Dynamic Reporting Mechanisms for Trust Management in Vehicular Ad-hoc Networks

Bo-Rang Lin[#1], Tsan-Pin Wang[*2]

[#] *Computer Science and Information Engineering, National Taichung University of Education*
No.140, Minsheng Rd., West Dist., Taichung Taiwan
[1]BCS103119@gm.ntcu.edu.tw

[*] *National Taichung University of Education*
No.140, Minsheng Rd., West Dist., Taichung Taiwan
[2] tpwang@mail.ntcu.edu.tw

***Abstract*— Advances in Internet of Things (IoT) technology, a lot of applications have been widely deployed in Vehicular ad-hoc networks (VANET). How to support safe and reliable transmission environment will be an important issue for supporting VANET applications. The solution demands a dynamic reporting mechanism against selfish and malicious vehicles. Real time reporting would cause wireless network congestion. Therefore, this paper proposes P-Persistent Reporting (PPR) mechanism to dynamically adjust reporting probability. The proposed mechanisms adopt an encryption method for massages, Certificate Authority to verify vehicles to increase reliability of forwarding. Finally, we compare PPR with Real time Reporting (RTR) and Periodic Reporting (PR) in terms of reporting cost and delay. Numerical results show that PPR mechanisms outperform RTR and PR, because PPR can dynamically adjust appropriate reporting probability for the underline environment.**

***Keywords*—Vehicular Ad-hoc Network (VANET), Dynamic Reporting Scheme, Trust Management**

1. INTRODUCTION

Advances in science and technology, security issues have been more and more important. The vehicular ad-hoc network (VANET) is a wireless mobile communication network that consists of vehicle to vehicle and/or vehicle to infrastructure composes temporary network topology. Vehicles can forward messages, and can be categorized four types: general vehicle and certified vehicle and selfish vehicle, malicious vehicle. The security issues are very important considering whether the messages can be safely transferred to the destination and the messages are tapped in forwarding messages.

First, the vehicle uses identity as a public key. Then vehicles can use the public key to encrypt messages. Hence, the encrypt message will be safety in messages of the transmission. As shown in Figure 1, node A wants to transport a secret message to node B. Thus, node A uses node B's identity as the public key to encrypt message. On receiving node A's encrypted message, node B uses itself private key to decrypt the message. Then node B can receive the original plaintext message [1].

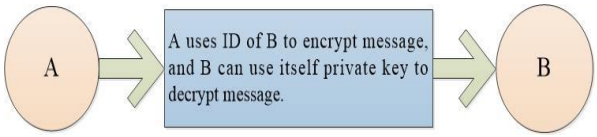

Fig. 1 Message Encryption

In transmitting encrypted messages, we can use Certificate Authority (CA) [2] to verify the reliability of vehicles. Other vehicles can rely on the certificated vehicles to relay messages, because the certificated vehicles are reliable and safe.

Each vehicle maintains a neighbor list that includes vehicle's identity, each vehicle's trust value [3] and distrust table. There is a demand on a dynamic reporting mechanism that may dynamically request for trust report by RSU.

In the dynamic reporting system architecture, we use MapReduce with Hadoop in Big Data [4], because data are huge amount, and the calculation has to complete in time.

Figure 2 illustrates dynamic reporting system architecture as follows.

1. Receiver vehicle returns an ACK for Sender vehicle, and return an ACK for RSU. When RSU receives an ACK from Receiver vehicle, RSU uses P-Persistent Reporting to request reporting,

and transport trust value with Neighbor list to RSU.

2. RSU transports trust value from itself to the cloud, and uses MapReduce with Hadoop in Big Data. Then statistics obtained the minimum trust value (e.g. Figure 3).

3. Finally, th cloud will return the minimum trust value for RSUs. After receiving the minimum trust value from the cloud, RSU transports it to neighbor vehicles, and shares between neighbor RSUs

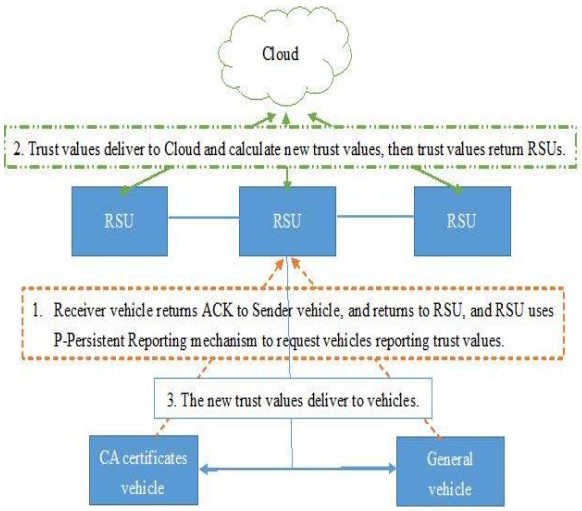

Fig. 2 Dynamic report system architecture

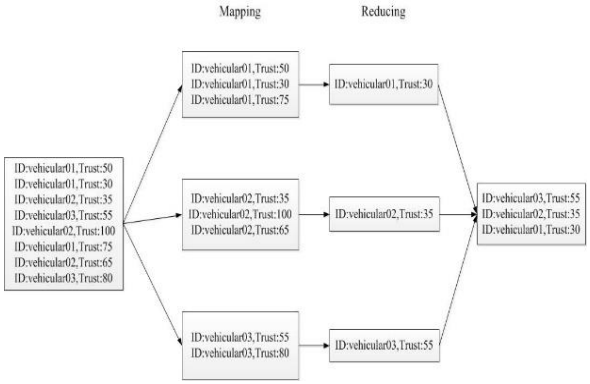

Fig. 3 Trust Management using MapReduce

Based on the game theory [5], all vehicles may be selfish, but they are rational. In this case of the minimum trust value, it can achieve deterrence utility and prevent selfish or malicious of vehicle behavior.

Neighbor vehicles uses the trust value as follows. If the trust value is high, it is trusted by neighbor vehicles. There are three cases: 1. The neighbor vehicles are CA certification. The sender examines the trust value of all neighbor vehicles. Higher trust value, higer priority to be selected in the transmission path [6]. 2. The neighbor vehicles are mixed with CA certified vehicles and non-CA certified vehicles. The sender will first choose CA certified neighbor vehicles in the transmission path, regardless of the level of trust value. 3. The neighbor vehicles are non-CA certification. The sender examines trust value of all neighbor vehicles. Higher trust value, higher priority to be selected in the transmission path.

This paper proposes effective and useful reporting mechanisms in Section 2. In Section 3, we will derive reporting mechanism delay formula. We will show performance analysis and results in Section 4. Finally, it is our conclusion in Section 5.

2. DYNAMIC TRUST REPORTING

RSUs may select one of the following reporting schemes.

1. **Real time Reporting**: In each time slot, RSU requests vehicles to report the trust value information and then Real time Reporting can instant find the trust value of the vehicle. Supposing t is the current reporting time. The t' is the next reporting time. We can denote t'=t+1. Although real time reporting can instant update information, and find whether the vehicle is selfish or malicious, but real time reporting spends cost higher than other reporting schemes since real time reporting reports in every time slot. If the trust value of the vehicles doesn't change often or the fewer vehicles change, other schemes will not need to report.

```
Real time Reporting
Begin
While (True)
{
        Perform reporting
        Wait for a time slot
}
End
```

2. **Periodic Reporting:** RSUs request vehicles periodically to report the trust value information, and update trust value information. Supposing t is the present reporting time. The t' is the next reporting time, and n is periodic reporting time. We have t'=t+n. Although Periodic Reporting spends lower cost than others, Periodic Reporting can't instant find whether a

vehicle is selfish or malicious. If the vehicle is active cooperation transmission message in periodic time, and then vehicle can be selfish or malicious between two reporting.

```
Periodic Reporting
Begin
//n: periodic report time slot
While (True)
{
        Perform reporting
        Wait for n time slots
}
End
```

3. **P-Persistent Reporting**: In each time slot, RSUs probabilistically request vehicles to report the trust information. In this manner, whether reports the trust information or not depends on the probability. Note that, the reporting probability and the selfish or malicious behavior are independently to each other. Supposing t is current reporting time. Assume that t' is the next reporting time and p is reporting probability. The p' is present reporting probability. Then, we can derive
p'=Random (0,1) if(p'<=p) t'=t+1 else t'=t+1.

   Since P-Persistent Reporting reports with a probability lower than Real time Reporting, the cost is lower. We can adjust the reporting probability to make P-Persistent Reporting mechanism become an appropriate mechanism.

```
P-Persistent Reporting
Begin
//p: probability of reporting
//p': random number, and 0≦p'≦1
While (True)
{
        p' = Random (0,1)
        If (p' <= p)
          Perform reporting
        Wait for a time slot
}
End
```

A simple comparison of the reporting mechanisms is shown in Figure 4. The figure has ten straight lines that denote ten time slots and four horizontal lines that denote four reporting methods (Real time Reporting and P-Persistent Reporting and Periodic Reporting). Three reporting mechanisms are denoted rotundity, rectangle, rhombus and triangle, respectively. The small red rotundity denotes that the vehicle has malicious or selfish behavior in the current time slot.

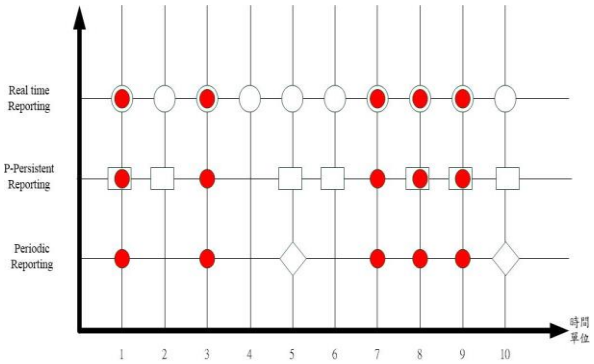

Fig. 4 Request Trust Reports Example

In each time slot, vehicles may change its behavior. Because Real time Reporting reports trust in each time slot, the each time slot appears rotundity in Figure 4. P-Persistent Reporting requests trust reporting probability that is assumed 0.7, and then the figure appears rectangle in 1, 2, 5, 6, 8, 9, 10 time slot respectively. Periodic Reporting is regular reporting where we assumes 5 time slots to report. Then the figure shows rhombus in 5, 10 time slot respectively. The vehicle has malicious or selfish behavior probability that is assumed 0.5. The figure displays small red rotundity in 1, 3, 7, 8, 9 time slots, respectively.

3. PERFORMANCE ANALYSIS

3.1. Reporting delay

In this section we derive the reporting delay for Real time Reporting, P-Persistent Reporting, Periodic Reporting, respectively.

The delay time (RTR_DT) is zero for Real time reporting mechanism. RSU requests vehicles to report whether there is malicious or selfish behavior in each slot time. Therefore, real time reporting mechanism has no delay time.

P-Persistent Reporting (PPR) mechanism doesn't request reporting to obtain vehicles whether there is malicious or selfish behaviour. The p denotes reporting probability, while 1-p denotes the probability without reporting. The pmsn denotes the probability that a vehicle

appears malicious or selfish behavior in each time slot. First, calculating PPR mechanism 1-p, and then multiplying by the previous time and the next time that they don't report, we can obtain

$$\text{PPR\_DT} = (1 - \text{p}) \cdot \text{pmsn} \cdot [1 + \text{PPR\_DT}]$$

That is,

$$\text{PPR\_DT} = (1 - \text{p}) \cdot \text{pmsn} + (1 - \text{p}) \cdot \text{pmsn} \cdot \text{PPR\_DT}$$

After transposing, we can represent

$$\text{PPR\_DT} - (1 - \text{p}) \cdot \text{pmsn} \cdot \text{PPR\_DT} = (1 - \text{p}) \cdot \text{pmsn}$$

And then reducing it

$$\text{PPR\_DT} \cdot [1 - \text{pmsn} \cdot (1 - \text{p})] = (1 - \text{p}) \cdot \text{pmsn}$$

Finally, we can get PPR mechanism delay

$$\text{PPR\_DT} = \frac{(1-p) \cdot pmsn}{1 - (1-p) \cdot pmsn} \qquad (1)$$

Periodic Reporting (PR) mechanism periodically request reporting to obtain whether a vehicle is with malicious or selfish behavior. The i denotes cumulative variable that represents each time slot. The pmsn denotes the probability that a vehicle appears malicious or selfish behavior in each time slot. The n is the period of reporting. We can use the mathematical method to calculate PR mechanism delay time slot i (range: 1~n-1), and multiply by pmsn. Finally, dividing by n for calculate the average delay, we can get

$$\text{PR\_DT} = \frac{\sum_{i=1}^{n-1} i \cdot pmsn}{n} \qquad (2)$$

3.2. Numerical analysis

We analyse the three reporting mechanism in terms of cost and average delay time (ADT) in this section.

$$\text{E(X)} = \frac{\sum_{\text{i=1}}^{\text{Num}} x_i \cdot \text{P}}{Num} \qquad (3)$$

The numerical results for reporting mechanisms are shown in Figure 5. The X is a random variable that denotes appearing time slot. The xi is the present time slot. The P is the reporting probability. The Num is the total reporting number. Finally, dividing the expectation by Num, we can get each time slot of expectation. Real time Reporting reports malicious or selfish behavior in each time slot. Thus, the expectation = (1*1) + … + (10*1) = 55/10 = 5.5. In P-Persistent Reporting the expectation = (1*0.7) + (2*0.7) + … + (10*0.7) = 38/10 = 3.8. In Periodic Reporting the expectation = (1*0.2) + (2*0.2) + … + (10*0.2) = 11/10 = 1.1.

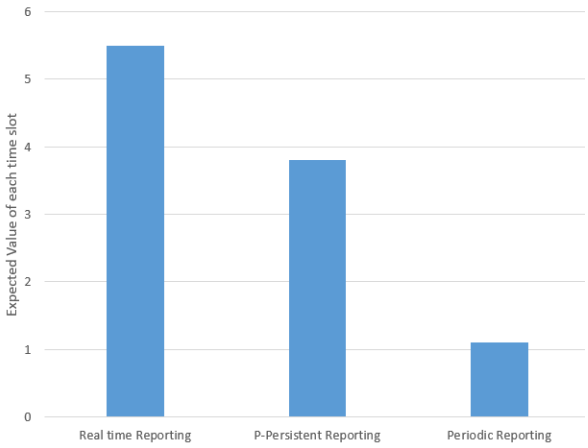

Fig. 5 Reporting malicious or selfish behavior number of expectation

Figure 6 illustrates the average delay for the three methods by calculating the delay time from the time with selfish behavior to the reporting time. Real time reporting requests reporting in each time slot. So RSU can obtain whether vehicles have malicious or selfish behavior immediately, that is, RTR_ADT is zero. The average delay time of P-Persistent Reporting (PPR_ADT) is 0.6 time slots. It denotes that RSUs require 0.6 time slots to obtain whether vehicles have malicious or selfish behaviour or not.

The average delay time of Periodic Reporting (PR_ADT) is 2.4 time slots. That is, RSUs require 2.4 time slots to obtain whether vehicles have malicious or selfish behaviour or not. Generally, PR_ADT is higher than others since Periodic Reporting needs more time to obtain whether vehicles have malicious or selfish behaviour or not. P-Persistent Reporting spends lower delay than Periodic Reporting. Although Real time Reporting spends zero time slot, it consumes higher cost as shown in the following.

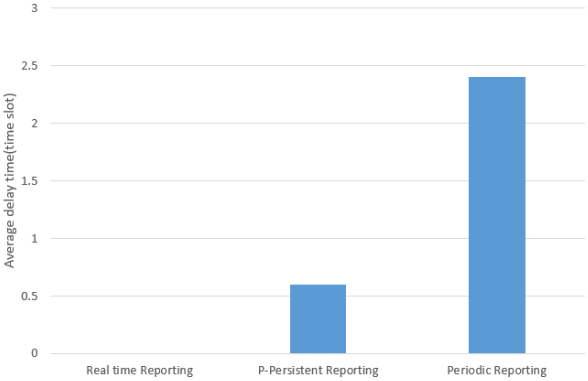

Fig. 6 Average delay time

Figure 7 shows the average reporting cost for the reporting mechanisms. The reporting cost of Real time Reporting (RTR_cost) is

$$\text{RTR\_cost} = 1 \qquad (4)$$

The cost of P-Persistent Reporting (PPR_cost) is

$$\text{PPR\_cost} = p \qquad (5)$$

The cost of Periodic Reporting (PR_cost) is

$$\text{PR\_cost} = \frac{1}{n} \qquad (6)$$

Using Equations (4), (5) and (6), we can compare the three reporting mechanism in terms of reporting cost

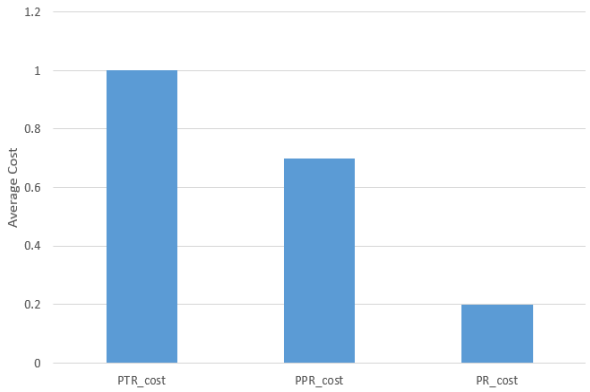

Fig. 7 Comparison in terms of reporting costs

The reporting delay should be as short as possible since vehicles will use the trust value to select a safe and better routing path. In this manner, Real time Reporting will be the best choice. But Real time Reporting spends the highest cost. In Periodic Reporting, the reporting delay leads to a periodic time slot. But the cost of Periodic Reporting cost will be the lowest one. P-Persistent Reporting can dynamically adjust its reporting probability. If a large number of vehicles within the RSU range, RSU increases reporting probability. Otherwise, if a smaller number of vehicles within the RSU range, RSU can decrease the reporting probability.

4. SIMULATION RESULTS

In this section, we show the simulation results for the reporting methods. The simulation program was written in Dev C++. We simulate a vehicle to produce 10000 behaviors in 10000 time slots. The simulation parameters are listed in Table 1.

Figure 8 shows the comparison of the reporting mechanisms in terms of the reporting number (cost). In Figure 8, the X axis denotes the reporting probability and the Y axis denotes the number of reporting. It is obvious that Real time Reporting mechanism has the largest number of reporting in all cases. The reporting number of Periodic Reporting mechanism is lower than the others. The PR is equal PPR, because their reporting probability are same.

TABLE 1
SIMULATE PARAMETER

Parameter name	Function	Value
p	P-Persistent Reporting reports probability	1,0.9,0.8,0.7,0.6,0.5, 0.33,0.25, 0.2,0.16
n	Periodic Reporting reports time slot interval	1,2,3,4,5,6
tmax	Maximum wait time slot	1,2,3,4,5,6
Num	Real time reporting reports number of sum	10000
pmsn	Nodes have malicious or selfish behavior probability	0.5
RTR_ADT	Real time Reporting mechanism gets average vehicle malicious or selfish behavior that its delay time	
PTR_ADT	P-Persistent Reporting mechanism gets average vehicle malicious or selfish behavior that its delay time	
PR_ADT	Periodic Reporting mechanism gets average vehicle malicious or selfish behavior that its delay time	
RTR_DT	Real time Reporting mechanism delay	
PTR_DT	P-Persistent Reporting mechanism delay	
PR_DT	Periodic Reporting mechanism delay	
Trust_value	Trust records number	50,100,150
Time_unit	Time slot	Assume 0.00083(s)
Vehicle_behavior	Vehicle of malicious or selfish behavior	0 or 1

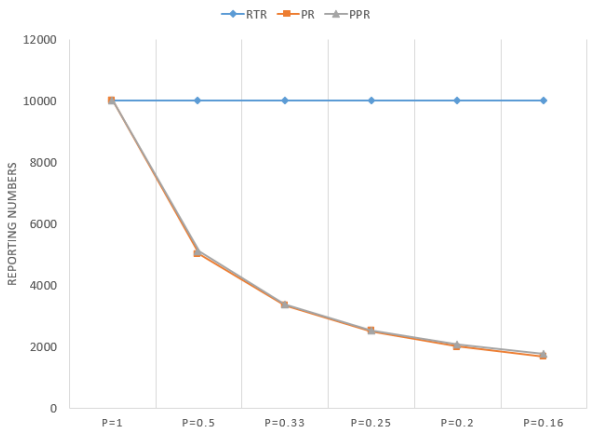

Fig. 8 Comparison in terms of the reporting number (cost)

Real time Reporting has the highest cost because it requests reporting in each time slot. Periodic Reporting is with a low cost because it requires reporting only in a period of time slot. P-Persistent Reporting mechanism has its cost between that of Real time Reporting and Periodic Reporting mechanism using different reporting probability to decide whether reports or not.

The reporting delay is calculated as follows.

reporting delay=upload + download + cloud computing + mechanism delay (That to assume upload, download and cloud computing are 0).

According to 802.11p protocol, the maximum transmission capacity for a vehicle is 27 Mbps (approximately to 3042 KB/sec). Suppose that there are three items records 50, 100 and 150 vehicles trust value text file with their files size are 1.26 KB, 2.53 KB and 3.8 KB (refer to Table 2), respectively. Then the time for transmission will be 1.26/3042 ≒ 41*10-5 (s), 2.53/3042 ≒ 83*10-5 (s) and 3.8/3042 ≒ 124*10-5 (s), respectively.

Real time Reporting mechanism can accurately detect whether vehicles have malicious or selfish behavior or not, but it has to spend time too much. Periodic Reporting mechanism arises more delay time. But Periodic Reporting mechanism has a reporting number lower than others. When P-Persistent Reporting mechanism probability is greater than 0.5, it spends cost much lower than real time reporting mechanism.

TABLE 2
FILE SIZE & TRANSMISSION RATR

	Value
The transmission rate	27 Mbps
50 numbers of trust value	1.26KB
100 numbers of trust value	2.53KB
150 numbers of trust value	3.80KB

Figure 9 shows the both delays of reporting mechanism for simulation (S_RTR_DT, S_PR_DT) and formula (F_RTR_DT, F_PR_DT) calculation.

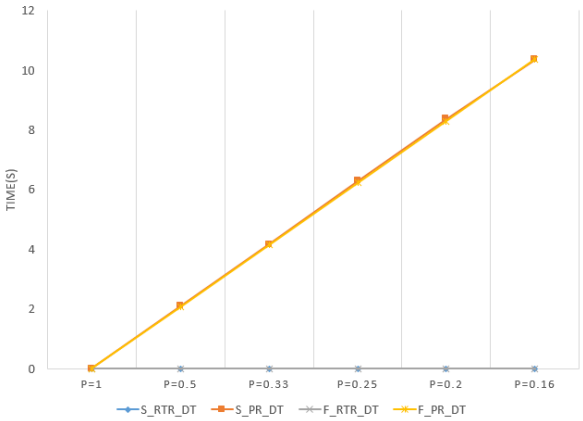

Fig. 9 Comparison of delay for simulation and formula calculation.

Figure 10 compares Real time Reporting and P-Persistent Reporting mechanism in terms of simulation and formula delay when p is greater than 0.5. When p increases, the delay of P-Persistent Reporting mechanism is approaching to 0. In this case, P-Persistent Reporting mechanism spends a cost lower than the others.

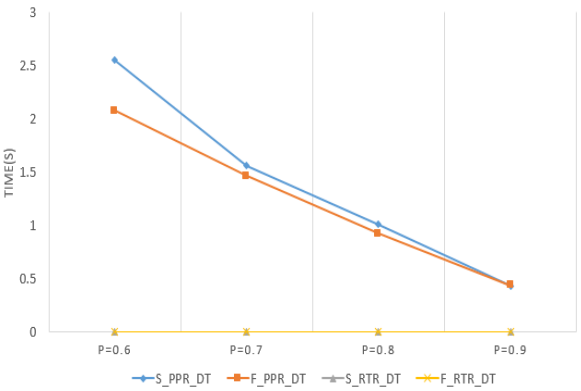

Fig. 10 Comparison of PPR and RTR in terms of formula and simulation

In the following, we compare the dynamic and static P-Persistent Reporting mechanisms. Suppose that the number of vehicles is 90 and 30, respectively. Using static P-Persistent Reporting with a reporting probability 0.7, we can obtain the reporting vehicles number are 840 in 10 sum reporting number. If using dynamic P-Persistent Reporting mechanism with a reporting probability 0.9 in much vehicles case or reporting probability is 0.5 in less vehicles case, we can

obtain the reporting vehicles number is 960 in 10 sum reporting number. Figure 11 allows us easily determine that dynamic P-Persistent Reporting mechanism is better than static P-Persistent Reporting mechanism.

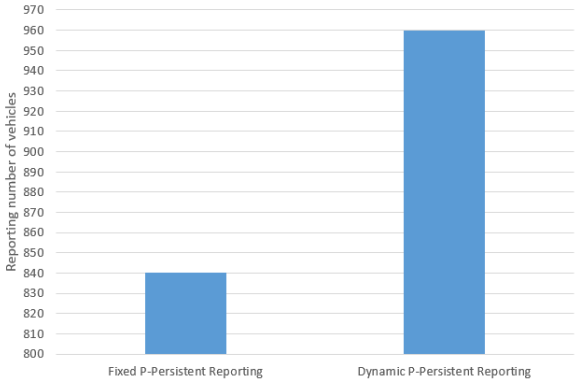

Fig. 11 Comparison of dynamic and static P-Persistent Reporting mechanisms

5. CONCLUSIONS

In this paper, we propose dynamic reporting mechanism against selfish and malicious vehicles. The proposed mechanisms adopt an encryption method for massages, Certificate Authority to verify vehicles to increase reliability of forwarding. Finally, we compare PPR with Real time Reporting (RTR) and Periodic Reporting (PR) in terms of reporting cost and delay. Numerical results show that PPR mechanisms outperform RTR and PR, because PPR can dynamically adjust appropriate reporting probability for the underline environment.

ACKNOWLEDGEMENT

This work was supported in part by the Ministry of Science and Technology under grant No. MOST 103-2221-E-142 -002.

REFERENCES

[1] Baldini, G.; Mahieu, V.; Fovino, I.N.; Trombetta, A.; Taddeo, M., *Identity-based security systems for vehicular ad-hoc networks*, 2013 International Conference on Connected Vehicles and Expo (ICCVE) , pp.672-678, 2-6 Dec. 2013.

[2] Prabhakar, M.; Singh, J.N.; Mahadevan, G., *Defensive mechanism for VANET security in game theoretic approach using heuristic based ant colony optimization*, 2013 International Conference on Computer Communication and Informatics (ICCCI), pp.1-7, 4-6 Jan. 2013.

[3] Chaurasia, B.K.; Verma, S.; Tomar, G.S., *Trust Computation in VANETs*, 2013 International Conference on Communication Systems and Network Technologies (CSNT), pp.468-471, 6-8 April 2013.

[4] Bedi, P.; Jindal, V., *Use of Big Data technology in Vehicular Ad-hoc Networks*, 2014 International Conference on Communications and Informatics (ICACCI), pp.1677-1683, 24-27 Sept. 2014.

[5] Tianrong Zhang; Fan Wu, *Stimulating traffic information transfer in non-cooperative vehicular ad hoc networks*, 2014 International Wireless Communications and Mobile Computing Conference (IWCMC), pp.225-230, 4-8 Aug. 2014.

[6] Doddamani, S.; Kumar, A., *Safety information routing protocol in Vehicular Ad hoc Networks*, 2015 2nd International Conference on Electronics and Communication Systems (ICECS), pp.859-864, 26-27 Feb. 2015.