Towards an Optimum Authentication Service Allocation and Availability in VANETs

Safi Ibrahim[1], Mohamed Hamdy[1], and Eman Shaaban[2]
(Corresponding author: Mohamed Hamdy)

Information Systems Department, Ain Shams University[1]
Computer Systems Department, Ain Shams University[2]
Al Khalifa Al Maamoun st., Abbassia , 11566 Cairo, Egypt
(Email: m.hamdy@cis.asu.edu.eg)

(Received May 28, 2016; revised and accepted Aug. 9 & Sept. 5, 2016)

Abstract

Authentication as a security key issue is required for securing the inter-vehicle communication. Mostly, authentication schemes that depend on the network infrastructure Road Side Unit (RSU) had been proven to have low computation and communication overhead. RSUs may become unavailable due to congestion or failure conditions. Replicating authentication service offered by RSUs to trusted vehicles in their ranges may present novel alternative to support the availability of such services. A complement to our previous replication protocol Central Push-based Replication Protocol (CPRP) is presented in this work. Two new replica allocation techniques are proposed to spawn new replicas in order to improve the authentication service availability that are offered from RSUs. The optimality (Correctness) of these techniques has been evaluated with different ratios of RSU failures in different realistic scenarios. The results showed that both techniques improve CPRP in increasing the authentication services availability.

Keywords: Allocation; Authentication; Availability; Road Side Unit; VANET

1 Introduction

Exchanging life critical messages in VANETs requires authentication. Many security researches consider authentication as the most important security issue for exchanging such messages. Authentication is needed to prove that the sender is the actual owner of the message and to avoid impersonation attack. Some Studies show that authentication services offered by Road Side units (RSU) have less computation and communications calculations than others [20, 21]. RSUs are located at certain positions on the road network similar to access points in traditional wireless networks to provide the necessary infrastructure support for network setup and communications.

RSUs may become unavailable due to congestion, physical damage or because of their high deployment and maintenance cost. Unavailability of RSUs will cause absence of vehicles communications at those areas. Replicating authentication services from RSUs to vehicles may offers an alternative to support such service availability when they are unavailable.

Replication is a classical approach for increasing service or data availability in wired or wireless networks. Pushing Authentication service from RSUs to vehicles may raises two questions : when to replicate the service and how to select the vehicle which will hold the replica.

Replication cost can be defined as the number of active replicas in the network at certain time. However, replica Allocation correctness measures how the distribution of replicas is optimum.

This work is a complement of our work that was published in [9]. The proposed Central push-based Replica Protocol (CPRP) was introduced to increase the availability of authentication service offered from the RSUs.

CPRP has three basic mechanisms: replica allocation, replica activation and replica deallocation. Its basic idea is to push the authentication service by RSU to replicate it to the most central vehicle in its communication range which is the nearest to the RSU. This replica still inactive until it finds that no RSU in its range. It becomes active replica and replaces the RSU in authenticating vehicles in this area.

As mentioned, the communication range of vehicles is quarter that of RSUs, thus vehicle can't cover as many vehicles when it becomes active. Another replicas should be spawned to assist the replica in authenticating vehicles.

In this work, two methods are proposed for generating new replicas. The first is the Epidemic-based scheme which doesn't depend on network analysis. It generates new replicas by pushing replicas epidemically. The second is topology-based scheme which depends on analyzing the network and compute node degrees, then push the subreplicas to vehicles with high degrees. In general, the topology analysis exposes the network to more security threats. The service provider vehicle should reveal the real identity for all analyzed vehicles to avoid malicious ones and to prevent impersonation attacks. Both methods are explained and evaluated in the next sections. Both techniques are compared in terms of enhancement the performance of CPRP on increasing the availability of the authentication service offered from RSU. They are also compared in terms of their replication degree and correctness of replica allocation.

The rest of the paper is organized as follows: Section 2 presents the literature review. In Section 3, basic assumptions for the two proposed schemes: Epidemic-based and Topology-based are stated. Section 4 introduces the proposed epidemic based scheme. The topology-based scheme is presented in Section 5. Simulation Configuration is introduced in Section 6. Section 7 presents comparison evaluation for the protocols in terms of authentication service availability improvement, Increase in replication degree and replica allocation correctness. Section 8 presents conclusion of work.

2 Related Work

In this section the literature review is introduced in terms of three points. On the one hand, authentication has an increasing interest from research in VANETs. It represents the key function of communication in any network. On the other hand, recently, researches on increasing the availability of network functionalities provide promising opportunities to achieve better security function. Data and service replication have been introduced in this work as an important mean for preserving the availability. Finally, Optimality (Correctness) of replica allocation schemes are introduced.

2.1 Authentication

Public Key Infrastructure (PKI) scheme is implemented in [16, 17, 19]. This scheme requires that each vehicle should be preloaded with a large number of public and private key pairs and the corresponding public key certificates. PKI requires large storage space in vehicles. Authority takes long time for tracking misbehaving vehicles due to long revocation list. Updating certificate revocation lists in vehicles consumes long time.

Many researches had tackled how to overcome the problems triggered by using PKI. In [21], (RAISE) rsu-aided message authentication scheme is proposed. RAISE is a symmetric key authentication scheme. In RAISE, RSUs assist vehicles in authenticating messages. Each message is attached with a short keyed-hash message authentication code (HMAC) which is generated by the vehicle, and the RSU in the range. RSU sends notice of authenticity to each vehicle. With the short HMAC attached to the message, the verification of message authenticity can be performed in a fast and efficient way. Although this technique outperforms PKI, it is not scalable. If two vehicles are not in the same range of the same RSU they can't communicate. Scalability problem was solved in [20]. Vehicle generates symmetric secret key with the first RSU it pass by. Then it uses this symmetric key to generate session keys with RSUs that are controlled by the same CA.

In [8], an anonymous ring signature scheme is introduced. This scheme outperforms the above schemes in which it offers low storage requirements and fast message authentication. It also doesn't depend on RSUs in authenticating vehicles.

In [3], they proposed an efficient message authentication scheme which is not vulnerable to impersonation attack based on elliptic curve cryptography.

2.2 Data and Service Replication

There are several studies that address service replication. Service replication is classified into two major classes interms of spawning new replicas. The first class doesn't depend on network topology analysis to make the replication decisions. This type is network transparent. Replication decisions occur at application layers and no information is required from lower network layers. [4] and [12] have largely been based on schemes that epidemically push the service on all available nodes. Using all nodes as a service holder is wasteful and unnecessary.

In [5], (SDP) Service Distribution Protocol For MANET is proposed. In SDP, the replication decision is based on service popularity which can be gained from client interest in the services. The service is replicated by the client with the highest interest in the service. This approach can achieve high service availability and correct service distribution.

Second class requires network topology. In [11] RegRes (Region Resident Service approach) is proposed. Each service determine its desired service carriers density within region. The RegRes runs on the carries to estimate the current density of service carriers. Then it applies a spawn policies to decide when and which node to spawn as new carriers. It account for variable node density, variable node mobility, replication cost and carriers that fail or leave the region.

In [1] V-PADA Vehicle Platoon Aware Data Access, a service replication solution. The concept lying behind this approach, is that vehicles move in platoons and follow the leader of the platoon. A vehicle which has a service to share with other vehicles in the same platoon, can predict platoon splits. If a vehicle leaves a platoon, it transfers its services or data to other vehicles to be able to access it. Each node has four states to be transferred between them, initials, Join, Quasi split and split.

In [2], Scalable data lookup and replication protocol for MANET (SCALAR) is proposed. SCALAR depends on constructing a connected dominating set based on a network graph. This set forms a virtual backbone upon which data or service replication takes place. SCALAR had solved the scalability and data accessibility of services and data in large networks. However, unneeded replicas may ba generated. SCALAR overloads the network with the dominating set computational overhead and recovery.

2.3 Optimality of Replica Allocation

Service replication protocols overload the network with additional computation overhead.

The optimality or correctness of replica allocation can reflect the optimal service distribution all over the network. In [5], they proposed a measure of correctness to mobile ad hoc network (MANET), which is a relation between the number of available active replicas inside a given partition and its size. The two proposed methods are *Linear Correctness Ratio* and *Rational Correctness Ratio*. They assumed that the correctness ratio is bounded between 0% and 100%. In Linear Correctness, If the partition has no replica, the ratio of correctness will be 0%. Else, if there is one or two replicas in the same partition, correctness ratio will be 100%. Otherwise, it is linearly inversely proportional to the number of replicas.

However, in rational correctness ratio; it is more sensitive to the number of active replicas inside a partition.

3 Basic Assumptions

In this section, some basic assumptions are stated as follows:

- As an extension to our previous work [9], the concrete authentication scheme that is applied in this work is Symmetric key Scheme of VANETs, because of its low computation and communication overhead compared to Public Key Infrastructure [21].
- Only the replica that is pushed by the RSU has the privilege to spawn new replicas and is termed Replica.
- Replicas spawned from the vehicle replica are considered Followers and haven't the privilege to spawn new replicas.
- Communication range of the replica is quarter than that of the RSU.
- If one of followers loose the connection of the Replica because it is out of its range it become invalid item If the Replica become inactive or hibernated because it enters RSU range, it hibernates all its Followers.

4 Epidemic Based Scheme

Epidemic based scheme is one of the proposed techniques to improve the performance of CPRP by epidemically spawn new replicas.

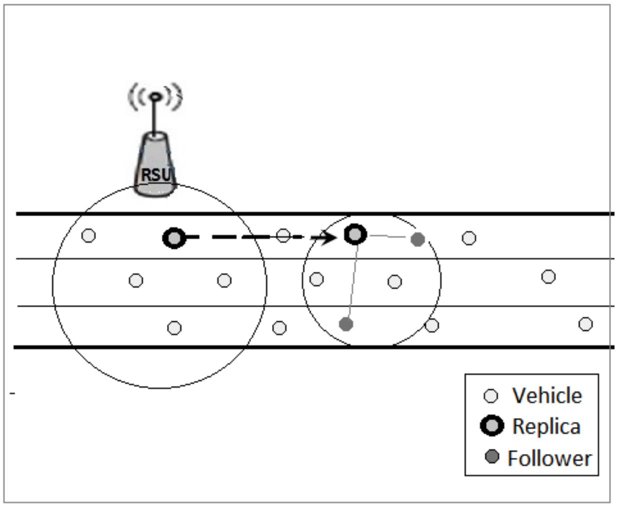


Figure 1: Spawning new replicas by epidemic-based approach

Figure 1 explains the mechanism of generating new replicas using this scheme. After the replica that is pushed by RSU becomes active because it is in uncovered area. It pushes the replica epidemically to the two farthest vehicles with in its communication range. one is in its movement direction. The other, is in the opposite movement direction. The two generated replicas becomes followers to the main replica.

At each second, the main replica checks if it has two replicas within its communication range. If it looses one or both, it reassigns new replicas.

Algorithm 1, summarizes the process of the epidemic based scheme as follows:

Algorithm 1 Enhance replica allocation protocol by epidemically analysis

```
Begin
for EACH SECOND do
    for all Active $Vrep$ do
        if $Vrep$ doesn't find Followers in its range then
            $Vrep$ calculates Dist with its neighbors
            $Vrep$ chooses the two farthest neighbors to
            push SUB-REPLICA
            The first in its direction
            The other in opposite direction
            $Vrep$ assign SUB-REPs as followers replica to
            it
        end if
    end for
end for
```

5 Topology Based Scheme

Topology based scheme is the second proposed scheme to enhance CPRP performance. This scheme depends on topology analysis of the network. After the replica that is pushed by RSU becomes active because it is in uncovered area.

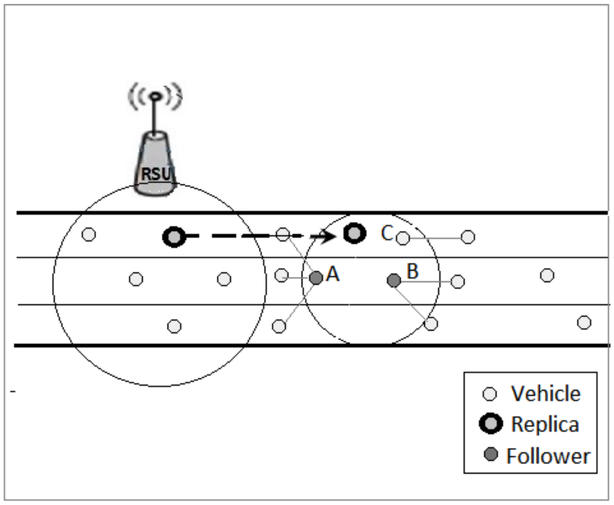


Figure 2: Spawning new replicas by topology analysis based approach

It sends inquiry to its neighbors about their degrees. Then, calculates the average degree received from all neighbors. Finally, it pushes its replica to nodes which have degrees more than the average degree.

Figure 2 explains the toplogy based scheme as follows: when the replica is out of the RSU range it becomes active. It sends to its neighbors vehicles inquiry about their neighbor number. Vehicle A replied with three neighbors, vehicle B replied with two neighbors and vehicle C replied with one neighbor. Replica vehicle calculate the average number of vehicles as $(3 + 2 + 1)/3 = 2$. Then, it makes decision to choose vehicles A and B which have two or more neighbors to push its replica.

Algorithm 2 summarizes the mechanism of the topology-based scheme as follows:

Algorithm 2 Enhance replica allocation by topology analysis

```
Begin
for EACH SECOND do
    for all Active $Vrep$ do
        $Vrep$ sends inquery to its neighbors about their DEG
        $Vrep$ calculate TOT-DEG from all neighbors
        $Vrep$ calculate AVG-DEG
        $Vrep$ push SUB-REP to neighbor V which has DEG greater than AVG-DEG
        $Vrep$ assign SUB-REPs as followers replica to it
    end for
end for
```

6 Simulation Configuration

In simulating this work, we use SUMO [18][1] (Simulation of Urban Mobility) to model the movement of vehicles. For network simulation we use OPNET [13, 15][2]. The vehicles movement are generated using car following model that explained in details in [14].

In this simulation we use a frame work proposed in [10] to simulate VANETs SUMO with OPNET. With SUMO we generate network and route files, then simulate all vehicles positions at each second. These positions are written in a dump file. We use the trace exporter for OPNET which is implemented and explained to generate one xml topology file with trajectory for each vehicle.To generate vehicles movement we use randomTrip.py module which assigns a trip for each vehicle randomly.

For simplicity we use bidirectional highway with length 5km, we used 400m as the RSU range and 100m as the vehicles range. RSUs are placed at 350m distance between each other. The average number of simulation's run is three. Table 1 summarizes the simulation configurations.

Table 1: Table of configuration parameters

Parameter	Value
Way	bidirectional highway
No. of lanes	two
Way Length	5 KM
RSU range	400 m
Vehicle range	100 m
RSU separated dis.	350 m
Hand off area	50 m
Mobility model	CAR FOLLOWING MODEL
Vehicle movements	random trips

7 Evaluation and Discussion

In this section, evaluation and comparison of the proposed techniques: epidemic based and topology based technique are done in terms of availability improvement, replication degree and replica allocation correctness.

As a complement of our previous work, simulation is done with the same configuration. 24 scenarios are generated for the simulation and are divided into two groups. We assume four RSUs failure ratios at: 30%, 50%, 70%, 90%. For the first group we have 12 scenarios generated as follows: For each RSU failure ratio, three scenarios are generated; with high network density, moderate network density and low network density. The same has done for the second group. For each RSU failure ratio, also three scenarios are generated but with high vehicles speed, moderate vehicles speed and low vehicles speed.

[1] A microscopic traffic vehicle simulator http://sourceforge.net/projects/sumo/

[2] Version 17.1, licensed to NTI (National Telecommunication Institute)

7.1 Availability Improvement

Authentication service availability is computed by accumulating and averaging the availability of all vehicles during the network life time.

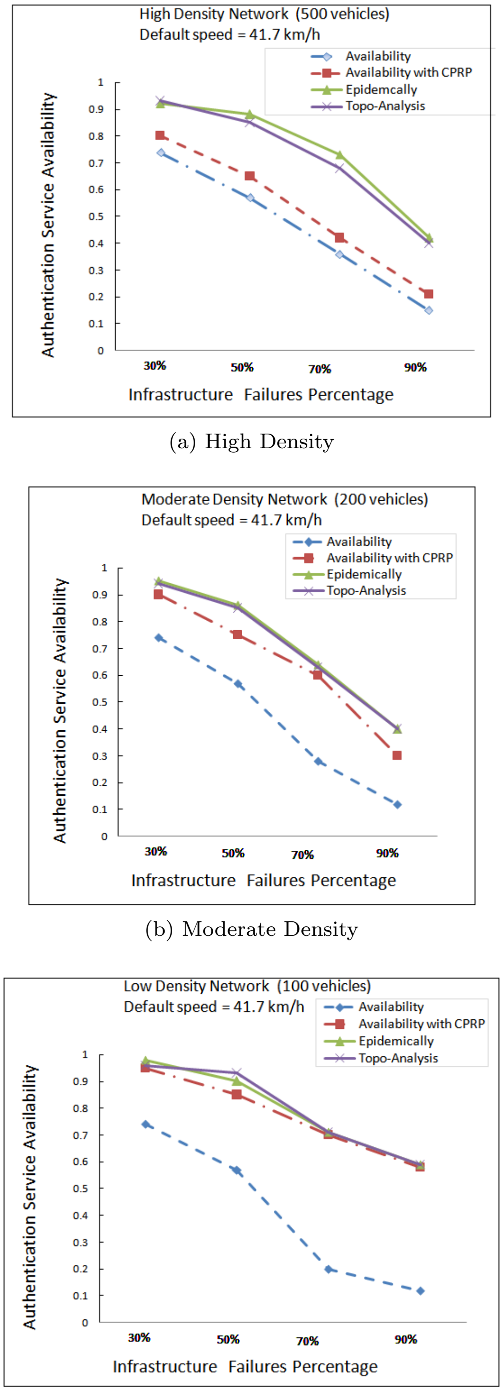
$$AuthAvail = \frac{1}{N}\sum_{i=1}^{N} A(v_i) \quad (1)$$

where $AuthAvail$ is the total Authentication Service Availability, N is the total number of vehicles, $A(v_i)$ is the vehicle i availability and is measured as follows:

$$A(v_i) = \begin{cases} 1 & \text{v}_i \in RSU_i or Replica \\ 0 & \text{otherwise} \end{cases} \quad (2)$$

First, when applying these techniques using the different network densities shown in Figure 3. We can observe that they converge and almost have the same performance in the three different densities. This is because both techniques spawn new replicas to improve the authentication service availability. The epidemic-based generates replicas surround the original, while topology-based selects the suitable vehicle by topology analysis. They improve the performance of CPRP in high density with highest difference about 2%. It is also observed that in high density network, the epidemic method slightly outperforms the topology based.

Next, when applying both techniques on different speed networks as shown in Figure 4. It can be observed that they converge also in their performance to be almost the same. They improve the performance of CPRP in low speed networks with highest difference about 1.3%. It is observed that the epidemic based slightly outperforms the topology based in moderate speed. However, in low speed density the topology based outperforms epidemical based.



(a) High Density

(b) Moderate Density

(c) Low Density

Figure 3: Authentication service availability improvement using two techniques vs. different network densities

7.2 Increase in Replication Degree

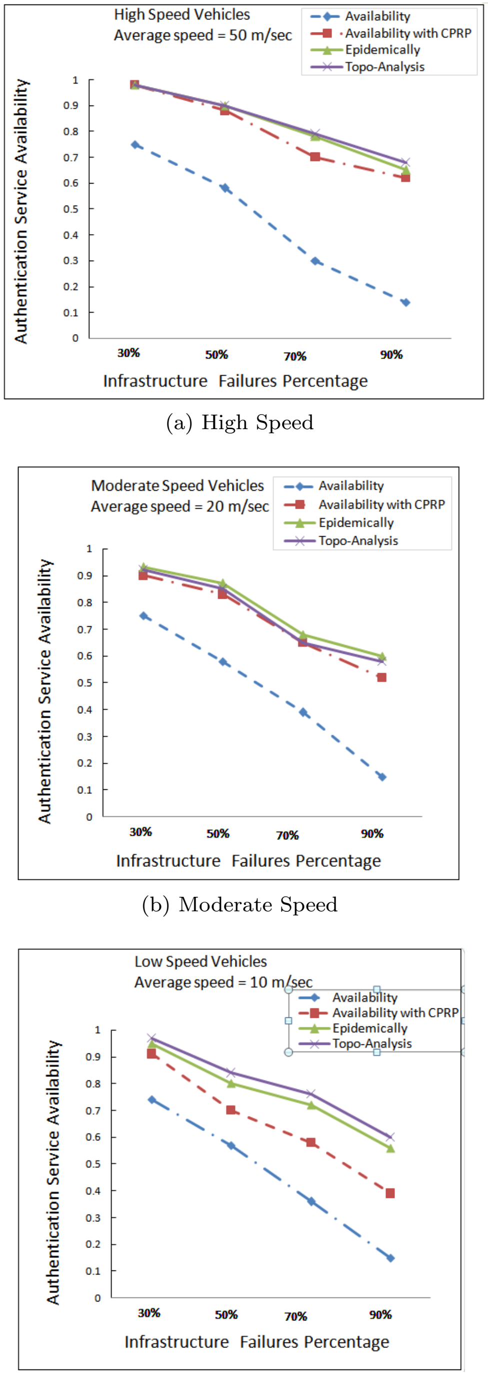
In this subsection, the results of using the two proposed techniques (Epidemic & Topology) to improve the performance of CPRP on increasing the replication degree during the network lifetime are displayed.

$$ReplicationDegree\% = \frac{1}{N}\sum_{i=1}^{N} V_i rep \cdot 100 \quad (3)$$

where N is the total number of vehicles and $V_i rep$ represents vehicle i that holds a replica.

Figures 5, 6 shows these effects on different network densities and different network speeds respectively. It is observed that applying both techniques begin with a value at 30% infrastructure failure then increases at 50% of infrastructure failure and finally decrease at 70% and 90%. The explanation of this is at low infrastructure failures spawning new replicas is low because the infrastructure existence hibernates the active replicas and prevents spawning new ones. From 70% infrastructure failure the situation changed because the main source to generate original replicas is the infrastructure. These replicas then can spawn new replicas.

First, for different network densities as shown in Figure 5. It is observed that applying both techniques, add



(a) High Speed

(b) Moderate Speed

(c) Low Speed

Figure 4: Authentication service availability improvement using two techniques vs. different vehicles speeds

additional replication efforts which cause additional waste of resources. Topology based technique has better performance in all scenarios and almost the same but with few decrease in high density network. The average replication degree increases after applying topology based by about 1% in high density network, 1.5% in moderate density network and by 1.75% in low density networks. On the other hand, applying epidemic based adds extra additional waste of resources in all densities scenarios. Average replication degree increases after applying epidemic by about 3% in high density network, 4.6% in moderate density network and by 7.6% in low density network. So, both topology based and epidemic based have low replication degree in high density network then it increases by decreasing the density. The interpretation is due to definition of replication degree which is the percentage of number of replicas over total nodes. So, the replicas ratio to total total nodes increases by decreasing the network density. Topology based outperforms epidemic based by 2% in high density, 3.1% in moderate density and by 5.85% in low density.

Second, for different network speed as shown in Figure 6. Also, applying both techniques add additional replication efforts which cause additional waste of recourse. Topology based outperforms the epidemic based in all scenarios and almost the same in all scenarios with few improvements in low speed networks. The average replication degree increases after applying topology based by about 1.3% in low speed network, 1.7% in moderate speed network and by 2.3% in high speed networks. On the other hand, applying epidemic based adds extra additional waste of resources in different speeds scenarios. Average replication degree increases after applying epidemic by about 2.5% in low speed network, 3.7% in moderate speed network and by 7.6% in high speed networks. So, both topology based and epidemic based have low replication degree in low speed network then it increases by increasing the speed. The interpretation of this is due to the increase of vehicles speeds allows for increasing of spawning new replicas when replicas reached an area not covered with infrastructure. So, the replicas ratio to total total nodes increases by increasing the network speed. Topology based outperforms epidemic based by 1.2% in low speed, 2% in moderate speed and by 5.3% in low speed.

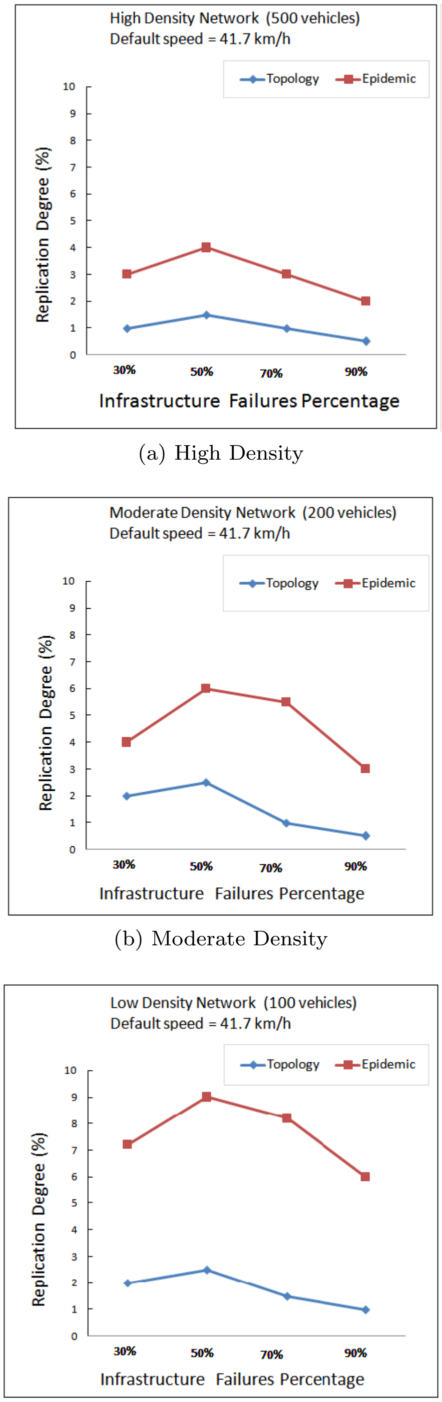
7.3 Replica Allocation Correctness

The replica allocation correctness means how the distribution of the generated replicas is optimal. In [6, 7], they proposed four different allocation correctness methods. In this work we propose a new replica allocation correctness for the optimal distribution of services in VANET.

Replica Allocation Correctness for the whole network is computed by accumulating and averaging the correctness values for all vehicles During the network lifetime as shown in Equation (4).

$$RAC = \frac{1}{N}\sum_{i=1}^{N} C_v(v_i) \qquad (4)$$

where RAC is the Total replica Allocation for the whole network, N is the total number of vehicles, $C_v(v_i)$ is the

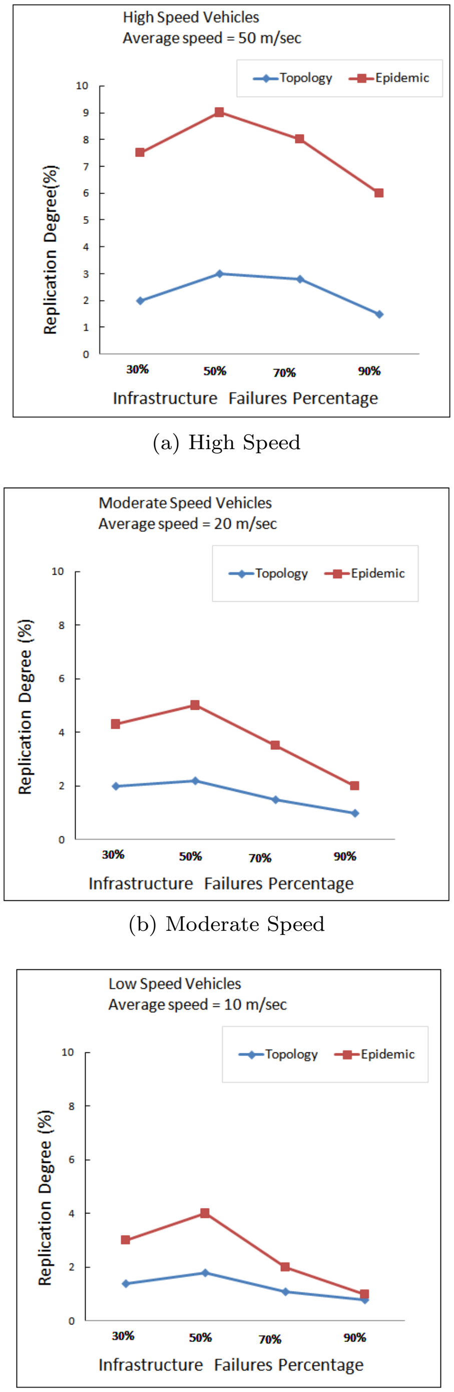


(a) High Density

(b) Moderate Density

(c) Low Density

Figure 5: Increase of replicas percentage vs. different network densities



(a) High Speed

(b) Moderate Speed

(c) Low Speed

Figure 6: Increase of replicas percentage vs. different vehicles speeds

vehicle's i correctness value and is measured as illustrated in Equation (5):

$$C_v(v_i) = \begin{cases} 0 & r = 0 \\ 1 & r = 1 \\ \frac{n-r}{n-1} & r > 1 \end{cases} \quad (5)$$

where r represents the sum of replicas that exist in the range of the vehicle v_i, and n represents the number of neighbors of the vehicle v_i.

The explanation of how to compute replica correctness value at each vehicle is as follows: if the vehicle is not in range with any RSU and have no replica in its range its correctness will be zero. But, if it has 1 replica in its range, its correctness is one. Otherwise, it is computed related to its neighbor as shown in the equation. This ratio adapts to congestion conditions. Figure 7 illustrates an example of VANET in ad hoc mode in the area that lack infrastructure. Gray nodes represent replicas. By using the Equation (5), vehicle A has no replica in its range its correctness is zero.Vehicle C has replicas on all of its neighbors, so its correctness is zero. Vehicle E has 1 replica so, its correctness is 1. Vehicles that have more than one replica in its range their correctness is computed related to their number of neighbors. If the number of neighbors is large it has greater correctness. Vehicle B has 2 replicas and 3 neighbors so its correctness is 1/2. Vehicle D has 5 neighbors, and has 2 replicas. Its correctness value is 3/4.

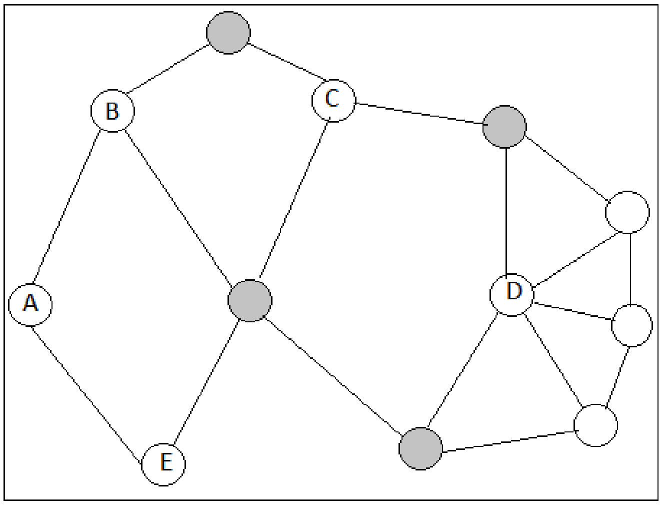
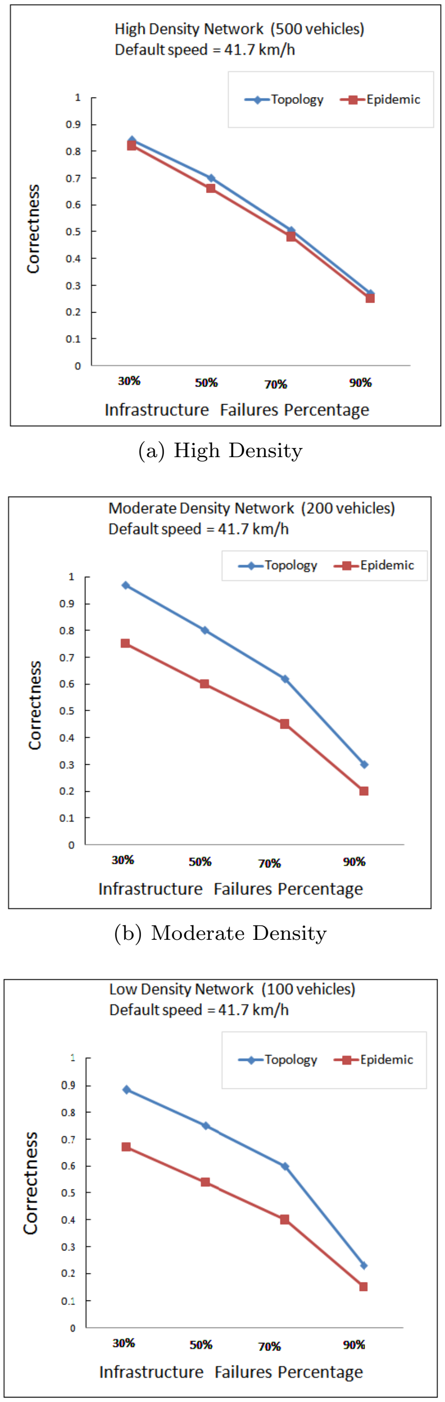


Figure 7: Example of replica allocation correctness

Figure 8 illustrates the replica allocation correctness values for both techniques using different network densities and different infrastructure failure ratios. It is observed that topology based schemes outperforms the epidemic based in almost all scenarios. Topology based scheme has the best performance with the moderate network density with average correctness about 67% for all infrastructure failure ratios. Then it achieves an average of 61% for low density network, and about 58% in High density networks. The interpretation of this is due to the topology scheme which depends on the analysis of network. When it is applied for high density networks there still vehicles not covered by infrastructure or one of the replicas especially with high infrastructure failure ratios. On the other hand when it is applied with low network densities; there may be additional unused replicas that decrease the correctness of the scheme. So, the optimum or best value gained from applying this scheme on different network densities is with the medium density network.

When the epidemic based scheme is applied with different network densities and with different infrastructure failure ratios, it shows the best average with high density network with about 55%. Then about 50% average correctness for medium density network, and 44% average correctness value for low density networks. This is interpreted as the epidemic scheme may generate additional useless replicas as density of the network decreases. So, it has its best correctness value with High Density Networks.



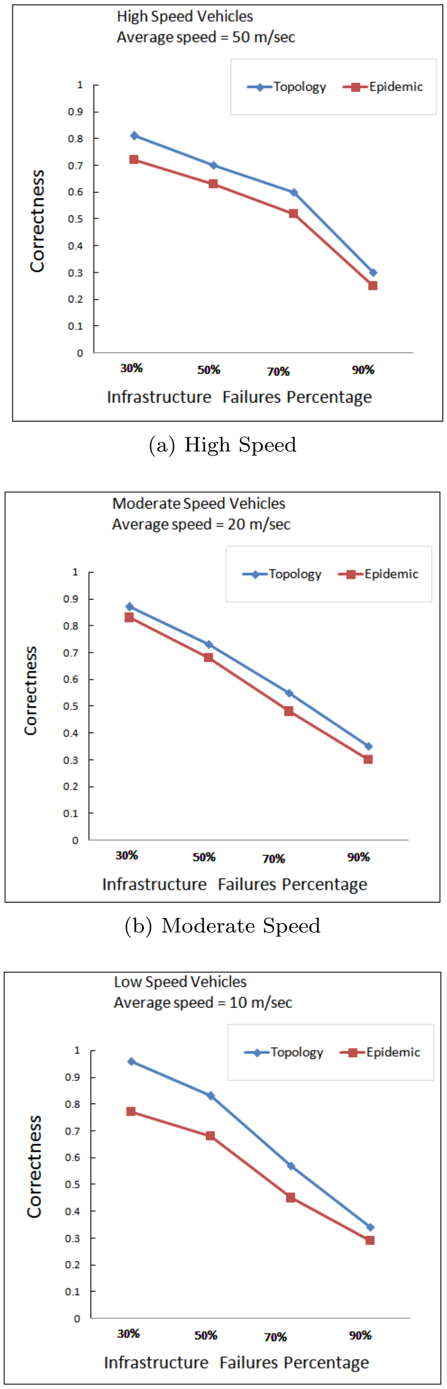
(a) High Density

(b) Moderate Density

(c) Low Density

Figure 8: Correctness of replica allocation VS. different network densities

Second, Figure 9 shows the replica allocation correctness values for both techniques using different network



(a) High Speed

(b) Moderate Speed

(c) Low Speed

Figure 9: Correctness of replica allocation VS. different Vehicles speeds

speeds and different infrastructure failure ratios. It is observed that topology based schemes outperforms the epidemic based in almost all scenarios. Topology based scheme has the best performance with the low speed network with average correctness about 67% for all infrastructure failure ratios. Then it achieves an average of 62% for moderate speed network, and about 60% in High speed networks. The interpretation of this is due to the topology scheme which depends on the analysis of network. When it is applied for low speed networks; the changing in replicas locations occur slowly which results in more stable availability. On the other hand, when it is applied with high speed networks the changing of replica allocation happens rapidly. So, applying the topology based scheme to improve the availability of CPRP has its best average correctness value with low speed networks, then with moderate speed then with high speed networks.

When the epidemic based scheme is applied with different network speeds and with different infrastructure failure ratios, it shows the best average correctness with moderate speed network with about 57%. Then about 55% average correctness for low speed network, and 53% average correctness value for high speed networks. This is interpreted as the epidemic scheme which depends on generating replicas epidemically generates more replicas in high speed networks. On the other hand, it generates insufficient replicas with the low speed networks. So, it has its best average correctness performance with moderate speed networks.

8 Conclusions

In this work, two schemes are proposed to improve the performance of CPRP protocol in terms of increasing the availability of authentication service offered by RSU in cases RSU unavailability. The first scheme is epidemic-based which spawns new replicas epidemically and doesn't depend on network analysis. The second scheme is topology-based scheme which depends on analyzing the network and compute node degrees, then pushes the new replicas to vehicles with high degrees.

This work is a complement to our previous work. Simulation is done with the same configuration. 24 scenarios are generated for the simulation and are divided into two groups. Four RSUs failure ratios are assumed at: 30%, 50%, 70% and 90%.

For the first group, 12 scenarios are generated as follows: for each RSU failure ratio, three scenarios are generated; with high network density, moderate network density and low network density. The same has done for the second group. For each RSU failure ratio, also three scenarios are generated but with high vehicles speed, moderate and low vehicles speed.

The performance of the two proposed schemes are compared and evaluated in terms of improve the availability of authentication service offered by RSU, increase in replication degree and optimality (correctness) of replica allocation.

Although, the topology-based scheme exposes the network to more security threats because it depends on network analysis which requires revealing the real identity of more vehicles, it shows better performance in all scenarios.

Table 2: Performance evaluation of both epidemic-based and topology-based with different network densities

Network	High Density	Moderate Density	Low Density
Improve Availability with Epidemic	21.8%	7.6%	2.5%
Improve Availability with Topology	19.4%	6.8%	2.7%
Replication Degree with Epidemic	3%	4.6%	7.6%
Replication Degree with Topology	1%	1.5%	1.75%
Correctness with Epidemic	55%	50%	44%
Correctness with Topology	58%	67%	61%

Table 3: Performance evaluation of both epidemic-based and topology-based with different speed networks

Network	High Speed	Moderate Speed	Low Speed
Improve Availability with Epidemic	3.25%	4.5%	11.25%
Improve Availability with Topology	4.25%	2.5%	14.7%
Replication Degree with Epidemic	7.6%	3.7%	2.5%
Replication Degree with Topology	1.3%	1.5%	1.7%
Correctness with Epidemic	53%	57%	55%
Correctness with Topology	60%	62%	67%

First, the performance of the two schemes are evaluated for the first group (Different Network Densities) as shown in Table 2.

- In terms of increasing the availability of authentication service: When applying the two techniques, they achieve about the same performance. But, they improve the performance of CPRP in high density with highest difference.
- In terms of increase in replication degree, topology-based scheme has better performance in all scenarios and is almost the same. Highest value of average replication degree by applying the topology-based scheme is with low density network. By applying epidemic-based scheme, the average replication degree has its greatest value also with low density network.
- In terms of correctness of replica allocation, topology-based scheme outperforms the epidemic-based in almost all scenarios. Topology-based has the highest average correctness with moderate density network. By applying epidemic based scheme, it shows the best average correctness performance with high density network.

Second, the performance of the two schemes are evaluated for the second group (Different speed networks) as shown in Table 3.

- In terms of increasing the availability of authentication service: When applying the two techniques, they converge to be almost the same. The improve the performance of low speed networks with highest difference. It is observed that the epidemic based scheme outperforms the topology based in moderate speed with few difference. But, in low speed network the topology based outperforms the epidemic based.
- In terms of increase in replication degree, topology-based outperforms the epidemic-based in all scenarios with few improvements in low speed networks. Average replication degree has its greatest value with high speed networks. By applying epidemic-based scheme. the average replication degree has its highest value also with high speed networks.
- In terms of correctness of replica allocation, topology-based scheme outperforms the epidemic-based in almost all scenarios. Topology-based has the highest average correctness with low speed network. By applying epidemic based scheme, it shows the best average correctness performance with moderate speed network.

References

[1] P. AGITH, "Enhancement of vehicular ad-hoc networks using vehicle platoon aware data access," *International Journal of Modern Engineering Research*, vol. 2, no. 2, pp. 273–277, 2012.

[2] E. Atsan and O. Ozkasap, "Scalar: Scalable data lookup and replication protocol for mobile ad hoc networks," *Computer Networks*, vol. 57, no. 17, pp. 3654–3672, 2013.

[3] M. Bayat, M. Barmshoory, M. Rahimi, and M. R. Aref, "A secure authentication scheme for vanets with batch verification," *Wireless Networks*, vol. 21, no. 5, pp. 1733–1743, 2015.

[4] M. Caliskan, D. Graupner, and M. Mauve, "Decentralized discovery of free parking places," in *Proceedings of the Third International Workshop on Vehicular Ad Hoc Networks (VANET'06)*, pp. 30–39, Los Angeles, CA, USA, Sept. 2006.

[5] M. El-Eliemy, *Service replication in wireless mobile ad hoc networks*, PhD thesis, Friedrich Schiller University of Jena, 2010.

[6] M. Hamdy and B. König-Ries, "An extended analysis of an interest-based service distribution protocol for mobile ad hoc networks," in *Proceedings of the International Conference on Wireless Information Networks and Systems (WINSYS'08)*, pp. 203–210, Porto, Portugal, July 2008.

[7] M. Hamdy and B. König-Ries, *Service Availability, Success Ratio, Prevalence, Replica Allocation Correctness, Replication Degree, and Effects of Different Replication/Hibernation Behavior Effects of the Service Distribution Protocol for Mobile Ad Hoc Networks*, Germany: University, 2008.

[8] Y. Huang, S. Zeng, and X. Liu, "Privacy-preserving communication for VANETs with conditionally anonymous ring signature," *International Journal of Network Security*, vol. 17, no. 2, pp. 135–141, 2015.

[9] S. Ibrahim and M. Hamdy, "Enabling less-infrastructure road communication networks for vanets," in *Proceedings of The fourth4th International Conference on Computer Science and Network Technology (ICCSNT'15)*, pp. 1–7, Harbin, China, Dec. 2015.

[10] F. Kaisser, C. Gransart, and M. Berbineau, "Simulations of VANET scenarios with OPNET and SUMO," in *4th International Workshop on Communication Technologies for Vehicles*, pp. 103–112, Vilnius, Lithuania, Apr. 2012.

[11] E. Koukoumidis, L. Peh, and M. Martonosi, "RegReS: Adaptively maintaining a target density of regional services in opportunistic vehicular networks," in *Ninth Annual IEEE International Conference on Pervasive Computing and Communications (PerCom'11)*, pp. 120–127, Seattle, WA, USA, Mar. 2011.

[12] U. Lee, E. Magistretti, M. Gerla, P. Bellavista, and A. Corradi, "Dissemination and harvesting of urban data using vehicular sensing platforms," *IEEE Transaction on Vehicular Technology*, vol. 58, no. 2, pp. 882–901, 2009.

[13] Z. Lu and H. YANG, *Unlocking the power of Opnet Modeler*, NewYork, USA: Cambridge University Press, 2012.

[14] T. V. Mathew, *Car Following Models*, ch. 14, pp. 1–8, Indian Institute of Technology, Bombay, 2014.

[15] OPNET, *Simulator*, Apr. 10, 2017. (`http://www.opnet.com/`)

[16] M. Raya and J. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security*, vol. 15, no. 1, pp. 39–68, 2007.

[17] M. Raya, D. Jungels, P. Papadimitratos, I. Aad, and J. Hubaux, "Certificate revocation in vehicular networks," Technical. Report, Laboratory for Computer Communications and Applications (LCA) School of Computer and Communication Sciences, Jan. 2006.

[18] SUMO, *Simulation of Urban MObility*, Apr. 10, 2017. (`http://sumo.sourceforge.net/`)

[19] A. Wasef and X. Shen, "EDR: efficient decentralized revocation protocol for vehicular ad hoc networks," *IEEE Transaction on Vehicular Technology*, vol. 58, no. 9, pp. 5214–5224, 2009.

[20] H. Wu and W. Hsieh, "RSU-based message authentication for vehicular ad-hoc networks," *Multimedia Tools Applications*, vol. 66, no. 2, pp. 215–227, 2013.

[21] C. Zhang, X. Lin, R. Lu, and P. Ho, "RAISE: an efficient RSU-aided message authentication scheme in vehicular communication networks," in *Proceedings of IEEE International Conference on Communications (ICC'08)*, pp. 1451–1457, Beijing, China, May 2008.

Biography

Safi Ibrahim. Received her BSc, MSc, in Information Technology from the faculty of Computers and Information Sciences, Cairo University, Cairo, Egypt. She is currently a Lecturer Assistant in the Department of Information Technology, Egyptian E-Learning University EELU, Cairo, Egypt. Her research interests include ad hoc networks, vehicular communication and Network Security. She has published about four publications in conference proceedings concerning these research areas. She teaches courses on Programming, Wireless Netwoks and Network Security.

Dr. Mohamed Hamdy is an associate professor in the Information Systems Department, the Faculty of Computer and information Sciences at Ain Shams University since 2016. Early 2011, he got his PhD in Mobile Ad Hoc Networks from Friedrich Schiller University Jena, Germany, then he has been back to his home Ain Shams University in Egypt and was working as an assistant professor. His research interest is in general in Wireless Networks, Mobile Data Management. He has engaged in several research projects in MANETs and Data Management.

Dr. Eman Shaaban Received her BSc, MSc, and PhD in computer engineering from Ain-Shams university, Cairo, Egypt. She is currently an associate professor in the Department of computer systems, faculty of computer and information sciences, Ain-Shams university, Cairo, Egypt. She teaches undergraduates courses on data communication, computer architectures and embedded systems, in addition to teaching graduate courses on wireless communications and sensor networks. Her research interests include ad hoc networks, wireless sensor networks, and vehicular communication. She has published over 25 technical papers in peer-reviewed journals and major conference proceeding concerning these research areas.