Using Network Aggregation for a Highly Efficient and Secured Transmission of Data on Vehicular

Chaitranjali. H
M.Tech, Dept. Of CSE,
AMCEC, Bangalore,
Karnataka, India

Mr. Doddegowda B. J
Associate Professor, Dept. Of CSE,
AMCEC, Bangalore,
Karnataka, India

***Abstract* — In-network aggregation in VANETs is any kind of multihop message dissemination. To do so, they exchange messages containing relevant information derived from atomic sensor readings. The usage of network aggregation in VANETs aim at improving communication efficiency by summarizing information that is exchanged between vehicles. Due to high bandwidth potential, the aggregation is suitable for all applications are focused in VANET that need to build and maintain up to date information in large areas. Vehicular ad hoc network (VANET) is a vehicle to vehicle (Inter-vehicle communication-IVC) and roadside to vehicle (RVC) communication system. Collision warning, current traffic situation, parking spots, road side warning(due to construction works etc.) are among the major active safety related services addressed by VANET. Issues with Infrastructure support, as an alternative solution to Vehicle to Vehicle (V2V) and roadside unit (RSU) communication have been proposed, as well. In this paper, a new routing is designed exclusively for VANETs and presents some initial performance. A generic model to describe and classify the proposed approaches, and identify future research challenges.**

Key Words — VANET, routing, ad hoc network, network aggregation, V2V, RSU.

I. INTRODUCTION

Vehicular ad hoc network (VANET) is a vehicle to vehicle (Inter-vehicle communication-IVC) and roadside to vehicle (RVC) communication system. The core idea of VANETs is to install dedicated short range radio communication (DSRC) units into vehicles, which enables wireless communication between vehicles and roadside equipment. DSRC supports both public safety and private operations in roadside to vehicle and vehicle to vehicle communication environments utilizing the IEEE 802.11p protocol. DSRC is meant to be a complement to cellular communications by providing very high data transfer rates in circumstances where minimizing latency in the communication link and isolating relatively small communication zones. This new type of communication is suitable for many application related to active safety, traffic efficiency and infotainment [1]. As an example, consider a vehicle that sends warning signals, while there is an traffic jam on the road. Approaching vehicles that receive the messages can break safely or use alternative routes, and the information transfer is not hindered by fog, curves or visual obstacles. Collision warning, current traffic situation, carbon emission, road condition warning (due to construction works etc.) get it among the many enormous reliability corresponding suppliers clarified out of VANET. Classic security paradigms rely on stored digital secret key and cryptographic algorithms. Correct implementation of security algorithms based on a pre-distributed secret key requires Password-Authenticated Key Exchange (PAKE) protocols. These protocols are provable high secure, but the thing is this require costly exponentiation operation and are not suitable for low power resource intensive application. The strong aspects are cost and bandwidth efficient of up to date information in large regions.

The major research challenges in the area lies in design of routing protocol, data sharing, security and privacy, network formation etc. Once deployed, VANETs have the potential to significantly reduce accidents, carbon emissions, and waiting times in traffic jam.

The vehicle-to-roadside communication configuration represents a single hop broadcast where the roadside unit sends a broadcast message in form so-called beacons between vehicles within immediate vicinity. Vehicle-to-roadside communication configuration provides a high bandwidth link between vehicles and roadside units. The roadside units may very well be place neither any specific kilometre nor significantly less, enabling high data rates to be maintained in heavy traffic. For instance, when broadcasting dynamic speed limits, the roadside unit will determine the appropriate speed limit according to its internal timetable and traffic conditions. Routing in VANET seemed to be explored or even explained widely in the past few years. Many routing protocol for VANETs so far, namely Greedy Perimeter Coordinator Routing, Geographic Source Routing or Connectivity-Aware Routing, used only one single route from the source to destination. As soon as an aggregation mechanism summarizes information several vehicles it needs a way to describe the area and time that the summarized information is about. These identifiers lead to another problem: a reduced amount of data used to describe information will not helpful if a much higher amount of data is required to describe the area to which the aggregated value refers. Some of their main conclusions were that: single-path and multipath have similar performance when source and destination are only a few (2-3) hops away, but for larger source-destination distances (4-5 hops) some difference is observed; route coupling plays a significant role. For application that requires dissemination of information from many vehicles in large area, geocast provides geographically limited flooding of messages in a specific destination region.

Together, beaconing and geocasts support applications that either requires frequent dissemination of information in a small area or infrequent dissemination of events in large area. But even efficient geocast protocols cannot support dissemination of frequent updates from large number of target vehicles in large regions, which is required by applications like traffic information system or parking spot finders. Where tolerable, information from multiple sources needs to be combined and aggregated during routing instead of being forwarded unmodified and only being evaluated by receiving vehicles. This is the goal of in-network aggregation protocols for VANETs [3]. Beaconing and geocast support application that either require frequent dissemination of information in small area or infrequent in a large area. Efficient geocast cannot support dissemination of frequent updates from many vehicles in large area. Wireless collision may occur. Suppose each vehicle every time sends the information to other vehicle and that information is getting stored in database, so unwanted information won't get discarded. Even within direct communication range is at most 12% of the available information can be forwarded, where in only 1% can be transported to vehicle in 5km distance. To overcome this we are introducing In-network aggregation for VANET.

II. RELATED WORK

In [4] F. Li et al they did research on VANET and brought the following conclusion. Vehicular ad hoc network (VANET) is an emerging new technology integrating ad hoc network, wireless LAN (WLAN) and cellular technology to achieve intelligent inter-vehicle communications and improve road traffic safety and efficiency. VANETs are distinguished from other kinds of ad hoc networks by their hybrid network architectures, node movement characteristics, and new application scenarios. Therefore, VANETs pose many unique networking research challenges, and the design of an efficient routing protocol for VANETs is very crucial. In this article, we discuss the research challenge of routing in VANETs and survey recent routing protocols and related mobility models for VANETs. In [5] I. Broustis et al, provide an in-depth discussion on the important studies related to architectural design and routing for vehicular networks. Moreover, we discuss the major security concerns appearing in vehicular networks. In [6] C. Lochert et al, show how position-based routing can be applied to a city scenario without assuming that nodes have access to a static street map and without using source routing. In [7] X. Huang et al, we examine the performance of node-disjoint multipath routing in VANETs. Through extensive simulations, we explore the effect of mutual interference on the behaviour of node-disjoint paths. It is shown that whether node-disjoint paths are able to improve performance, compared with the single path, is determined by path coupling and the source-destination distance. Results show that node-disjoint multipath routing can be applied to VANETs to substantially improve performance in terms of delay and packet delivery probability only if the node-disjoint paths are properly chosen.

III. PROPOSED SYSTEM

VANET routing protocol not based on MANET protocols variations, and also according to the characteristics of urban environment from the very beginning. Junction-based Multipath Source Routing or JMSR for short. JMSR is a geographic routing protocol, in the sense that it exploits the location of the nodes and also of the street junctions, known via digital street maps. It maintains concurrently two paths from the source to the destination as a series of junctions the packets should pass through, and not as a series of nodes-relays. We believe that in-network aggregation is an important building block to enable multi-hop information dissemination in vehicular ad hoc networks. Strong aspects are cost- and bandwidth-efficient dissemination of up-to-date information in large regions. In this paper, we offer a comprehensive overview of existing protocol proposals, including a discussion of the requirements that they're going to accommodate, or even models to categorize or maybe take a look at the idea. We can the main strength of the aggregation protocols in providing almost real time information about the extended vicinity of a vehicle. Further assuming that multiple messages are combined in one packet to save packet headed overhead and ignoring wireless transmission collision. Such merging of different information item like speed, time, position, and route can provide bandwidth savings and do not modify information in the forwarding phase.

A. Applications

Applications for vehicular networks can be broadly categorized into safety application, traffic efficiency applications, and infotainment applications [8]. Active safety applications are a major use case for VANETs and are likely to be part of first deployments. However, safety applications typically require exact data to be transmitted with little to no latency. These requirements directly contradict the aims of in-network aggregation. In contrast to safety applications, traffic efficiency applications often require periodic multi-hop dissemination of large amounts of information in wide areas, thereby consuming more wireless bandwidth if implemented naïvely. In addition, safety messages can be used as information source by in-network aggregation protocols. Safety messages often contain traffic-efficiency-relevant information, such as vehicle velocity or outside temperature.

B. Reduction in Data

In VANET protocols, data reduction is often done in a distance-based manner. With increasing distance from the source of a measurement, the provided information becomes increasingly coarse. Hence, it can be described and transmitted with a lower number of bits per second on the medium. It is also conceivable to reduce the spatial resolution by summarizing measurements from larger and larger geographical areas into single aggregates with increasing distance. Or, data representations with a lower accuracy, and thus a smaller size, can be used for measurement data from larger distances. Basically, aggregation schemes can aim to reduce the size of these packets, reduce the number of packets, or a combination of both. If packet size is reduced and collisions are less likely to occur. If fewer packets are transmitted, channel connection is reduced. All these approaches—alone or in combination—in essence reduce the network bandwidth that is spent to convey information about a certain part of the real world.

C. Overhead Reduction

As soon as an aggregation mechanism summarizes information from several vehicles, it needs a way to describe the area and time that the summarized information is about. These identifiers lead to another problem: a reduced amount of data used to describe information will not be helpful if a much higher amount of (meta-) data is required to describe the area to which the aggregated value refers. Practical aggregation mechanisms therefore depend on efficient means to encode the scope of an aggregate in both time and space. For one-dimensional roads, such as highways, the encoding problem is manageable: two points suffice to describe an interval on the road. To distinguish different roads, a road ID can be added.

D. Preservation of Data Utility

While reduction of data and overhead are necessary to cope with bandwidth requirements, it is equally important to ensure that the data utility after aggregation, sometimes referred to as quality of information (QoI) [9], [10], still meets application requirements. Note that metrics to judge data utility cannot be generalized but instead depend on the requirements of a particular application. The issues discussed so far deal with quality loss introduced by the aggregation mechanism itself. The extent to which aggregation results are affected by such faults largely depends on the aggregation function used.

E. Flexibility

From the requirements formulated above, it is obvious that an aggregation mechanism needs to be able to adapt to different situations. Similarly, different applications require a level of aggregation that matches their specific requirements. In essence, fulfilling both requirements often means that very coarse-grained aggregation is mandatory for information far away, while information close to the own vehicle needs to be represented in a much more fine-grained way. Thus, schemes that use simple road segmentation approaches are in general not flexible enough.

F. Privacy

Privacy has been highlighted as an important property for VANET deployment [11]. Aggregation has intrinsic privacy benefits, because information is summarized more and more with increasing distance to the participating vehicles. Thus, the further away an observer is from a target vehicle, the less information she gets about the exact position, speed, and other information items from the observed vehicle.

G. Information Integrity Protection(Key Exchange Policy)

In contrast to the intrinsically higher level of privacy, the resilience of aggregation mechanisms against malicious data manipulation is generally lower than the resilience of comparable schemes using exact information. That is, the attacker’s goal is to create messages suggesting a specific traffic or other situation, which diverts from the real world in a way beneficial to the attacker. The attacker is assumed to possess valid key material issued by a public key infrastructure (PKI) (e.g., [12]) to create signatures on her messages. So a Key Exchange mechanism has been introduced where it is possible to piggyback a session key exchange protocol on the authentication protocol. The Verifier can recover these secret indices at the end of a successful authentication. If the length of secret indices is not enough to encode the whole secret key, the authentication protocol may be repeated multiple times until the required number of secret bits is transmitted to the Verifier.

H. In-network aggregation

In typical sensor network scenarios, data is collected by sensor nodes throughout some area, and needs to be made available at some central node(s), where it is processed, analyzed, and used by the application. In-network aggregation deals with this distributed processing of data within the network. Data aggregation techniques are tightly coupled with how data is gathered at the sensor nodes as well as how packets are routed through the network, and have a significant impact on overall network efficiency (e.g., by reducing the number of transmissions or the length of the packets to be transmitted).

IV. ALGORITHM

Algorithm: SOTIS: Fusion ($A1, \ldots, An$)
Input: A set of aggregates $\{A1, \ldots, An\} \subset A$.
Result: An aggregates A that represents the merged data of all

Aggregates
If $A1, \ldots, An \in O$ then
A<-((GetSegment(p),r1), GetCurrentTime( ),
$1/n \sum^{n}_{i=1} v_i$)
else
A<- $A_{\mathrm{argmax}\ i}\ (A_i)$
end
return A

ISSN: 2278-0181
ICESMART-2015 Conference Proceedings

One of the earliest mechanisms is self organizing traffic information system (SOTIS) [13], which was originally introduced in 2003. The core idea of SOTIS is to impose a fixed segmentation on the road network, which correlates with the wireless communication range.

Fusion: Atomic observations are merged by creating a new summary record about a road segment. The function GetSegment is used to determine the fixed segment ID corresponding to a given position. The time stamp is set to the current time. All atomic speed values are averaged. Aggregates are not merged further; given two aggregates, the fusion function will drop the older aggregate.

By disseminating only summarized information about road segments, SOTIS achieves a much higher awareness of the current traffic situation than dissemination of atomic information. Moreover, SOTIS reduces the number of packets that are sent over the wireless channel.

V. RESULTS

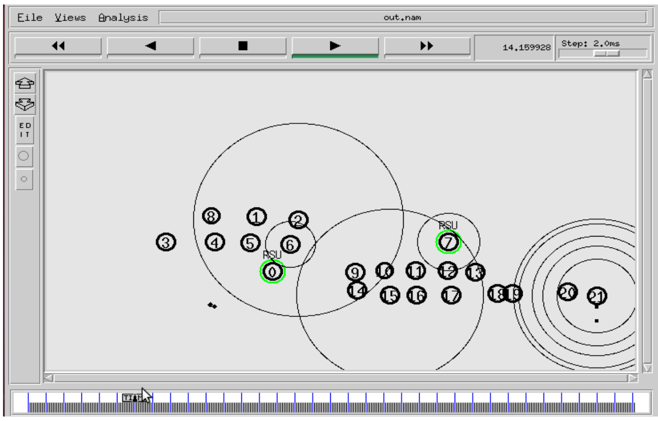

Fig.1 RSU handoff in VANETs

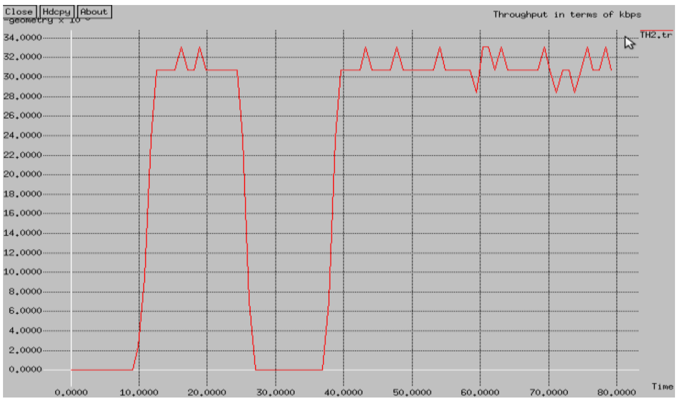

Fig.2 Throughput graph

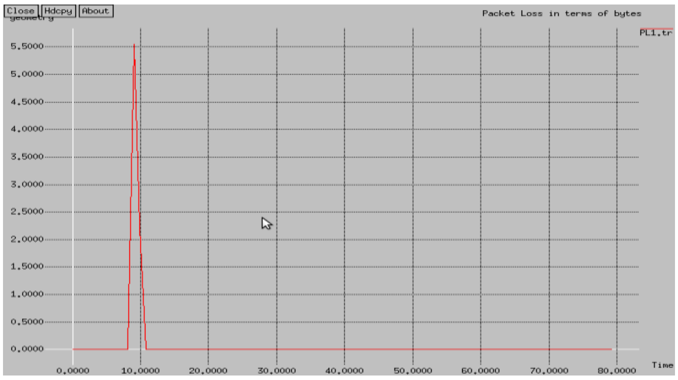

Fig.3 Packet loss graph

Figure 1 shows RSU handoff in VANET, a handoff occurs when a vehicle moves beyond the radio range of one RSU, and into the range of another RSU. When a vehicle moves and loses connectivity to its RSU, it starts gathering information on the RSUs present in the vicinity by broadcasting probe messages. The vehicle can receive responses from multiple RSUs, and based on some implementation-dependent policy, it sends a reassociation request to one of the RSUs. The RSU responds with either a success or a failure. On a successful response, the vehicle is associated with the new RSU, and the pre-handoff RSU exchanges vehicle-specific context information with this new RSU.

Figure 2 shows throughput graph, depends on time the throughput graph will be plotted. When vehicles moves within the range of RSU, at that time throughput will keeps on increasing upto maximum range and when vehicles moves out off range of RSU, then the throughput will be decrease and figure 3 shows packet loss graph ,packet will may not be or may be loss while sending the current traffic reports between vehicles.

VI. CONCLUSION

Vehicular networks are currently approaching their initial deployment. An important issue, in-network aggregation is not currently being implemented. The research literature offers a number of proposals for suitable aggregation mechanisms with varying degrees of flexibility, scalability, and integrity protection. In this paper, we have presented a generic architecture and used it to categorize different aggregation mechanisms and asses their suitability for solving particular challenges. Identification of major future challenges to further investigate generic aggregation protocols, which are able to integrate information from different domains, such as traffic information, weather information system, road warnings, and parking spots.

Once VANET deployments reach larger and larger scale, it is important that research in aggregation mechanisms, simpler information dissemination protocols can be complemented with more advanced aggregation mechanisms.

REFERENCES

[1] M. Emmelmann, B. Bochow, and C. Kellum, *Vehicular Networking: Automotive Applications and Beyond*. Hoboken, NJ, USA: Wiley, 2010, ser. Intelligent Transport Systems.

[2] *Intelligent Transport Systems (ITS); Vehicular Communications; Basic set of Applications; Part 2:Specification of Cooperative Awareness Basic Service*, ETSI EN 302 637-2, 2013.

[3] E. Schoch, F. Kargl, M. Weber, and T. Leinmuller, "Communication patterns in VANETs," *IEEE Commun. Mag.*, vol. 46, no. 11, pp. 119–125, Nov. 2008.

[4] Fan Li and Yu Wang, University of North Carolina at Charlotte, *Routing in Vehicular Ad Hoc Networks: A Survey*, JUNE 2007IEEE.

[5] Broustis, Ioannis; Faloutsos, Michali, *Routing in Vehicular Networks*: Feasibility, Modeling, and Security, DEC. 2008 IEEE.

[6] C. Lochert, B. Scheuermann, C. Wewetzer, A. Luebke, and M. Mauve, "Data aggregation and roadside unit placement for a VANET traffic information system," in *Proc. 5th ACMInt.Workshop VANET*, 2008, pp. 58–65.

[7] F. Schaub, Z. Ma, and F. Kargl, "Privacy requirements in vehicular communication systems," in *Proc. IEEE Int. Conf. Privacy, Security, Risk, and Trust (Passat)/Symp. Secure Comput.*, Vancouver, BC, Canada, 2009.

[8] H. Hartenstein and K. Laberteaux, *VANET: Vehicular Applications and Inter-Networking Technologies*. Hoboken, NJ, USA: Wiley, 2010, ser. Intelligent Transport Systems.

[9] C. Feng, R. Zhang, S. Jiang, and Z. Li, "QoI-based data gathering and routing guidance in VANETs," in *Web-Age Information Management*, vol. 7419, Z. Bao, Y. Gao, Y. Gu, L. Guo, Y. Li, J. Lu, Z. Ren, C. Wang, and X. Zhang, Eds. Berlin, Germany: Springer-Verlag, 2012, ser. Lecture Notes in Computer Science, pp. 87–98.

[10] E. Gelenbe and L. Hey, "Quality of information: An empirical approach," in *Proc. 5th IEEE Int. Conf. MASS*, 2008, pp. 30–735.

[11] F. Schaub, Z. Ma, and F. Kargl, "Privacy requirements in vehicular communication systems," in *Proc. IEEE Int. Conf. Privacy, Security, Risk, and Trust (Passat)/Symp. Secure Comput.*, Vancouver, BC, Canada, 2009, pp. 139–145.

[12] *Intelligent Transport Systems (ITS); Security; Security Header and Certificate Formats*, ETSI TS 103 097, 2013.

[13] L. Wischhof, A. Ebner, H. Rohling, M. Lott, and R. Halfmann, "SOTIS—A self-organizing traffic information system," in *Proc. 57th IEEE Semiannu. VTC-Spring*, 2003, pp. 2442–2446.