifically, Figure 6 gives the detailed description of this direct broadcast link, *i.e.* the data path between sensor nodes, cluster-head nodes and OBUs on vehicles.

#### D. Analysis of the integrated network model

For the integrated system model we established, one concern is that the limited energy supply of sensor nodes may not support the real-time communication between vehicles and sensor nodes. However, this is not a big issue in our network model. Indeed, unlike roadside units (RSUs) in IoVs, sensor nodes, including the cluster-node nodes, are unactivated in most time, until receiving requests for communication from vehicles.

Particularly, for cluster-head nodes, they only to need to communicate with some vehicles, and thus save energy by taking advantage of inner communication in IoVs. Taking a similar research as an example, this gives NS2-based network simulation, and shows the energy consumption of cluster-head nodes are about three times of that of regular nodes [23]. Compared with RSUs, these cluster-head sensor nodes still consumes less energy and are much cheaper for deploying large-scale networks.

This system model leads to another concern, lacking of security assurance. In next section, we will present a new broadcast authentication protocol which suits this integrated network.

## IV. PROTOCOL DESIGN

### A. Notation

Here, we give some notations of variables:

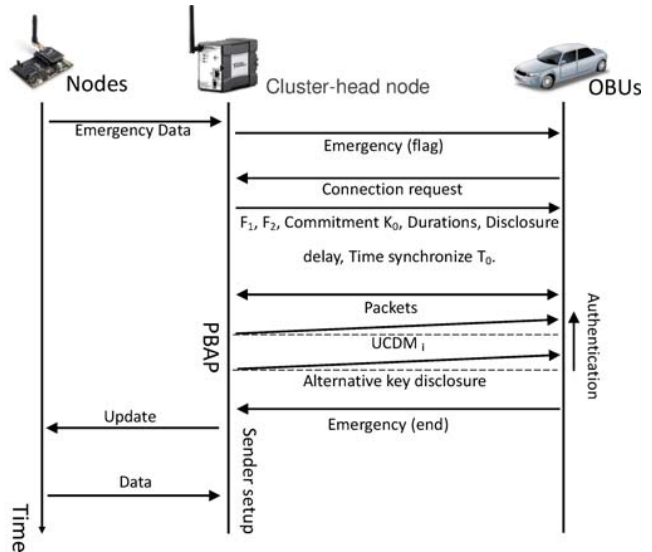


Fig. 6: Broadcasting process

- $I_{i,m}$  : the  $m^{th}$  part in the  $i^{th}$  time interval.
- $F$  : one-way hash function to produce key chain.
- $P_{i,m}$  : authenticated packet can be received in the interval  $I_{i,m}$ .
- $K_{i,m}$  : the  $m^{th}$  key used in time interval  $I_i$  to authenticate  $P_{i,m}$ .
- $K_{i,j}$  : a key stored in interval  $I_i$  to verify  $K_{i,m}, (m > j)$ .
- $d$  : disclosure delay  $d$  in secondary key chains.
- $MAC_i^C(M)$  : message generated with a secret key  $K_i$ .

### B. Protocol overview

In WSNs which use multi-level  $\mu$ TESLA, the cluster-head nodes only need to broadcast data to nodes. However, in the integrated networks, when cluster-head nodes broadcast data, they need to determine the potential receivers of the data are nodes or OBUs. After determining the potential receivers of the data, the cluster-head node will choose different key chains to handle the information. So we improve multi-level  $\mu$ TESLA to fit the needs of the integrated network.

In our PBAP, the three-level key chains consist of a high-level key chain, multiple low-level key chains and alternative multiple key chains. We divide broadcast into two types. The first type happens when the potential receivers are nodes. In this situation, the base stations will use multiple low-level key chains to encrypt data and use high-level key chain to form CDM just like multi-level  $\mu$ TESLA. The high-level key chain is generated by using  $F_0$  while low-level key chains are generated by using  $F_1$ .

The second type happens when the potential receivers are OBUs. The cluster-head nodes will choose a  $K_{n_2}$  as a new last key randomly, and use  $K_i = F_1(K_{i+1})$  where  $i = 0, 1, 2, \dots, n_2-1$  to generate a series of keys. These key chains are named pseudo-high-level key chains, and are used to form  $UCDM_i$  (Urgent Commitment Distribution Message). The alternative multiple key chains will play a low-key function. The secondary key chains in the type will be generated by using  $K_i = F_2(K_{i+1})$  where  $i = 0, 1, 2, \dots, n_2-1$ . Both  $F_1$  and  $F_2$  are one-way function, which can produce one-way key chains.

Algorithm 1 describes the data transmission path in this integrated system with PBAP. In this pseudocode, line 1 to line 15 depicts the communication between sensor nodes and cluster-head nodes in normal and urgent cases; line 16 to line 30 depicts the communication between cluster-head nodes and vehicles.

---

**Algorithm 1** An algorithm about how the system in integrated network works.

---

**Require:** nodes' storage space  $\mathbb{S}_1$ , cluster-head node's storage space  $\mathbb{S}_2$ , vehicle's storage space  $\mathbb{S}_3$ , upper storage space  $\mathbb{S}_4$

**Ensure:** data transmission path.

```

1: for each  $n \in \mathbb{N}$  do
2:   node  $n$  collect data periodically.
3:    $\mathbb{S}_1 \leftarrow data$ .
4:   if the data shows no abnormalities then
5:     nodes transmit the data to the cluster-head node periodically.
6:      $\mathbb{S}_2 \leftarrow \mathbb{S}_1$  periodically.
7:   end if
8:   if the data shows emergency then
9:     nodes transmit the data to the cluster-head node immediately.
10:     $\mathbb{S}_2 \leftarrow \mathbb{S}_1$  immediately.
11:    return  $\mathbb{S}_1$ .
12:  else
13:    node  $n$  may be damaged
14:  end if
15: end for
16: for cluster-head node do
17:  broadcast instructions to nodes occasionally.
18:  data can be received at any time.
19:  if the received data  $\mathbb{S}_2$  shows an emergency then
20:    broadcast  $\mathbb{S}_2$  to passing vehicles immediately.
21:     $\mathbb{S}_3 \leftarrow \mathbb{S}_2$  immediately.
22:  end if
23:  if received passing vehicle's request then
24:    broadcast  $\mathbb{S}_2$  to passing vehicles immediately.
25:     $\mathbb{S}_3 \leftarrow \mathbb{S}_2$  immediately.
26:  else
27:    upload data through Internet.
28:     $\mathbb{S}_4 \leftarrow \mathbb{S}_2$  occasionally.
29:  end if
30: end for

```

---

### C. Detailed description of broadcasting process

1) *Initialization and sender setup:* Some basic preparation work needed to be done for broadcasting to sensor nodes is just as multi-level  $\mu$ TESLA does. These include (1) generate a series of high-level keys by choosing an initial key  $K_{n_0}$  randomly using a one-way function  $F_0$ ; (2) choose a one-way function  $F_1$ , which can produce one-way key chains of length  $n_1$ , and these key chains are used to form low-level keys; (3) divide the whole lifetime of nodes into  $n_0$  parts, and divide each high-level key interval into  $n_1$  parts; (4) time synchronization in the system and confirm other parameter such as low-level key disclosure delay  $d$  and initialization time  $T_0$ .

Cluster-head node needs to complete the following steps for broadcasting to vehicles. (1) guarantee a one-way function  $F_2$ , which can produce alternative multiple key chains of length

$n_3$ ; (2) divide each *UCDM* interval into  $n_3$  parts; (3) other parameter such as the alternative key disclosure delay  $d_2$ .

The initial parameters sensor nodes needed can be distributed to nodes by predetermining and broadcasting. However, every time a short-term direct communication between cluster-head node and vehicles happens, the number of passing vehicles is limited. The initial parameters vehicles need can be distributed to vehicles by unicasting or broadcasting.

#### 2) Bootstrapping a new receiver:

For a new node receiver:

The protocol of the new Broadcast Authentication Protocol follows directly from the multi-level  $\mu$ TESLA. When nodes are initialized, the nodes' clocks are synchronized with the cluster-head node. The nodes will receive one-way hash function  $F_0, F_1$  for high-level key chain and low-level key chains, the commitment  $K_0$  of the high-level key chain, time interval for high-level key chain and low-level key chains, initialization time  $T_0$  and the low-level key disclosure delay  $d$ .

For a new vehicle receiver:

In addition to different key chains and time intervals, two processes are basically the same. When vehicles are initialized, the vehicles' clocks are synchronized with the cluster-head node. The vehicles will receive one-way hash function  $F_1, F_2$  for pseudo-high-level key chains and alternative multiple key chains, the commitment  $K_0$  of the pseudo-high-level key chain, time interval for pseudo-high-level key chain and alternative multiple key chains, initialization time  $T_0$ , and the alternative multiple key disclosure delay  $d_2$ .

3) *Broadcasting authenticated packet:* Time is divided into a series of parts. Normal packet  $P_{i,m}$  will be distributed in interval  $I_{i,m}$ . Each packet corresponds to a secondary key. The secondary key  $K_{i,m}$  will be distributed in interval  $I_{i,m+d}$ .  $CDM_i$  or  $UCDM_i$  will be distributed in  $I_i$ . Since  $CDM_i$  and  $UCDM_i$  are more important when compared to normal packet, cluster-head node usually choose to broadcast  $CDM_i$  or  $UCDM_i$  by  $n$  times in interval  $I_i$ .

4) *Authenticating broadcast packets:* Delayed release is the key to this part. Each membership's clocks in the integrated network are synchronized with the cluster-head node once they are initialized. Time is divided into almost fixed time intervals. Each time intervals related to two keys of different one-way key chain. Take a node receiver as an example, the node receives  $CDM_{i-2}$  in interval  $I_{i-2}$  and  $CDM_{i-1}$  in interval  $I_{i-1}$ .

$$CDM_{i-2} = i - 2 |K_{i,0}| MAC_{K'_{i-2}}(i - 2 |K_{i,0}| K_{i-3}).$$

The node will authenticate  $K_{i,0}$  after verifying that  $F_0(K_{i-3}) = F_0(K_{i-2})$ . Then,  $K_{i,0}$  will be stored as a identify method to  $K_{i,m}$ . So when node receive  $P_{i,m}$  in interval  $I_{i,m}$ . The corresponding key  $K_{i,m}$  will be distributed in interval  $I_{i,m+d}$ . The node will authenticate the key by verifying that  $F_1^{m-j}(K_{i,m}) = K_{i,j}$ , where  $K_{i,j}$  is low-level key which had already been authenticated by  $K_{i,0}$ .

When the receivers are vehicles, the process has some differences. The cluster-head node generates a series of pseudo-high-level keys by choosing a  $K_{n_2}$  as a new last key randomly and using  $K_i = F_1(K_{i+1})$  where  $i = 0, 1, 2, \dots, n_2-1$ . These keys are used to form  $UCDM_i$  (Urgent Commitment Distribution Message).

$$UCDM_i = i |K_{i+2,0}| MAC_{K'_i}(i + 2 |K_{i+2,0}| K_{i-1}).$$

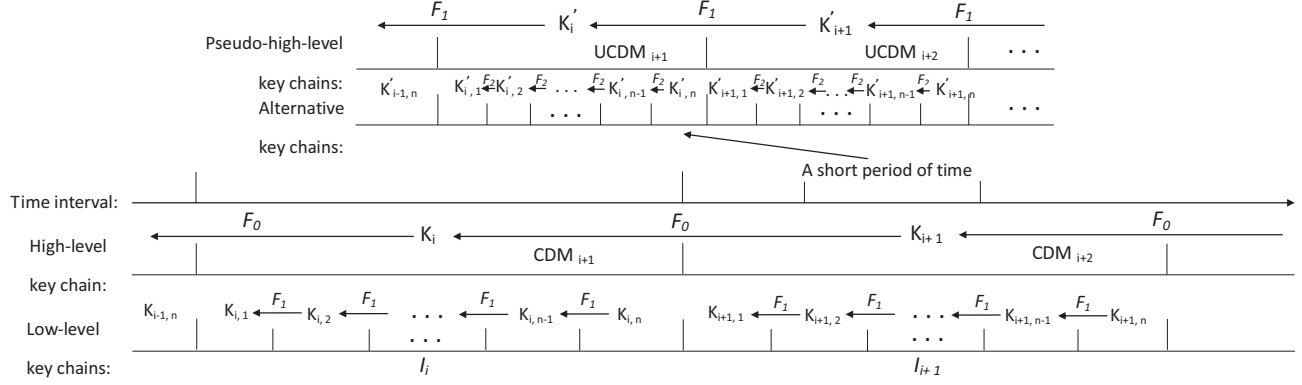


Fig. 7: Generation and usage of keys in PBAP

The alternative multiple key chains will play a low-key function in this type. The secondary key chains in the type will be generated by using  $K_i = F_2(K_{i+1})$  where  $i = 0, 1, 2, \dots, n_2-1$ . How to broadcast and authenticate normal messages are just in the same way as in the multi-level  $\mu$ TESLA. After a short-term connection with passing vehicles, the cluster-head node can prepare for the next connection by calculating the next pseudo-high-level keys in advance. Since we consider OBU as a unit which has enough computing power and storage space, we think there are other ways which can also broadcast authenticated packet, and we will discuss these in section VI.

## V. ANALYSIS AND EXPERIMENT

### A. Improvement analysis

In our system, cluster-head nodes shoulder two missions. One is maintaining a steady long-term connection with sensor nodes. Another mission is getting ready to build random short-term connections with passing vehicles. Our goal is to design an appropriate broadcast protocol which is suitable for a steady long-term connection with sensor nodes as well as short-term direct communication between cluster-head nodes and vehicles. The different characteristics of two networks decide that the existing broadcast protocols are no longer suitable for the integrated network.

For the first mission, how to ensure the random short-term connections with passing vehicles would not produce too much influence on the steady long-term connection is our main focus. In a single WSN, multi-level  $\mu$ TESLA can embody good characteristics like long-term and low-power. For sensor node networks, the high-level key chain's length is fixed based on the entire sensor network lifetime. However, the occasional exchanges of information with passing vehicles would bring some uncertainties to this length-fixed key chain. The random short-term connections require high delivery rate and short delay, which would result in overusing  $CDM_i$  as well as lack of high-level key chain.

The simplest way is to reserve a section of high-level key chain in case of possible exhaustion. However, the unpredictable times of interaction with vehicles and 60 times delivery rate compared to usual cases would lead to improper key chain length. Thus if only simply being lengthened, the key chain may possibly be exhausted when more frequent exchange of information interaction among the integrated network happen.

Instead, our protocol guarantees no exhaustion by using alternative multiple key chains in random short-term connections for the integrated network. Every time when short-term connections happens, the cluster-head node will choose a  $K_{n_2}$  as a new last key randomly, and use  $K_i = F_1(K_{i+1})$  where  $i = 0, 1, 2, \dots, n_2-1$  to generate a series of keys. These keys, as pseudo-high-level keys, are used to form  $UCDM_i$  in the second type. The alternative multiple key chains will play a low-key function in this type. The secondary key chains in the type will be generated by using  $K_i = F_2(K_{i+1})$  where  $i = 0, 1, 2, \dots, n_3-1$ . Besides, we think it would be better to help members in system to distinguish whether the messages belong to, thus using different key chain will be better. For example,  $UCDM_i$  which contains information needed by vehicle with the new key chain can be received by the vehicle, without affecting the original sensor network.

For the second mission, high delivery rate and short delay are our goals in building a short-term direct link. However, because of the low requirement of information interaction frequency in WSNs, for the high-level key chain, the interval between two broadcast of  $CDM_i$  (about 60 seconds) is longer than the time spent when a vehicle go through (about 6-12 seconds).

While for the low-level key chains, if sensor nodes repeat broadcasting  $CDM_i$  10 times, the interval between two  $CDM_i$  distributions is around 6 seconds, which will lead to lack of enough  $CDM_i$  to support decrypting data. If this mechanism doesn't change to suit the integrated networks, some vehicle may even not be able to receive the first  $CDM_i$  signal, thus cannot successfully decrypt the data packet, the situation of the vehicle and interactive broadcasting node corresponds ineffective interaction. In this situation, if a vehicle establishes contact with a cluster-head node during the time interval  $I_i$ , even if we assume that when a cluster-head node releases the next  $CDM_i$  signal directly (in sensor networks,  $CDM_i$  signals are randomly released) after establishing radio contact with the vehicle, the vehicle will receive the commitment  $K_{i+2,0}$  of low-level key chain after it first received  $CDM_i$ . However, by time interval  $I_{i+2}$ , the vehicle had already been out of the broadcast distance of cluster-head node. Our protocol solves these problems by using passing vehicles' sufficient priority and alternative two-level TESLA.

### B. Security analysis

Multi-level  $\mu$ TESLA has many schemes to reply different security problem. The security of our protocol is completely inherited from multi-level  $\mu$ TESLA. Our protocol applies to all schemes in multi-level  $\mu$ TESLA. Take DoS-resistant scheme in multi-level  $\mu$ TESLA as an example, the scheme is designed to reply to DoS attacks. On the basis of the original scheme,  $H(CDM_{i+1})$  is added into  $CDM_i$ , which  $H$  is a pseudorandom function which is used to authenticate the next  $CDM$ . Thus, receivers can authenticate  $CDM_{i+1}$  immediately if they had received  $H(CDM_{i+1})$  in  $CDM_i$  already. Therefore, the scheme can defeat memory-based DoS attacks. Moreover, the system can choose to use these schemes in the steady long-term connection with sensor nodes or short-term connections with passing vehicles by specific conditions in the system.

### C. Simulation

In our system, we assume that Distributed Sensor Network and Internet of Vehicles form an integrated network. The distributed sensor network's cluster-head node directly conveys some data to vehicle going through. Distributed Sensor Network is right on the side of road, and the cluster-head nodes' valid broadcast distance is 200 meter. Simultaneously, we assume vehicles going through with a speed of 60-120 kilometers per hour (16.67-33.33 meters per second) which also means the vehicle may leave the effective broadcast distance after only 6-12 seconds' communication with cluster-head nodes.

According to the reference data from schemes in multi-level  $\mu$ TESLA, the duration of each high-level time interval is 60 s and the duration of each low-level key is 100 ms. In the simulation, we compare the different terms of performance about multi-level  $\mu$ TESLA and PBAP. Since the initial set of deliver rate in multi-level  $\mu$ TESLA is for a steady long-term connection with sensor nodes, this long interval can't meet the needs of our integrated network. Thus, we assume multi-level  $\mu$ TESLA increases its delivery rate when build a short-term connection with passing vehicles.

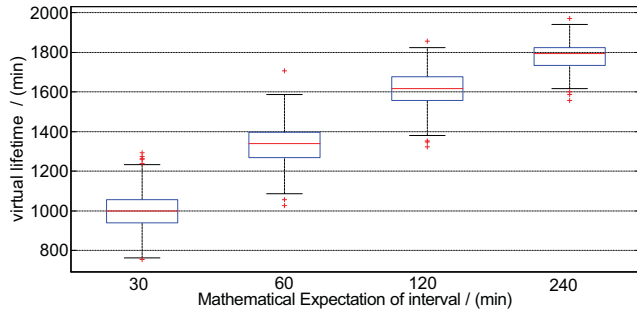


Fig. 8: Dispersion degree of virtual lifetime

Figure 8 and Figure 9 show the limitations of existing protocol and the outstanding stability of PBAP. Figure 8 is Boxplot, which shows the dispersion degree of simulation results about the performance of multi-level  $\mu$ TESLA in the system. Horizontal ordinate indicates the mathematical expectation of interval between two emergencies. Vertical ordinate indicates virtual lifetime of multi-level  $\mu$ TESLA scheme with a 2000-keys high level key chain. In the simulation, the occurrence of the emergency is normal distribution and we repeat our simulation 500 times respectively according different expectation

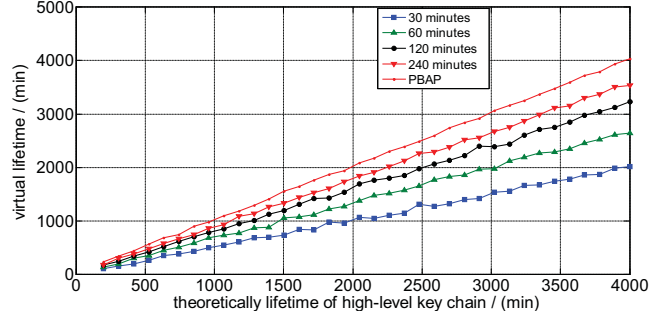


Fig. 9: Compare of virtual lifetime

in order to simulate the actual performance. Figure 8 shows that the existing protocol's extremely limited performance in the face of random emergency.

Figure 9 compares the lifetime cycle of multi-level  $\mu$ TESLA and PBAP in a fixed length of high-level key chain. Horizontal ordinate indicates the theoretically life cycle of high-level key chain, while vertical ordinate indicates the virtual lifetime of high-level key chain in our simulation. According to the figure, PBAP shows its great ability of lengthening the lifetime of key chains and random occurrence of the emergency hardly affects PBAP.

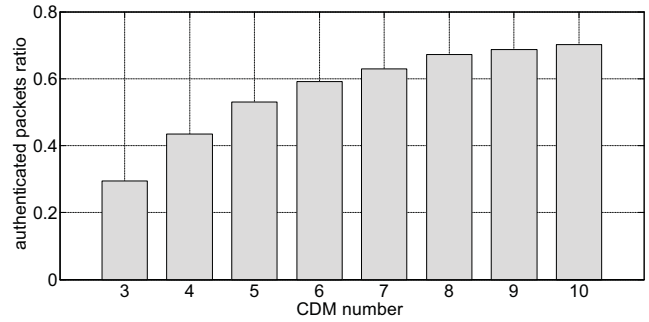


Fig. 10: Impact of frequency of broadcasting CDM

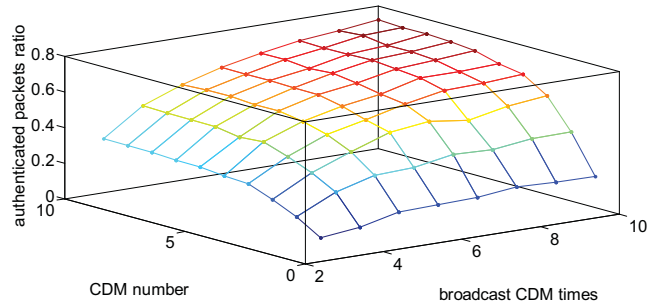


Fig. 11: Impact of CDM on ratio of authenticated packets

Figure 10 and Figure 11 illustrate the performance of PBAP under DoS attacks when PBAP has a short-term connection with passing vehicles. We simulate transmission rate in different  $CDM$  buffers and the repetitions of broadcasting  $CDM_i$  under a fixed percentage of forged  $CDM_i$  packets, which is 90%. The simulation results validate the applicability of

PBAP in the system model and the effective security ability inherited from multi-level  $\mu$ TESLA. In Figure 10, we find that the authenticated packets ratio increases with the quantity of repeating broadcast times of  $CDM$ . Figure 11 shows PBAP's comprehensive performance under different broadcast times and frequencies of  $CDM$ , which can help us to choose the appropriate allocation for a specific environment conditions.

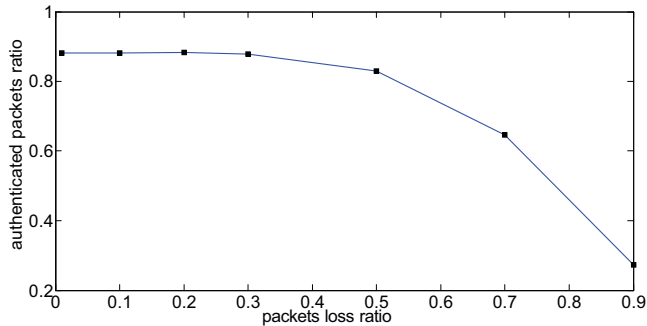


Fig. 12: Impact of packets loss rate on PBAP

Figure 12 inherits the previous simulations and shows the influence of packets lost ratio under a fixed percentage of forged  $CDM_i$  packets, which is 90%. We assume that the time of repeating  $CDM$  broadcast is 10. In the previous simulation, according to reference data in multi-level TESLA, we assume the packets lost ratio is 50%. However, in practice, packets lost ratio will change in different situation. Figure 12 shows that PBAP maintains a good DoS-tolerant ability. If the packet loss rate is less than 50%, PBAP can maintain a high authenticated packets ratio.

## VI. CONCLUSION AND FUTURE WORK

In this paper, we build an integrated system model to set up a direction communication method between WSNs and IoVs, which can be applied to many scenarios. Afterwards, we design and evaluate PBAP, a new broadcast authentication protocol which is suitable for this system model and provides reliable message authentication, which is confirmed by our simulation. Since the communication between vehicles and sensor nodes is realizable and secure when using our protocol, this integrated network would play an important role in the coming era of IoVs.

For future work to enhance the function of PBAP, several additional constraints in real life may be considered. First, given the high speed of vehicles and varying distance between vehicles and cluster-head nodes, time intervals in the alternative low-level key chain may vary as well to improve the efficiency of authentication process. Second, considering the possible hostile attacks such as DoS attacks, our protocol could be improved by setting the selection mechanism of received packages to minimize the threat of DoS attacks. Third, we can explore performance of other schemes inherited by multi-level  $\mu$ TESLA in PBAP.

## ACKNOWLEDGEMENT

This work was supported in part by CCF-Tencent Open Fund, in part by Shanghai Jiao Tong University 211 Fund.

## REFERENCES

- [1] Leng, Ying, and Lingshu Zhao, *Novel design of intelligent internet-of-vehicles management system based on cloud-computing and Internet-of-Things*, in Proceedings of the 1st International Conference on Electronic and Mechanical Engineering and Information Technology (EMEIT), Harbin, Heilongjiang, China, pp. 3190-3193, Aug. 2011.
- [2] L. Mainetti, L. Patrono, and A. Vilei, *Evolution of wireless sensor networks towards the internet of things: A survey*, in Proceedings of the 19th International Conference on Software, Telecommunications and Computer Networks (SoftCOM), Split-Hvar-Dubrovnik, Croatia, pp. 1-6, Sept. 2011.
- [3] L. Atzori, A. Luigi, Antonio Iera, and G. Morabito, *The internet of things: A survey*, Computer networks, vol. 54, no. 15, pp. 2787-2805, Oct. 2010.
- [4] J. Manyika, M. Chui, B. Brown, J. Bughin, R. Dobbs, C. Roxburgh, and A. H. Byers, *Big data: The next frontier for innovation, competition, and productivity*, May 2011.
- [5] N. Ahmad, N. Riaz, and M. Hussain, *Ad hoc wireless sensor network architecture for disaster survivor detection*, International Journal of Advanced Science and Technology, vol. 34, pp. 9-16, Sept. 2011.
- [6] K. C. Rahman, *A survey on sensor network*, Journal of Computer and Information Technology, vol. 1, no. 1, pp. 76-87, 2010.
- [7] K. Lu, Y. Qian, M. Guizani, and H. H. Chen, *A framework for a distributed key management scheme in heterogeneous wireless sensor networks*, IEEE Transactions on Wireless Communications, vol. 7, no. 2, pp. 639-647, Feb. 2008.
- [8] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Cullar, *SPINS: Security protocols for sensor networks*, Wireless Networks, vol. 8, no. 5, pp.521-534, Sept. 2002.
- [9] A. Boukerche, H. A. B. F. Oliveria, E. F. Nakamura, and A. A. F. Loureiro, *Vehicular ad hoc networks: A new challenge for localization-based systems*, Computer Communications, vol. 31, no. 12, pp. 2838-2849, July 2008.
- [10] S. Biswas, and J. Mistic, *Proxy signature-based RSU message broadcasting in VANETs*, in Proceedings of the 25th Biennial Symposium on Communications (QBSC), Kingston, ON, Canada, pp. 5-9, May 2010.
- [11] D. Liu, and P. Ning, *Multilevel  $\mu$ TESLA: Broadcast authentication for distributed sensor networks*, ACM Transactions on Embedded Computing Systems (TECS), vol. 3, no. 4, pp. 800-836, Nov. 2004.
- [12] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, *Wireless sensor networks: a survey*, Computer Networks, vol. 38, no. 4, pp. 393-422, March 2002.
- [13] D. Estrin, R. Govindan, J. Heidemann, and S. Kumar, *Next century challenges: Scalable coordination in sensor networks*, in Proceedings of the 5th annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom), New York, NY, USA, pp. 263-270, August 1999.
- [14] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, *Efficient authentication and signing of multicast streams over lossy channels*, IEEE Symposium on Security and Privacy, Berkeley, CA, USA, pp. 56-73, May 2000.
- [15] K. Akkaya, and M. Younis, *A survey on routing protocols for wireless sensor networks*, Ad hoc Networks, vol. 3, no. 3, pp. 325-349, May 2005.
- [16] A. Studer, F. Bai, B. Bellur, and A. Perrig, *Flexible, extensible, and efficient VANET authentication*, Journal of Communications and Networks, vol. 11, no. 6, pp. 574-588, Dec. 2009.
- [17] U. Lee, and M. Gerla, *A survey of urban vehicular sensing platforms*, Computer Networks, vol. 54, no. 4, pp. 527-544, March 2010.
- [18] S. Gaonkar, J. Li, R. R. Choudhury, L. Cox, and A. Schmidt, *Microblog: sharing and querying content through mobile phones and social participation*, in Proceedings of the 6th International Conference on Mobile Systems, Applications, and Services (MobiSys), Breckenridge, Colorado, pp. 174-186, June 2008.
- [19] D. Jiang, V. Tailiwal, A. Meier, W. Holfelder, and R. Herrtwich, *Design of 5.9 GHz DSRC-based vehicular safety communication*, Wireless Communications, vol. 13, no. 5, pp. 36-43, Oct. 2006.
- [20] U. Lee, B. Zhou, M. Gerla, E. Magistretti, P. Bellavista, and A. Corradi, *Mobeyes: smart mobs for urban monitoring with a vehicular sensor network*, Wireless Communications, vol.13, no. 5, pp. 52-57, Oct. 2006.
- [21] J. Eriksson, L. Girod, B. Hull, R. Newton, S. Madden, and H. Balakrishnan, *The pothole patrol: using a mobile sensor network for road surface monitoring*, in Proceedings of the 6th International Conference on Mobile Systems, Applications, and Services (MobiSys), Breckenridge, Colorado, pp. 29-39, June 2008.
- [22] S. Yousefi, M. S. Mousavi, and M. Fathy, *Vehicular ad hoc networks (VANETs): challenges and perspectives*, in Proceedings of the 6th International Conference on ITS Telecommunications (ITST), Chengdu, China, pp. 761-766, June 2006.
- [23] H. Qin, Z. Li, Y. Wang, X. Lu, W. Zhang and G. Wang, *An integrated network of roadside sensors and vehicles for driving safety: Concept, design and experiments*, in Proceedings of the 8th International Conference on Pervasive Computing and Communications (PerCom), Mannheim, Germany, pp. 79-87, March 2010.