AN ECONOMICAL, DEPLOYABLE AND SECURE VEHICULAR AD HOC NETWORK

Baber Aslam, Ping Wang and Cliff Zou
School of Electrical Engineering and Computer Science
University of Central Florida
Orlando, FL 32816

ABSTRACT

With the significant development of wireless technologies, vehicular ad-hoc network (VANET) has gradually become the killing application for automobile industry. Many VANET systems have been developed in recent years. However, the majority of them have the assumption that all or most vehicles have wireless communication devices installed along with an elaborate road side infrastructure. This assumption is not true for the critical and long transition period when only a small portion of vehicles will be equipped with wireless communication devices (we refer them as smart vehicles) and limited roadside infrastructure will exist.

In this paper, we present an economical, scalable and deployable VANET system design that could facilitate the gradual deployment of wireless communication among vehicles. Economical RoadSide Service Units (RSSU) that do not need expensive Internet access (especially in rural areas) can be incrementally deployed along critical road sections. They behave as traffic information storage and relay points to serve any passing by smart vehicles, while smart vehicles report/receive traffic information to/from RSSUs and relay information between RSSUs. In addition, RSSUs provide strong but economical information assurance to VANET similar to the public-key base Internet web service—RSSUs behave like web servers with certificates and vehicles behave like client computers. In this way, the mature Internet-like public-key infrastructure can be directly deployed in VANET without requiring digital certificate for every smart vehicle, which is complicated to manage and very expensive considering the huge vehicular population. We show that we can achieve connectivity with a high degree of confidence with a small number of smart vehicles and few RSSUs.

1. INTRODUCTION

Wireless networks can have an infrastructure or an infrastructure-less architecture. The infrastructure-less architecture is also known as ad hoc network or mobile ad hoc network (MANET) since the devices (nodes) are usually mobile. Vehicles when equipped with computing devices also become mobile nodes and the network becomes vehicular ad hoc network (VANET). Applications of VANET include delivery of general information, delivery of entertainment content, business applications, public safety warnings, communication, etc. In this paper our focus is on applications that do not require sustained and high data rates, since it will not be possible to provide such a QoS during initial stages of VANET deployment.

VANETs have hybrid architecture containing both the infrastructure and the ad hoc architectures. The Vehicle to Vehicle (V2V) communication is ad hoc and Vehicle to Infrastructure (V2I) communication is through access points (roadside units). These roadside units (base stations) are then connected to the Internet and provide necessary services to vehicles. The provision of these services largely depends on connectivity of these roadside units to each other and to the Internet. The success of VANET depends on existence of roadside infrastructure and sufficient number of vehicles equipped with wireless communication devices (we refer them as "smart vehicles"). Most VANET researches are based on either or both of these requirements.

However, both of these requirements will not be realistic during initial years of VANET deployment. It will not be economically feasible to initially install a large number of fully networked roadside units to cover a region. Further, during the long transition period, there will not be sufficient number of smart vehicles to enable V2V communication, which is an essential element in all VANET applications. The roadside infrastructure will remain uneconomical in rural areas even after initial deployment since there will not be sufficient number of smart vehicles for years to come. V2V communication between vehicles traveling in opposite direction is very important for effective routing of messages. This may not be possible at some places due to road layout or because of uneven distribution of traffic (normally related to working hours).

Although there are plenty of VANET researches, but the solutions to the issues which will be existing during long transition period in VANET deployment, discussed above, are largely ignored. In this paper, we present an economical, scalable and deployable VANET system design to solve these challenges. From now on we will mostly refer "smart vehicle(s)" as "vehicle(s)" unless there is a need to explicitly mention smart vehicle(s).

The main contributions of this paper are twofold. First, we present a VANET system design that is economical, realistic, incremental and deployable during the initial long transition period when smart vehicles have low penetration rate. The proposed solution also ensures V2V communication in above mentioned situations which are necessary for the success of VANETs. Core component in our solution, the RoadSide Service Units (RSSU), can be standalone with minimum intelligence in its basic form. Our proposed solution does not require RSSUs to be interconnected or connected to the Internet. We present a basic protocol that makes the communication between roadside service units possible via vehicles. The simulation results indicate considerable performance gains just by using standalone RSSUs.

Second, this system design enables an economical and strong information assurance in VANET ─ RSSUs behave like web servers with certificates and vehicles behave like client computers. In this way, the mature Internet-like public-key infrastructure can be directly deployed in VANET without the complicated and expensive requirement of digital certificate in every vehicle.

The paper is organized as follows. In section 2 we present related work. Section 3 gives detailed description of our proposed solution and Section 4 highlights its security features. Section 5 presents the simulation details. And finally, Section 6 concludes this paper.

2. RELATED WORK

Most of the existing research in VANET assumes that sufficient number of vehicles will be present to relay the messages [1-3]. Though some of the researches address the routing in disconnected networks [4-6] but during the initial deployment there will not be sufficient number of vehicles to even form small clusters for these protocols to work. Further lack of roadside infrastructure will also make hybrid protocols [7] difficult to work.

In V2V communication protocols [4, 8, 9] based on the delay tolerant network (DTN) techniques [10], the mobile nodes temporarily store a message if no route is available and later opportunistically forward the message. These protocols may solve the disconnected network problem due to uneven distribution of traffic but are not an effective solution to low penetration issues.

Infostations architecture uses high speed and generally dispersed access points which afford transfer of high volume of data at cost of connectivity [11, 12]. This architecture cannot solve the low penetration problem since the infostations will generally be widely dispersed and also these must be fully networked with backbone which will be quite expensive to install and maintain.

A class of protocols uses store and forward approach for V2V communications [1, 13]. MDDV [1] uses predictability of vehicle movement to route the messages. In VADD [13], a vehicle carries a message until it finds another vehicle in communication range, it then forwards the message. Both the protocols [1, 13] assume vehicles to be equipped with GPS and digital maps, and are used to transfer messages between vehicles in multi hops. Further, VADD bases its message forwarding decision on detailed traffic statistics (vehicle density, vehicle speeds, etc).

Lochert et al. [14] show that the networked, connected via backbone, stationary supporting units (SSUs) improve the performance dramatically as opposed to the standalone SSUs. V2V communication plays an important part in their scenario. Whereas in our case V2V communication is not possible since we have considered very limited penetration rate and our results show that standalone RSSUs do increase the performance.

Our work comes closer to protocols that use vehicles to transfer messages between roadside units [15-17]. M.C. Chuah et al. [15] present a protocol using multi-hop V2V communication between road side units. They present a detailed mechanism for forwarding of messages at each hop. B. Pretit et al. [16] present a set of protocols for data relaying between roadside units using vehicles. They give different options for transfer of data between a source/sink and a vehicle, but do not give the routing details among the road side units. Y. Ding et al. [17] present a static node assisted adaptive routing protocol. It is a multi-hop protocol using static nodes at the intersections to store and forward the messages.

Our research work differs from above mentioned protocols in many ways. We do not assume vehicles to be equipped with GPS and digital map, or have road statistical data which is more realistic especially in initial transition period. Our protocol does not involve V2V communication, thus it works well when vehicles are sparsely distributed on roads. We do not assume roadside units to be connected to infrastructure (i.e., fully networked or connected to the backbone), which makes our solution economical and practical during transition stage. We present an integrated solution involving vehicles and roadside units with varying degree of capabilities. Besides being economical, the solution is also scalable and can easily be upgraded without any major modifications in protocol.

3. PROPOSED SOLUTION

The common characteristic of all VANET applications is either collection or dissemination of information from/to vehicles. V2V and V2I communications compliment each

other in achieving this flow of information. During initial stages both V2I (also infrastructure to infrastructure - I2I) and V2V communications will not be very effective. We suggest improving V2I communication by using roadside service units (RSSU), which in turn will complement the lack of V2V communication. The motivation of our solution is to make roadside units light weight, simple/easy to install and economical. Our proposed RSSU does not need to be connected with other RSSUs or the Internet to provide its services. It may or may not be locally connected. Standalone or locally networked RSSUs besides being economical are also very easy to install and maintain as compared to fully networked roadside units. Further, for V2V communication RSSUs will increase the chances of information transfer by relaying messages. Standalone or locally networked RSSUs raise the issue of I2I communication, we address this by using unicast routing between RSSUs using either local network or vehicles as medium. A possible architecture is shown in figure 1.
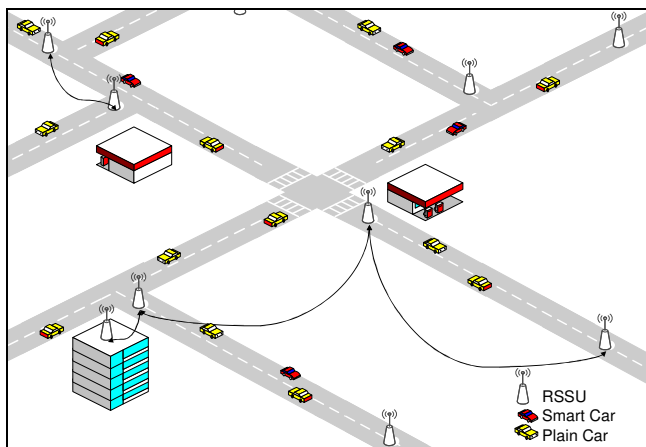

Figure 1: The proposed architecture consists of RSSUs deployed along the roads. RSSUs can be standalone, locally connected to adjacent RSSU (two on the up-left corner), or connected to backbone infrastructure (three on the bottom of the figure).

Store and forward is the basic capability and enables an RSSU to transfer messages between spatially and temporally displaced vehicles. Each RSSU will have a distinct identification and an associated digital signature certificate. Each RSSU will be aware of local map, its own location and locations of other RSSUs in the area. This information can be added at the time of installation of the RSSUs. When a RSSU is added to the network its data can be communicated to other RSSUs via proposed communication methods. This data can also be updated along with certificate renewal. A new RSSU may also advertise itself when added to the network.

3.1 Vehicle to RSSU Communication

Each RSSU will advertise its existence and services offered by periodic beacons. The beacon will include RSSU ID, RSSU certificate, location of RSSU, current time, location of adjacent RSSUs, services offered and critical safety information. Critical safety information is included in beacon to reduce the information relaying time. The beacon message will be signed by its issuing RSSU.

3.2 RSSU to RSSU Communication

Routing will be table driven. Data transmission will be limited to adjacent nodes only. End to end communication will be restricted to special cases only such as passing of malicious vehicle information. This can be achieved by relaying information to a unit which is known to be connected to backbone.

If RSSUs are not locally connected then the RSSUs relay messages through vehicles. The addressing information will include the destination RSSU ID and its location. If the message is end-to-end (i.e. not between adjacent RSSUs) then routing information will also be included. Routing information will include locations and IDs of intermediate RSSUs. The message will be signed by originator and confidential information may also be encrypted. The originator's certificate will be appended with the message.

The basic idea of *opportunistic routing* is used [24]. The RSSU controls/selects number of vehicles/nodes relaying the message. RSSU broadcasts the message to every vehicle in range, after receiving the message; each vehicle waits for a random amount of time and then acknowledges the message. On hearing the acknowledgement all other nodes discard the message, therefore only one node which acknowledges first is selected as message relay. One possible problem can be when the relaying vehicle diverts from the route before delivering the message. In this case probability of success can be increased by letting more than one vehicle to acknowledge and carry the message. (Mathematical analysis of number of nodes required to deliver the message with some probability of confidence is discussed later). Another possible issue is hidden node problem (due to small number of vehicles during initial stages of VANET deployment the chances of having a hidden node will also be less); in this case more than one vehicle will acknowledge and carry the message. This will provide redundancy to the protocol. This will however require duplicate suppression at the destination.

The acknowledgements will be restricted to only one hop. End to end acknowledgement may be included as an optional service. The calculation of acknowledgement timeouts is discussed later.

3.2.1 Operation

RSSU broadcasts the message. Each receiving vehicle compares the destination location with its direction of travel and discards the message if it's for a RSSU in opposite direction otherwise it acknowledges the message as discussed before. If a vehicle is not equipped with GPS then it can use the locations of RSSU it has just passed and current RSSU to determine its direction of travel. Alternatively, RSSU can include the ID of RSSU which a vehicle must have passed if it's along the desired direction. The carrying vehicle relays the message to each intermediate node that is listed in the routing information of the message and the destination node.

A RSSU on receiving the message, checks message integrity and then sends acknowledgement to immediate upstream RSSU according to the routing information in the message. If the message has already been received then it is discarded and no further action is required. This ensures duplicate elimination on per hop basis.

If the RSSU is not the destination then it waits for the acknowledgement from its downstream RSSU since the same vehicle may also deliver the message to the next RSSU. But if the downstream traffic density is low then the RSSU may elect to take opportunity of available traffic even before the end of timer. (To simplify the logic the RSSU may rebroadcast the message before starting the wait timer).

If no acknowledgement is received then the RSSU broadcasts the message and resets its timer. This process is then repeated for a fixed number of times. This guards against network overloading. There may be the cases when message has been received but acknowledgement cannot be sent due to lack of upstream traffic. The flow of message and its acknowledgements are shown in figure 2.

3.2.2 Acknowledgement Wait Time

Each RSSU waits for acknowledgement before retrying. The wait time (W_t) depends on the distance to next node, average speed of vehicles and traffic conditions. It is directly related to distance (L) and inversely related to vehicle speed (s) and traffic density (d) (upstream).

$$W_t = 2\frac{L}{s} + \frac{1}{ds} + \varepsilon \tag{1}$$

Where ε is a constant which caters for processing done at node before sending the acknowledgement.

The final wait time will be estimated using equation (3). Here α is the smoothing factor, M is acknowledge arrival time and D is smoothed deviation (from TCP RTT model [18])

$$D = \alpha D + (1-\alpha)|W_t - M| \tag{2}$$
$$TimeOut = W_t + 4 \times D \tag{3}$$

3.2.3 Number of Relay Vehicles

Suppose between two RSSUs, there are one or several road diversions. Among the traffic flow entering from the source RSSU, only p fraction of flow goes to the destination RSSU. N represents the number of vehicles
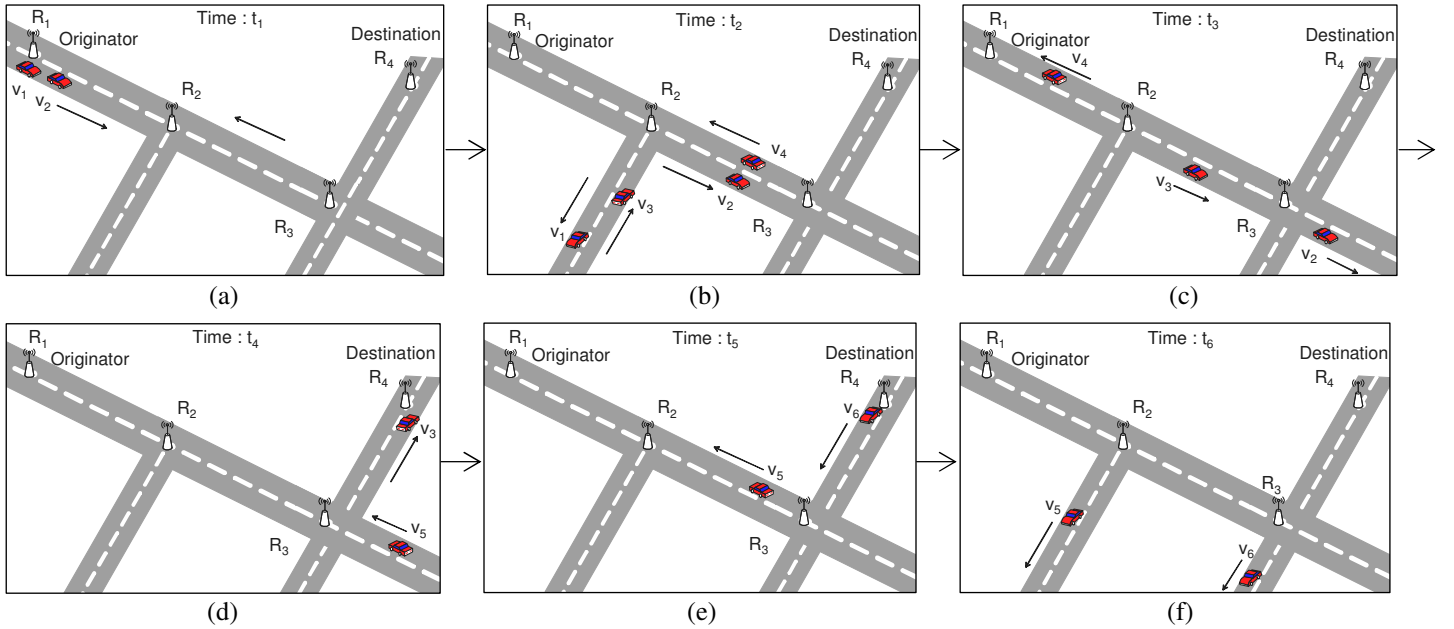

Figure 2: Flow of Message from RSSU₁ to RSSU₄ via RSSU₂ and RSSU₃. (a) V₁ and V₂ receive the message from RSSU₁. (b) V₁ and V₂ deliver the message to RSSU₂, V₁ diverts to its right at road junction, V₃ and V₄ approach RSSU₂. (c) V₂ delivers the message to RSSU₃, V₃ receives the message from RSSU₂, V₄ carries the acknowledgement message from RSSU₂ for RSSU₁. (d) V₃ delivers the message to RSSU₄, V₅ approaches RSSU₃. (e) V₆ receives the acknowledgement message from RSSU₄ for RSSU₃; V₅ carries the acknowledgement message from RSSU₃ for RSSU₂. (f) The acknowledgement messages delivered by V₆ and V₅ to RSSU₃ and RSSU₂ respectively.

passing the source RSSU, the random variable *X* represents the number of vehicles passing the destination RSSU. Let's find out how many vehicles (*N*) should the source RSSU ask to carry message, in order to let the destination RSSU to have at least *k* vehicles passing through it, with a confidence of probability *Pc* (such as 95%)?

Because each vehicle has an independent probability *p* to go to the destination RSSU, the random variable *X* follows *Binomial distribution* [19]. If we denote $f(n;N,p)$ as the probability of exactly *n* vehicles going through the destination, then according to Binomial distribution, we can derive:

$$f(n;N,p) = \binom{N}{n} p^n (1-p)^{N-n} \qquad (4)$$

The question we asked above means that the probability of having less than *k* vehicles passing through the destination RSSU must be no more than *1-P_c*. Thus the following inequality formula must be satisfied:

$$f(0;N,p) + f(1;N,p) + ... + f(k-1;N,p) \le 1 - P_c \qquad (5)$$

For *k>1* (which will be case if we want more than one vehicle to deliver the message for redundancy or security purposes) formula (5) does not have a closed-form solution. To derive the value of *N*, we can test *N*=1, *N*=2, *N*=3,..., until we find the smallest value of *N* satisfying the formula.

When *k=1*, the above formula means that the value of *N* must satisfy:

$$(1-p)^N \le 1 - P_c \qquad (6)$$

or

$$N \ge \frac{\log(1-P_c)}{\log(1-p)} \qquad (7)$$

Formula (7) gives the value of *N* for one vehicle passing the destination. For example, if *p* = 0.5 and *Pc* = 0.95 we get *N* =5 which means that in order to have 95% confidence that a message sent by the source reaches the destination, we need to relay the message through at least 5 vehicles.

4. SECURITY SUPPORT

The proposed solution does not require each vehicle to have a certificate, as opposed to previous vehicular public key infrastructures where every vehicle is assumed to have a certificate [20, 21]. In addition to being expensive and difficult for average user, the existing schemes also pose a considerable difficulty in certificate issuance, renewal and revocation. Instead, we use well established Internet client-server security model, where only servers have certificates, such as the Transport Layer Security (TLS) Protocol [22]. In our design only RSSUs will have certificates.

Such security design has tremendous advantages. First, we can directly use the mature and secure Internet public-key based protocols in VANETs. Second, because RSSUs are static and used only mainly for local areas, certificates for RSSUs can be issued very flexibly at either city level, state level or national level (certificates for vehicles, on the other hand, have to be national level since vehicles can appear in any place in a country). This makes certificate management scalable and economical. For example, certificates can be controlled by the department of transportation in a town or city. The renewal of certificates may be accomplished via a security vehicle driving along the road and issuing renewal certificate to each RSSU passing by (Similar to "Mobile Meter Reading Systems" [23]). In later stages of VANET deployment, vehicles may also be issued with certificates, thus improving on security and services.

RSSUs can also provide security services such as Data Verification and Secure Positioning. An RSSU can provide a passing-by vehicle a signed time-location stamp, based on the vehicle's identification. This vehicle can later use this stamp as proof of its presence at the location and time certified by the issuing RSSU. This service will also aid in the data verification processes in VANETs.

5. SIMULATION

Simulations were carried out to check the effectiveness of proposed solution. The simulator designed does not incorporate the details of different protocol layers. The implementation of Physical and MAC layers have been omitted. All nodes have same transmission and reception ranges. Successful transfer of a message between the source and the destination nodes is assumed if both the nodes are within communication range of each other.

5.1 Simulation Scenario I

This set of simulations were carried out to find the minimum number of vehicles required to successfully transfer a message from the source RSSU to the destination RSSU with a given probability of confidence. A region of 25000m X 6250m was simulated. When a vehicle traveling towards the destination RSSU passes by the source RSSU, the source RSSU transmits the message to the vehicle. The message is then carried by vehicle for possible delivery to the destination RSSU. On each junction of roads, the vehicle decides to either maintain its direction of travel or divert according to a defined probability. If the vehicle diverts and fails to deliver the message to the destination RSSU, then the source RSSU retransmits the message. This procedure is repeated until

the message is successfully received by the destination RSSU. In this way, the source RSSU sends 1000 messages and the number of retransmissions for each message is recorded. The simulation was repeated 100,000 times and average number of messages received successfully after a particular number of retransmissions was recorded. The probability *(p)* that a vehicle passing the source RSSU will also pass the destination RSSU was varied from 0.1 to 1.0. Results are shown in figure 3; it can be seen that the analytical and experimental results are identical.

5.2 Simulation Scenario II

During the initial stages of VANET deployment, V2V communication will not be very effective and also due to limited number of road infrastructure the V2I communication will also be very limited. We have taken two cases and compared the number of vehicles required and time required to transfer a message from a source of information (which can be scene of incident, or a RSSU) to a destination (which can be an emergency response vehicle or a RSSU) in these cases. In first case, we have a limited number of roadside infrastructure and messages are transferred between the source and the destination via vehicles only. In the second case we have intermediate standalone roadside units between the source and the destination, which help in relaying the message. In this case it is assumed that the source is also a standalone RSSUs. This is a reasonable assumption since any vehicle can deliver the incident information to this RSSU. Simulations helped us to ascertain the effectiveness of relaying the messages using vehicles, both with and without intermediate standalone-RSSUs.

A region of 25000m X 6250m with road network as shown in figure 2 was simulated. The number of smart vehicles on the simulation field (a total road length of 35000m), at any one time, was kept to 5. This small number of vehicles was used to check the effectiveness of solution during initial deployment stages of VANET. V2V communication is also ignored due to this small number of

smart vehicles. At each junction the vehicle can divert from its current direction of travel with a probability of diversion *Pd*. In the first case, each vehicle passing the source of information carries the information until it is delivered to the destination. In the second case the source RSSU retransmits the message until it is received by the destination. A vehicle carrying a message relays the message to any intermediate RSSU which it encounters. The number of retries (vehicles used to carry the information from the source) and the total time taken for the information to reach the destination are recorded for each such message. A total of 1000 messages were transmitted. The results are shown in figure 4. Figure 4(b) shows that for Two RSSUs (without intermediate RSSUs) the number of vehicles is minimum for *Pd=0.5* and increases for *Pd ≠ 0.5*. This is due to the road layout since at first road junction a low *Pd* is helpful but at second road junction a high *Pd* is more advantageous. The number of vehicles for Multiple RSSUs almost remains constant, this happen because now the vehicles traveling on other roads also play part in successful delivery of message. Same pattern of results is followed in transmission delay of messages as shown in figure 4(c). The results indicate a high performance gain when multiple (standalone intermediate) RSSUs are used. This is true for both the message transmission delays and the number of relay vehicles used.

6. CONCLUSION

There are numerous applications of VANETs but most of them are not workable until a critical mass of fully networked roadside units and smart vehicles is achieved. It will be very difficult to achieve this critical mass in initial years of VANETs, this will further slow down the market penetration. Even when reasonable market penetration has been achieved, the dynamicity of traffic will result in reduced utility of VANET capabilities. One possible solution is to install pervasive fully networked roadside infrastructure but this will be an expensive and
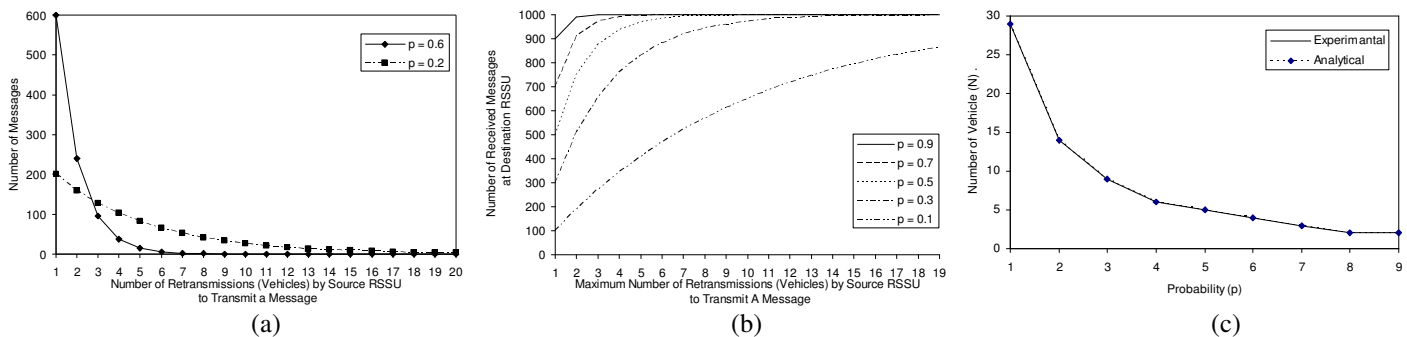

(a)   (b)   (c)

Figure 3: (a) For the probability *p = 0.2* and *p=0.6* (that a vehicle passing source will also pass destination), the number of messages successfully received at destination RSSU after a given number of retransmissions by source RSSU. (b) For different values of probability *p*, the number of received messages at destination after less than or equal to each given number of retransmissions. (c) Number of Relay Vehicles (*N*) required to deliver the message at destination with a 95% probability of confidence (*Pc*) and different values of probability (*p*).

impracticable solution. We have presented an economical and practicable solution to address this issue. We have presented an integrated solution incorporating roadside units with very basic functionality. Our solution is economical, scalable and upgradeable. We show that the solution is workable with a small number of vehicles.

7. REFERENCES

[1] H. Wu, R.M. Fujimoto, R. Guensler, M. Hunter 2004 "MDDV: Mobility centric Data Dissemination Algorithm for Vehicular Networks " ACM VANET, October 2004.

[2] Q. Xu, T. Mak, R. Sengupta, 2004 "Vehicle-to-Vehicle Safety Messaging in DSRC ", ACM VANET, Oct 2004.

[3] G. Korkmaz, E. Ekici, F. Ozguner, U. Ozguner, 2004 "Urban Multi-Hop Broadcast Protocol for Inter-Vehicle Communication Systems", ACM VANET, October 2004.

[4] A. Vahdat, D. Becker, 2000 "Epidemic Routing for Partially-connected Ad-Hoc Networks", Technical Report CS-2000-06, Duke University, July 2000.

[5] N. Wisitpongphan, F. Bai, P. Mudalige, V. Sadekar, and O. Tonguz, "Routing in Sparse Vehicular Ad Hoc Wireless Networks," IEEE Journal on Selected Areas in Comm., vol. 25 issue 8, pp. 1538-1556, October 2007.

[6] T. Spyropoulos, K. Psounis, and C. S. Raghavendra, "Efficient routing in intermittently connected mobile networks: The multi-copy case," IEEE Transactions on Networking, Vol 16, Issue 1, pp. 77 – 90, Feb. 2008.

[7] M. Mabiala, A. Busson, and V. Vèque, "Inside VANET: hybrid network dimensioning and routing protocol comparison," In Proc. of IEEE 65th VTC2007-Spring, pp. 227-232, April 2007.

[8] K. Fall, " A Delay-Tolerant Network Architecture for Challenged Internets," ACM SIGCOMM, August 2003.

[9] T. Little and A. Agarwal, "An Information Propagation Scheme for VANETs," In Proc. of the 8th Intl IEEE Conf on Intelligent Transportation Systems , September 2005.

[10] S. Jain, K. Fall and R. Patra, " Routing in a Delay Tolerant Network," SIGCOMM, August 2004.

[11] D. Goodman, J. Borras, N. Mandayam, and R. Yates, "INFOSTATIONS: A New System Model for Data and Messaging Services," IEEE VTC97, May 1997.

[12] T. Small and Z. J. Hass, "The Shared Wireless Infostation Model - A New Ad Hoc Networking Paradigm (or Where there is a Whale, there is a Way)," MobiHoc, June 2003.

[13] J. Zhao and G. Cao, "VADD: Vehicle-Assisted Data Delivery in Vehicular Ad Hoc Networks," InfoCom, 2006.

[14] C. Lochert, B. Scheuermann, M. Caliskan and M. Mauve, "The Feasibility of Information Dissemination in Vehicular Ad-Hoc Networks," WONS 2007, January 2007.

[15] M. C. Chuah, and F. Fu, "Performance Study of Robust Data Transfer Protocol for VANETs," LNCS - Springer, Vol 4325, pp. 377-39, 2006.

[16] B. Petit, M. Ammar and R. Fujimoto, "Protocols for Roadside-to-Roadside Data Relaying over Vehicular Networks", In Proc. of IEEE WCNC, April 2006.

[17] Y. Ding, C. Wang, and L. Xiao, "A Static-Node Assisted Adaptive Routing Protocol in Vehicular Networks," ACM VANET, September 2007.

[18] V. Jacobson, "Congestion Avoidance and Control," ACM SIGCOM, August 1988.

[19] Binomial Distribution. Wikipedia. [Online] http://en.wikipedia.org/wiki/Binomial_distribution

[20] M. Raya, P. Papadimitratos, and J.-P. Hubaux, " Securing Vehicular Communications," IEEE Wireless Communications Magazine, pp 8-15, 2006.

[21] P. Papadimitratos, L. Buttyan, J-P. Hubaux, F. Kargl, A. Kung, and M. Raya, "Architecture for Secure and Private Vehicular Communications," In Proc. of the 7th Intl Conf on ITS Telecomm, June 2007.

[22] RFC 4346: "The Transport Layer Security (TLS) Protocol Version 1.1".

[23] Mobile Meter Reading, [online] http://www.progress-energy.com/custservice/flares/meters/index.asp

[24] J. Kim and S. Bohacek, "A Comparison of Opportunistic and Deterministic Forwarding in Mobile Multihop Wireless Networks," MobiOpp 2007.
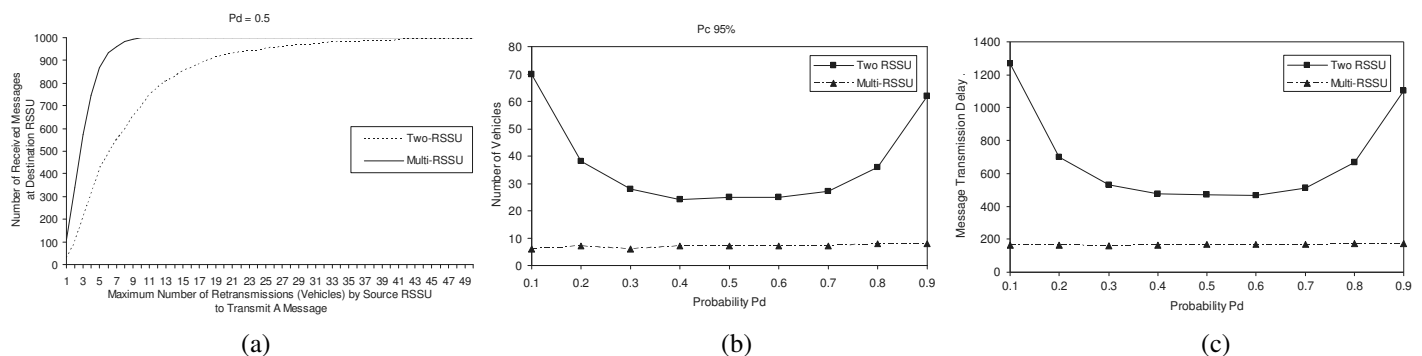
Figure 4: Simulation results for Two-RSSU (without intermediate RSSUs) and Multi-RSSU (with intermediate standalone-RSSUs) (a) For probability of diversion *Pd = 0.5 (that a vehicle passing road junction will divert from its direction of travel)*, the number of received messages at the destination after less than or equal to each given number of retransmissions by the source RSSU. (b) Number of Relay Vehicles used by the source RSSU to deliver the message at the destination with a 95% probability of confidence (*Pc*) for different probabilities (*Pd*). (c) Message transmission delay for different probabilities (*Pd*).