International Journal of Scientific & Engineering Research, Volume 5, Issue 2, February-2014
ISSN 2229-5518

An Efficient Data Replication Method for Data Access Applications in Vehicular Ad-Hoc Networks

Saranya S, II- M.Tech/CSE, PRIST University, Puducherry, India – 605007, Mis.R.Backiyalakshmi, Assistant Professor/CSE, PRIST University, Puducherry, India - 605007.

Abstract - Due to the high vehicle mobility, the topology of vehicular ad hoc networks (VANETs) dynamically changes, and disconnections may frequently occur. When two vehicles are disconnected, they are not able to access data from each other. Data replication has been widely used to reduce the effect of intermittent connectivity and improve data access performance in distributed systems. However, many nodes in VANET may only have limited storage space, and thus cannot replicate all the data such as large music files or video clips. To address this problem, we propose an efficient data replication method for data access applications in VANETs. In this method the vehicles are grouped into a platoon and they contribute part of their buffers to replicate data for others in the same platoon and share data with them. When a vehicle leaves the platoon, it prefetches interested data and transfers its buffered data to other vehicles in advance so that they can still access the data after it leaves. We implement this algorithm in NS-2 and GrooveNet Simulators. The GrooveNet Simulator is used to generate the vehicle mobility trace file, which is used in the ns-2 simulations. Extensive simulation results show that this method provides high data availability, low data access overhead, and low false alarm rate.

Key Words: ad hoc networks, Data replication, platoon, vehicular ad hoc network (VANET).

IJSER

1. INTRODUCTION

VANET is a form of Mobile ad-hoc network, to provide communications among nearby vehicles and between vehicles and nearby fixed equipment, usually described as roadside equipment.Vehicular networks represent an interesting application scenario for not only traffic safety and efficiency but more commercial applications and entertainment support as well, such as service scheduling, content sharing, peer-to-peer marketing, and urban data Collecting.

Vehicular ad-hoc networks (VANETs) have been envisioned to be useful in road safety and many commercial applications. For example, a vehicular network can be used to alert drivers to potential traffic jams, providing increased convenience and efficiency. It can also be used to propagate emergency warning to drivers behind a vehicle (or incident) to avoid multicar collisions. As more and more vehicles are equipped with communication capabilities that allow inter-vehicle communication, large-scale VANETs are expected to be available in the near future.

The proliferation of low-cost wireless connectivity, combined with the growth of distributed peer-to-peer cooperative systems, is transforming next-generation vehicular networks. Drivers and passengers inside moving vehicles will be able to obtain and share their interested data, such as MP3 music, news, and video clips.The nodes in a VANET, such as vehicles or in-vehicle mobile devices and sensors, should not be able (or willing) to replicate all data items in the network. The solutions for fast and convenient data access in VANETs. It is based on a well-known phenomenon called “vehicle platoon” in VANETs, where vehicles often travel in closely spaced groups. A report from the Department of Transportation has indicated that the platooning probability for vehicles on highway can be higher than 70%. If vehicles move as a relatively stable platoon, they can contribute part of their buffer to replicate data for other vehicles in the same platoon and share data with them. Data redundancy in the same platoon can be reduced through cooperative replication; therefore, more data can be stored in the platoon, improving the data availability and reducing the data access delay. How platoon-aware data replication can be used to improve the performance of data access in a VANET.

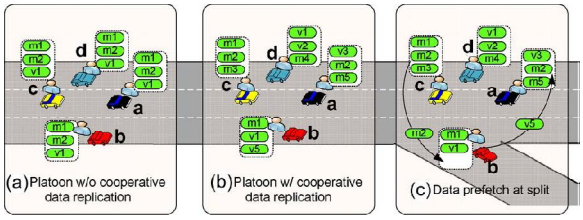

Fig. 1. Platoon-based data access in VANETs

International Journal of Scientific & Engineering Research, Volume 5, Issue 2, February-2014
ISSN 2229-5518

The different data access paradigm in VANETs where each vehicle queries useful data from nearby neighboring vehicles. To make use of the platoon mobility pattern of vehicles and cooperatively replicate data within platoon to improve the data access performance.

If vehicles move as a relatively stable platoon, they can contribute part of their buffer to replicate data for other vehicles in the same platoon and share data with them. Data redundancy in the same platoon can be reduced through cooperative replication; therefore, more data can be stored in the platoon, improving the data availability and reducing the data access delay.

If vehicles know that they have formed a stable vehicle platoon, they can cooperatively replicate data and more efficiently organize their buffer. Some vehicles may leave the platoon, and they may not be able to access the data replicated by other platoon members. To address this problem, the splitting vehicle should Prefetch its most interested data and transfer its buffered data copies to other platoon members.

2. EXISTING SYSTEM

Data replication has been widely used to reduce the effect of intermittent connectivity and improve data access performance in distributed systems. Data replication can increase data availability and reduce the query delay if there is plenty of storage space in the vehicles. Replicating the same data in all the neighboring nodes should be avoided. In vehicular ad hoc network, vehicles tend to move in an organized fashion (Platoon) whereas in MANET, nodes move randomly. Making the vehicles cooperatively replicate data and more efficiently organize their buffer.

Due to the high vehicle mobility, the topology of vehicular ad hoc networks (VANETs) dynamically changes, and disconnections may frequently occur. When two vehicles are disconnected, they are not able to access data from each other. Thus, data availability in VANETs is lower than that in conventional wired networks.All these existing researches on vehicle platoon identification rely on roadside sensors for centralized vehicle mobility observation and analysis.

Data replication can increase data availability and reduce the query delay if there is plenty of storage space in the vehicles. However, many nodes may only have limited storage space, bandwidth, and power. They may only have resource-constrained mobile phones, which have limited storage, and thus cannot replicate all the data such as large music files or video clips.

The contact time of vehicles may not always be long enough to transmit all data items. To replicate the data, nodes need to transmit it from other nodes, and obviously, there will be huge bandwidth and power cost for a large volume of data.Making the vehicles cooperatively replicate data and more efficiently organize their buffer.

The vehicle-to-vehicle approach, however, is more flexible and cost effective in VANETs, particularly in rural or highway areas, which lack roadside infrastructure support.

From the splitting vehicle point of view, it may not be able to access the most interested data placed at other platoon members after it is disconnected from the platoon. The vehicle platoon point of view, if there are some primary data copies buffered at the splitting vehicle, the splitting may also significantly affect the intraplatoon data access. Moreover, if the primary data copy is the only data copy in the platoon, other platoon members will not be able to access the data after splitting.

The non cooperative solution prefers replicating the most frequently accessed data, thus having a relatively high local hit rate, compared with the connection-based solution, in which each vehicle may buffer data for other vehicles while does not have opportunity to Prefetch its own interested data before splitting.

2.1 Drawbacks

In existing system it does not have split prediction capability and less data availability. The high mobility of vehicles and the unreliable wireless communication significantly degrade the performance of data access in vehicular ad hoc networks (VANETs).Another problem is many nodes may only have limited storage space, bandwidth, and power.

3. PROPOSED SYSTEM

The data access solution for VANET's, includes the following two components are A vehicle-platooning protocol is proposed to quickly identify the platoon and predict the split process. In this protocol, stochastic time series analysis is used to detect vehicle Platoon and mobility anomalies, and a two-step split prediction method is introduced to accelerate the detection and reduce false alarm due to road curvature.

Second, a platoon-based data management component is introduced to achieve high data availability and reduce the intra platoon data access cost. Specifically, we propose two cost-effective data replication algorithms to find the best vehicle to replicate each data item inside the platoon, and it provides data Prefetch and transfer heuristics when there is a split detected.

International Journal of Scientific & Engineering Research, Volume 5, Issue 2, February-2014
ISSN 2229-5518

Data replication has been widely used to reduce the effect of intermittent connectivity and improve data access performance in distributed systems. Data replication can increase data availability and reduce the query delay if there is plenty of storage space in the vehicles. Replicating the same data in all the neighboring nodes should be avoided. In vehicular ad hoc network, vehicles tend to move in an organized fashion (Platoon) whereas in MANET, nodes move randomly. Making the vehicles cooperatively replicate data and more efficiently organize their buffer.

Two Cost-effective data replication algorithm to find the best vehicle to replicate each data item inside the platoon. To help vehicles and roadside infrastructure easily and quickly get the data, the data may have to be carefully placed. Vehicle should be able to detect the split as soon as possible, and then they can prefetch and transfer the data in advance before the split.Data redundancy in the same platoon can be reduced through cooperative replication. Cooperative data access with the support of roadside infrastructures. to improve data availability, replicating the same data near neighboring nodes should be avoided.

To help vehicles and roadside infrastructure easily and quickly get the data, the data may have to be carefully placed. Vehicle should be able to detect the split as soon as possible, and then they can prefetch and transfer the data in advance before the split.Data redundancy in the same platoon can be reduced through cooperative replication. Cooperative data access with the support of roadside infrastructures. to improve data availability, replicating the same data near neighboring nodes should be avoided.

Adding security using PKI standard. While sharing the files securely. At the basic level, PKI (Public Key Infrastructure) can be described as a technique that enables users on a network to securely exchange data. This is achieved by the use of public key/ private key pair, that are generate authority. A PKI is an arrangement that binds public keys with users identities through a certificate authority (CA). CA uniquely identifies user identities individually. To achieve that, each user must be individually registered with a CA . After registration the CA adds this user to a list and updates its list of users identities and their assigned public keys. In addition to the registered users, CA will keep another list of the users with revoked certification.

Using this technique, each vehicle on the road will keep count of the vehicles it passes and authenticate them. Authentication will take place using an infrastructure aid that will deliver as explained above some unique valid IDs that can be understood by all vehicles on the road, and as mentioned above will preserve the privacy.

Data access by exploiting the vehicle platoon behavior, where vehicles often travel in closely spaced groups.There has been some work on group-based data access in mobile networks. A report from the server has indicated that the platooning probability for vehicles on same path can be higher than the approximation.

Advantage for PKI infrastructure is the smooth and easy logic behind the PKI infrastructure: To sign a message, the sender encrypts a message with his private key. The receiver decrypts with the public key of the sender and if the 'message' is what is expected then the receiver knows that it can only be send by the sender.

To encrypt something the sender encrypts the message with the public key of the receiver. Then only the receiver can decrypt the message using his private key. the creation of a shared for encryption and decryption of data.

The traditional shared key can be stolen by a hacker or a an intruder in the middle, and then this person will be able to decrypt the secret data using the shared key he/she could have. Using PKI prevents this, since both parties have different public keys.

The concepts of multi-platoon merge scheme are used in proposed system. First form the virtual gateway between the each nodes, here we are make the interval based updation about the platoons communications, through the virtual gateway we can get efficient transactional datas about the platoons at the same time not need to search the communication data from platoons nodes.

4.1 PROBLEM DEFINITION

All vehicles' drivers want to make sure that their identity is preserved while exchanging messages with the other entities on the road. Vanet are based on node to node communications; where nodes establish connections with other node in order to exchange information of different nature .The nodes are not connected by any sort of physical medium in Vanets; it is completely based on wireless infrastructure less environment and managing the security communication using PKI (Public key Infrastructure) standards. Investigates how to detect the platoon and the platoon partition by vehicles in a distributed manner without any centralized system support. To explore how good or how poor the model is by incorporating such approximation of vehicle interactions in terms of the independence. How the number of vehicles in the road segment varies with the data access shift between the vehicles. How the mean number vehicles in the road side within the data access varies with the phase shift between vehicles to road side infrastructures and vehicles to vehicles. How vehicular Data replication has been widely used to reduce the effect of intermittent connectivity and improve data access performance in distributed systems How the PKI (Public Key Infrastructure) can be described as a technique that enables users on a network to securely exchange data. This is achieved by the use of public key/ private key pair, that are generate authority. How the security applications on a VANET ready vehicle can't be

International Journal of Scientific & Engineering Research, Volume 5, Issue 2, February-2014
ISSN 2229-5518

achieved without a regular maintenance of the equipment that VANET provides. Actually, a regular check on the software and hardware will allow the authorities to ensure that vehicle's software hasn't been changed or modified for the sake of impairing the VANET network on the road.

4.2 SYSTEM ANALYSIS

Due to the high vehicle mobility, the topology of vehicular ad hoc networks (VANETs) dynamically changes, and disconnections may frequently occur. When two vehicles are disconnected, they are not able to access data from each other. Data replication has been widely used to reduce the effect of intermittent connectivity and improve data access performance in distributed systems. When a vehicle leaves the platoon, it prefetches interested data and transfers its buffered data to other vehicles in advance so that they can still access the data after it leaves. If vehicles move as a relatively stable platoon, they can contribute part of their buffer to replicate data for other vehicles in the same platoon and share data with them. Data redundancy in the same platoon can be reduced through cooperative replication; therefore, more data can be stored in the platoon, improving the data availability and reducing the data access delay. Although vehicle platoons have not been used as a design parameter to facilitate data access in VANETs, their effects on traffic control and design of traffic signal timing have been studied for a long time. A car-following model was developed to describe vehicle platoon movements. Further developed algorithms to identify vehicle platoons from road traffic and optimized the setting of transferring the data. All these existing researches on vehicle platoon identification rely on roadside sensors for centralized vehicle mobility observation and analysis. Investigates how to detect the platoon and the platoon partition by vehicles in a distributed manner without any centralized system support

Vehicle Selection

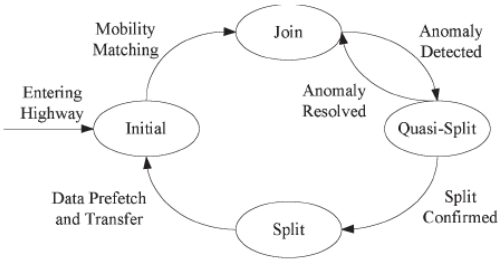

Fig. 2. State transition diagram of vehicles in V-PADA

The most intuitive approach in detecting mobility anomaly is only based on the distance between the monitoring vehicle and its reference vehicle. A mobility anomaly is detected when the distance becomes larger than a predefined threshold. However, it is difficult to find the appropriate threshold. If the threshold is large while the monitoring vehicle and the reference vehicle are close to each other, the anomaly may not be detected, even after a relative large position change the relative position change between the monitoring vehicle and its reference vehicle to detect mobility anomaly.

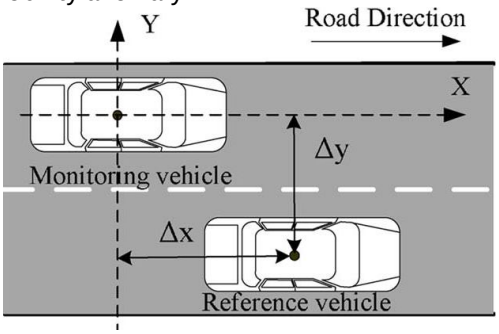

Fig. 3. Platoon-based mobility model.

Still use the Cartesian coordination system to determine the relative position of the reference vehicle in terms of Δx and Δy and use time series analysis on the relative position change to detect mobility anomaly given the standard position deviation and the detection confidence interval, the detection boundary. The relative motion between the two vehicles and thus can be used to quickly detect any abnormal position change. Securing VANET application is very crucial to the implementation for this technology. To make sure that the car is broadcasting a message is not a selfish or malicious vehicle. To face this problem, there is a need of a vehicle authentication mechanism. Vehicle authentication is though necessary to ensure the integrity and reliability of the messages exchanged in the network.

At the basic level, PKI (Public Key Infrastructure) can be described as a technique that enables users on a network to securely exchange data. This is achieved by the use of public key/ private key pair, that are generate authority. A PKI is an arrangement that binds public keys with users identities through a certificate authority (CA). CA uniquely identifies user identities individually. To achieve that, each user must be individually registered with a CA. After registration the CA adds this user to a list and updates its list of user's identities and their assigned registered users.

Security applications on a VANET ready vehicle can't be achieved without a regular maintenance of the equipment that VANET provides. Actually, a regular check on the software and hardware will allow the authorities to ensure that vehicle's software hasn't been changed or modified for the sake of impairing the VANET network on the road.

Inspection takes place in most of the countries worldwide once a year. An idea of inspecting VANET

International Journal of Scientific & Engineering Research, Volume 5, Issue 2, February-2014
ISSN 2229-5518

equipment more frequently (once in six months) would be very helpful in preventing hackers from modifying the purpose of the revocation list certificate. That is, download the latest updated list of vehicles whose certifications have been revoked for breach of VANET security regulations. Most of the existing schemes are fully depending on the individual platoons.

. Implement the multi platoons communication scheme, to form the virtual gateway between the each vehicles, here make the interval based updation about the platoons communications, through the virtual gateway can get efficient transactional data's about the platoons at the same time not need to search the communication data from the platoons, so make a efficient transaction in vehicle

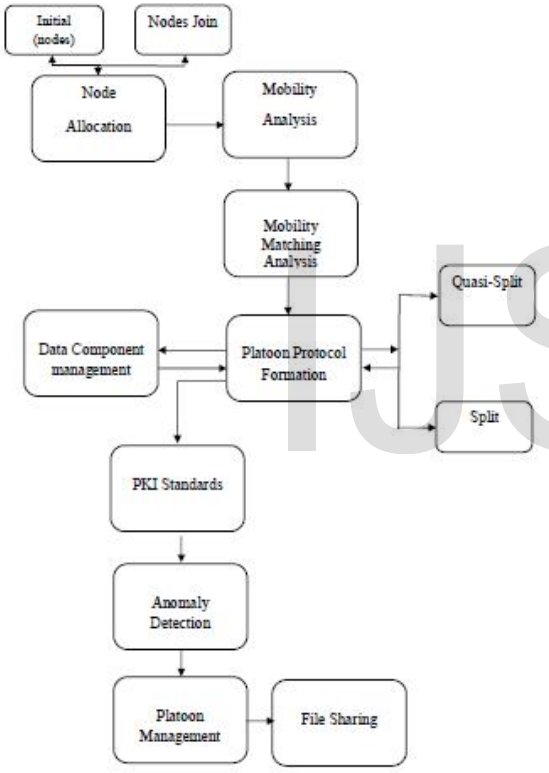

Fig. 4. Dataflow Diagram

1. Mobility matching
2. Data component management
3. Anomaly detection
4. Platoon Initialization
5. Platoon management and result analysis
6. Data access with security.
7. Multi-platoon merge scheme
8. Performance evaluation.

4.2.1 Mobility matching

In VANETs, vehicles usually move as a platoon. Although there have been a few group mobility models such as the reference point group mobility (RPGM). We assume that each vehicle platoon has a group motion vector (GM) that defines the movement of the entire platoon. The group motion vector follows the road layouts.

All vehicles in the same Platoon share the same group motion vector and have different random motion vectors (RM) due to their mobility deviation. The mobility matching identifies and matching the details regarding the vehicle and platoon. This helps to communicate and share their data's with them self.

4.2.2 Data component management

The data component management manages all the available data, data splitting process to achieve high data availability and reduce the intra platoon data access cost. The splitting vehicle should Prefetch its most interested data and transfer its buffered primary data copies to other platoon members.

If a vehicle moves on a straight road, its moving direction is usually stable; otherwise, if it is passing a curve road, its moving direction may continuously change. they can contribute part of their buffer to replicate data for other vehicles in the same platoon and share data with them. Data redundancy in the same platoon can be reduced through cooperative replication; therefore, more data can be stored in the platoon, improving the data availability and reducing the data access delay.

The heuristics for the vehicles to prefetch and transfer data before vehicle splits so that vehicles can still access their interested data after split. The splitting vehicle can easily locate the nearest nodes that have the data and Prefetch it. These all process can be done with the help of data component management module.

4.2.3 Anomaly detection

While the transmission the data can be by the anonym users, this may affect the data. For privacy and security the proposed model creates an additional environment known as anomaly detection. For secured transmission PKI Standards. All these existing researches on vehicle platoon identification rely on roadside sensors for centralized vehicle mobility observation and analysis. However, investigates how to detect the platoon and the platoon partition by vehicles in a distributed manner without any centralized system support.

The mobility anomaly comes from the acceleration or deceleration of the splitting vehicle. Since vehicles move on the same straight road and in the same direction, this split can be easily confirmed in the first step by comparing their moving directions after the mobility anomaly is

International Journal of Scientific & Engineering Research, Volume 5, Issue 2, February-2014
ISSN 2229-5518

detected. If both the monitoring vehicle and its reference vehicle are in the same direction, the reference vehicle still moves on the highway, but the monitoring vehicle switches to a curving ramp.

Because the moving direction of the monitoring vehicle keeps changing but the moving direction of the reference vehicle is stable, they are moving on different roads, and the split can be confirmed. if the reference vehicle is far from the monitoring vehicle, any slight direction change of the monitoring vehicle may result in a large relative position deviation from the reference vehicle, which may result in prediction errors.

4.2.4 Platoon Initialization

The platooning creation groups all the vehicles which are close together. Vehicles often travel in closely spaced groups. Vehicle platoons have been used as a design parameter to facilitate data access in VANET

Data access by exploiting the vehicle platoon behavior, where vehicles often travel in closely spaced groups.There has been some work on group-based data access in mobile networks. A report from the server has indicated that the platooning probability for vehicles on same path can be higher than the approximate result.

Creating a special protocol which analysis and maintain all the relaxant details through four states which are initial, join, quasi-split and split. Groups are organized with explicit join/leave messages and that the partition is detected only after two nodes move out of their communication range.

4.2.5. Platoon management and result analysis

Creating the platoon protocol and maintaining them will be considered in this module. The monitoring vehicle and its reference vehicle periodically exchange their movement profile through beacon messages by which the monitoring vehicle can get a series of relative coordinates of the reference. The management module concentrates the following process. Platoon identification, diagnostics checking and split prediction.

4.2.6. Data access with security

PKI (Public Key Infrastructure) standard is used for security propose. PKI (Public Key Infrastructure) can be described as a technique that enables users on a network to securely exchange data. This is achieved by the use of public key/ private key pair, that are generate authority. A PKI is an arrangement that binds public keys with users identities through a certificate authority (CA).CA uniquely identifies user identities individually.

To achieve that, each user must be individually registered with a CA. After registration the CA adds this user to a list and updates its list of user's identities and their assigned registered users, CA will keep another list of the users with revoked certification. Meaning, the ones who were registered before, and for a reason, they should not trusted anymore.

Security applications on a VANET ready vehicle can't be achieved without a regular maintenance of the equipment that VANET provides. Actually, a regular check on the software and hardware will allow the authorities (DMV in the case of America) to ensure that vehicle's software hasn't been changed or modified for the sake of impairing the VANET network on the road. As we know inspection takes place in most of the countries worldwide once a year. An idea of inspecting VANET equipment more frequently (once in six months) would be very helpful in preventing hackers from modifying the purpose of the revocation list certificate. That is, download the latest updated list of vehicles whose certifications have been revoked for breach of VANET security regulations.

4.2.7. Multi-platoon merge scheme

Most of the existing schemes are fully depending on the individual platoons, to implement the multi platoons communication scheme, in this module we are going to form the virtual gateway between the each vehicles, here we are make the interval based updation about the platoons communications, through the virtual gateway Using virtual gateway(VC) get the efficient transactional data's about the platoons at the same time not need to search the communication data from the platoons, so have to make a efficient transaction using multi-platoon merge in vehicles between the vehicles VC is advanced software that distributes multi platoon throughout the locations.

4.2.8. Performance evaluation

Performance Evaluation is a constructive process to acknowledge the performance of a non-probationary .A comparison of one existing performance to a group of comparable proposed output. Based on conventional wisdom one would argue against implementing the NS2 system for performance reasons.

5. Results and Discussion

Comparison of existing system and the proposed system through packets and time The above chart describes DCF consists of minimum amount of transaction losses occur than the DSRC The data losses can be find by adding data to the original information comparing to DSRC the DCF sends more packets in the area. In proposed system adding a security propose using PKI(Public Key Infrastructure).Encryption and decryption based PKI algorithm has gathering more information.

IJSER

International Journal of Scientific & Engineering Research, Volume 5, Issue 2, February-2014
ISSN 2229-5518

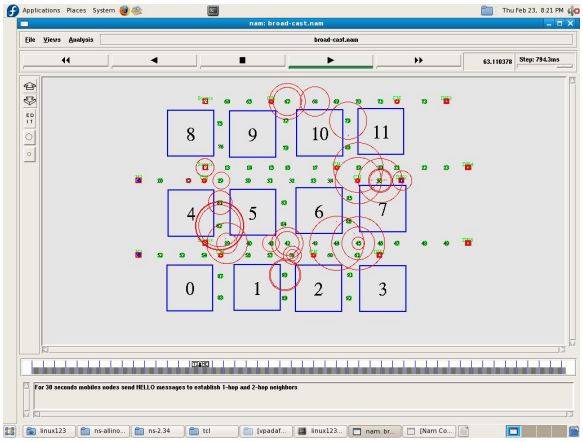

Fig.5. Drop the Unwanted Data

The network was created and waiting for initializing the list and then sorted all list. Calculating the distance of each list for allocating nodes. After Calculating list the nodes are formed they particular area and then searching soure and destination of all nodes. Source and destination are allocated.Source sending the data to particular Destination in platoon . The join process can be detected with techniques.

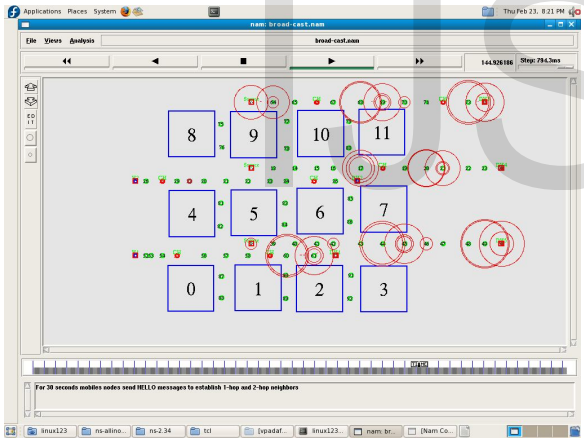

Fig. 5. Data Transfered

After one node is detected to join the platoon, it enters the Join state and sends out a platoon-join message to all platoon members to announce that a new member has joined the platoon. This will not affect the performance of the platooning protocol too much because both join and split actions can always be detected by neighboring vehicles through its beacons.

Each vehicle can store up to 100-MB data in its local buffer, but initially, it randomly picks data as its local data until the local buffer is full. All nodes in the platoon remove the old data items from the buffer, and thus, the newly released memory can be used by other applications.

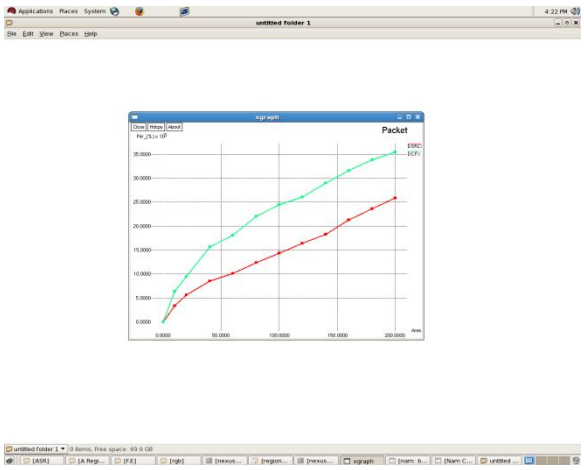

Fig.6 Comparison between DSRC and DCF..

The nodes are transfered the data to the particular Destination. Securing VANET application is very crucial to the implementation for this technology. Need to make sure that the car is broadcasting a message is not a selfish or malicious vehicle. To face this problem, there is a need of a vehicle authentication mechanism. Vehicle authentication is though necessary to ensure the integrity and reliability of the messages exchanged in the network.

Implementation of VANETs on the road is availability. Meaning that all the system (Software and hardware) should be available to send receive message all the time, for communication. if a vehicle have to now some climate condition and news, it should send a request messages to all the neighbouring vehicles in real time or near real time so that VANET is the range of coverage of the broadcasting a message.

A message can be lost in the case of too few cars on the road, because there will be no vehicle to work as relay to that specific message and can be lost. Securing VANETs communication possible is the fact that most of the drivers of the road are considered, or at least, most likely to be honest. Meaning that most of the users of the technology will attempt to modify or change the software or the configuration they are given.

Therefore, most vehicles are most likely considered to act as it was intended at the conception level of the developers. Therefore, it is considered that most of the communication flow is not erroneous or injected by pranksters or hackers. However, this doesn't deny the fact of the possibility of having an unwanted or erroneous message flowing in the network using PKI Standards.

6. CONCLUSION

V-PADA, is a novel vehicle-platoon-aware data access solution for VANETs. V-PADA makes use of the "vehicle platoon" mobility pattern to collaboratively replicate data and optimize data access among vehicles. V-PADA consists

International Journal of Scientific & Engineering Research, Volume 5, Issue 2, February-2014
ISSN 2229-5518

of two components. First, a vehicle-platooning protocol is designed to identify the platoon and quickly predict vehicle split. Second, a data management component is introduced to achieve high data availability and reduce the intraplatoon data access cost. To the best of our knowledge, this is the first work to exploit vehicle-platoon behavior for data access, considering various vehicle splits. The proposed solution in this paper is not limited to VANETs and can be extended to other mobile ad hoc networks.

In the future, solutions for mobility anomaly detection and cooperative data access with the support of roadside infrastructures and more complicated security algorithm.

REFERENCES

[1]. D. Gerlough and. Huber, "Traffic flow theory—A monograph," Transp. Res. Board, Washington, DC, Special Rep. 165, 1975.

[2]. R. Hall and C. Chin, "Vehicle sorting for platoon formation: Impacts of highway entry and throughput," California PATH Program, ITS, Univ California, Berkeley, Richmond, CA, California PATH Res. Rep. UCBITS-PRR-2002-7, 2002.

[3]. Y. Huang, P.Sistla, and O.Wolfson, "Data replication for mobile computers," in *Proc. ACM SIGMOD*, 1994, pp. 13–24.

[4]. U. Lee, E. Magistretti, M. Gerla, P. Bellavista, and A. Corradi, "Dissemination and harvesting of urban data using vehicular sensing platforms," *IEEE Trans. Veh. Technol.*, vol. 58, no. 2, pp. 882–901.

[5]. J. Rybicki, B. Scheuermann, M. Koegel, and M. Mauve, "Peertis: A peer-to-peer traffic information system," in *Proc. ACM VANET*, 2009,pp. 23–32.

[6]. Y. Zhang, J. Zhao, and G. Cao, "Roadcast: A popularity aware content sharing scheme in VANETs," in *Proc. IEEE ICDCS*, 2009, pp. 223–230.

[7]. Y. Zhang, J. Zhao, and G. Cao, "On scheduling vehicle-roadside data access," in *Proc. ACM VANET*, 2007, pp. 9–18.

[8]. Y. Zhang, J. Zhao, and G. Cao, "Service scheduling of vehicle-roadside data access," *Mobile Netw. Appl.*, vol. 15, no. 1, pp. 83–96, Feb. 2010.

[9]. J. Zhao, Y. Zhang, and G. Cao, "Data pouring and buffering on the road: a new data dissemination paradigm for vehicular ad hoc network

[10]. Yang Zhang, *Guohong Cao,* "V-PADA: Vehicle-Platoon-Aware Data Access in VANETs" *IEEE Transactions Vehicular Technology, vol. 60, no. 5, pp. 2326–2339,*June 2011.

IJSER