VEHICLE-TO-VEHICLE COMMUNICATION USING WSN FOR ENHANCED ROAD SAFETY

Ms.G.Yasotha
Assistant Professor, Bharathiyar Institute of engineering for women, Tamilnadu, India

Abstract

Vehicle-to-vehicle communication and vehicle-to-roadside sensor communication are introduced with the help of hybrid ITS safety architecture. To implement this network require major investments for purchase, installation and maintenance. The roadside wireless sensor and networking technology represents a cost-effective solution and can leverage the deployment of the system as a whole. Compare to the other services of the hybrid communication system, the paper propose accident prevention and post-accident investigation. A system and protocol architecture with a fully distributed concept for efficient and secure storage of sensor data is introduced. For deployment, this architecture would likely to be a combination of dedicated road-side units as a centralized network element for communication and data storage. For the proposed system, this describes the main components (radio, networking and services, security). Finally, the paper describes the prototype implementation and experimental test bed featuring hardware and software platforms for vehicle on-board units and sensor nodes.

Keywords: vehicular communication, wireless sensor networks.

I. INTRODUCTION

In order to make roads safer, cleaner, smarter, sensor and communication technologies are mostly considered in research, standardization and development. While today’s vehicles are already able to sense the surrounding environment and we can expect that future cars will communicate with a roadside communication infrastructure and with each other. Connected vehicles can create a fundamental building block of intelligent transport systems (ITS) and can provide abundant application services to improve safety and comfort of driving.

Among the various wireless technologies for vehicular communication, we can identify a clear trend in the usage of Wireless LAN. The standards IEEE 802.11p as well as the frequency band allocations in the above 5.8 GHz band for various public safety services then clearly indicate its deployment. For vehicle-to-infrastructure communications, the system architecture assumes access points with IEEE 802.11p network interfaces to be arranged at least in the dedicated locations (such as road intersections), whereas the system is still able to deliver information even when no access point is available within the communication range of a vehicle. A particular technology is vehicular ad hoc networking (VANET), that enables communication over multiple wireless hops, potentially but its not necessarily including roadside access points.

While the development of vehicular communication technology based on IEEE 802.11p has considerably progressed in the previous years, the introduction and wide-scale deployment of such a system has not been decided till now. In a purely vehicular communication system, i.e. without roadside access points, a minimum market dissemination of equipped vehicles are required for applications to work. This can at the best to be achieved a few years after an initial commercial
roll-out. To accelerate the proceeds of such investment, a roadside infrastructure could be installed along major road from corner to corner a country. However, costs for purchase, installation and maintenance represent a major investment and in turn can be an obstruction for a successful introduction.

A harmonizing solution to the deployment of road-side access points consists of road-side wireless sensors. These devices characterize a cost effective solution and allow creating wireless sensor networks (WSN), but are subject to energy and processing power constraints. For battery-powered sensor nodes, IEEE 802.15.4 is a ingrained radio technology that permits embedded systems to function up to years on a simple pair of AA batteries. WSN islands can be rolled out along the road, such as on the road surface or at road restrictions (curves, tunnels and bridges), and even on a wider scale. They can be used to determine physical data like temperature, humidity, light, or sense and track movements.

In this paper, we propose and consider a hybrid architecture that combines vehicle-to-vehicle communication and vehicle-to-roadside sensor communication. From the wide range of possible use cases, we have chosen accident avoidance and post-accident analysis, which we regard as important future services.

For accident avoidance, roadside sensor nodes measure the road condition at several positions on the surface, combined the measured values and communicate their aggregated value to an approaching vehicle. The vehicle generates a notice message and distributes it to all vehicles in a certain geographical area, potentially using wireless multi-hop communication. For post-accident investigation, sensor nodes always measure the road condition and store this information within the WSN itself. When a accident occurs, road situation data stored over a adequately long duration can be used for forensic restoration of road accidents. In contrast to the accident prevention service, such a responsibility service needs to be restricted to a well specified group of end-users, e.g. assurance companies or the road patrol. Information stored in the WSN can also be utilized to judge a driver’s and the driving style according to the road condition at the moment of an accident.

The fusion, road-side WSN – VANET communication architecture assumes that vehicles are equipped with an on board-unit (OBU) and two wireless network interfaces; namely IEEE 802.11p and IEEE 802.15.4. The sensor data will be stored in a distributed and redundant database in the sensor nodes. Data are also transmitted to future vehicles, which can inject vulnerability warnings into the VANET. As compared to the systems architecture, the one just presented allows to decrease costs for ITS road-side communication facilities. In such a setting rejection of road-side equipment other than the sensor nodes themselves is necessary. We argue that the WSN hardware, roll-out and maintenance costs are a important success criterion for a real WSN island penetration in the context of vehicular communication since the roll-out of WSN islands with high possibility is an investment of a single or few providers. Maintaining the costs for road-side tools less also motivates our decision not to use tamper challenging modules in the sensor nodes. Accordingly, the best achievable security is achieved by applying pure software solutions.

Alternative system architecture is also obtainable in this paper. we do not consider costs for road-side equipment as primary design standard and therefore add a more powerful RSU to each road-side WSN island. Such a setting is valuable with respect to a straightforward storage of monitored data, but also paves the way to an possible WSN and/or VANET communication over the Internet. As an example, live environmental information could be pressed to the car navigation system. The coexistence of both approaches is also likely since it provides a good cooperation between
costs and connectivity, provide a road operator the choice between two systems

II. SCENARIO AND USE CASES

Roads have always been unsafe, and a lot of efforts have been undertaken to get better their security. Vehicles, education, road signs have been improved during generations. However, dangers stay behind and with the rise of computer and wireless technologies, new solutions are accessible to assist the driver in hazardous situations and to reduce road dangers.

We envision that in a near future, vehicles will be prepared with wireless devices, so they can communicate with each other. The most important application of this technology is to let vehicles exchange about their current context. In detail, the information exchanged can be of 2 types, (i) periodic exchange of status messages among the vehicles in direct communication range and (ii) safety messages triggered by a hazardous event and distributed in a geographical region. At the same time frame of the VANET deployment, we be expecting that WSN technologies would have reach the necessary maturity to be rolled out in a great scale at an reasonable cost. We foresee that WSN roadside islands will be installed in exact dangerous locations to support drivers with current road and weather situation. Normally, WSN technologies help where neither the vehicle’s sensors nor the driver can sense the danger, e.g. very localized road condition, animal cross the road out of a forest, etc. The roadside WSN islands considerably extend the sensing range of a vehicle. consequently, either the driver or the vehicle itself could initiate suitable reactions according to the current environmental situation with the overall aim to enlarge the driver’s safety.

The set-up of a combined WSN and VANET architecture aims at the provisioning of two harmonizing services:

1) Accident prevention. When a car passed by a sensor network, it retrieve fresh environmental data collected by the roadside sensors. Data can include various physical quantities, such as temperature, humidity and light, and also detect moving obstacles (such as animals); moreover, it can be processed within the WSN network, in order to acquire higher level information. The received information’s are processed in the vehicle’s OBU and potentially displayed to the driver. Hence, wireless sensor nodes are complement compared to other sensors installed in a car (such as radar). However, wireless sensor nodes are external devices and its principle can measure road conditions data more accurately than an on-board sensor. In addition to the data of the wireless sensor node may include a set of data covering a period of quantity collected over a time-span and make the data more conceivable.

Once a vehicle has processed the sensor data, it may understand the data as a dangerous situation and trigger a safety warning message. For this message, the vehicle determines a geographical region defined by a geometric shape and broadcasts the message to its nearby vehicles. The communication system of the vehicles ensures that the data packets are consistently distributed to all vehicles located within a region. As a result, vehicles that collect the information are warned about dangerous spot ahead of time and can take suitable countermeasures.

2) Post-accident investigation: In this case, sensor nodes are continuously measure and store the environmental data. These datas include the collected quantities (e.g. temperature) and also event data, such as before detected obstacles and vehicles. Storing this type of information over a long time period may be of interest for a forensic team. In distinguish to the accident
prevention service; such a liability service will be limited to a well specific group of ending users, e.g. insurance companies or the road patrol. These authoritative users can recover the sensor data from the roadside WSN islands from (nearly) any time in the past for forensics purposes. Typical examples are retroactive detection of accident causes and assessment of drivers’ activities with respect to the road conditions at the time of the accident.

The two scenarios describe above pose various functional and performance-related necessities for the data communication and storage. A fundamental assumption is that a communication system for vehicle-to-roadside communication will be rolled out if the expenses for the roadside equipment, installation, and maintenance are minimal. This leads to system architecture with very low cost autonomous sensor networks and without the deployment of dedicated roadside units. While sensor nodes may disappear over time due to their constrained energy capabilities, both communication among sensors and data storage need to be distributed and redundantly controlled. Likewise, sensor nodes’ data transmission to approaching vehicles and distribution of data for persistent storage require energy-efficient communication protocols. The main requirements for the security are to ensure the consistency and the trustworthiness of the data being communicated from the WSN to the vehicles. In adding together, as the data are stored for a relative long duration within the roadside WSN, they shall not be stored in plain-text. In turn, in order to reduce costs, software-based security solutions are chosen over costly hardware components or tamper-resistant modules on sensor nodes.

III. PROTOTYPE IMPLEMENTATION AND EXPERIMENTAL TESTBED

We have developed a software prototype and set up an experimental test bed as proof-of-concept of the proposed architecture together with the integrated communication system for VANET and WSN, as well as a safety middleware secure distributed storage in sensor nodes. The test bed was offered in a live demonstration at the 14th ITS World Congress and Exhibition in Beijing in 2007.

A. Setup

For the VANET node, we used the hardware NEC Link Bird-MX, an embedded system mainly planned for vehicle. For the wireless sensor network, we tested the system on commercially accessible TelosB platforms.

The protocol stack of this vehicular communication system is implemented in C for the Linux OS, which results in higher performance and good portability to embedded systems. We tested our roadside application in two setups. In an indoor lab setup the network is deploy over a small area as a proof-of-concept. In this road setup, we have deployed the WSN to cover an outdoor area in order to show the probability of WSN-to-vehicle communication. In both experiments, the post-accident investigation characteristic of our WSN application was also demonstrated and tested.

B. Indoor Setup and Tests

The purpose of the indoor tests was to observe the capability of every vehicle inside the Geo-broadcast range to receive warning signals initiate by the WSN. Three VANET nodes run a application that displays vulnerability warnings to drivers via a visual HMI. Every VANET nodes run Geo cast as part of the communication protocol stack. The position of the vehicles are mocked by a 4th control PC, which feeds the VANET nodes with position information and allowed to reset, pause or start the experiment at every time. Because of the propinquity of the equipment, packet dropping is also emulated based on the distance between communication nodes. In the experiment, one of the VANET nodes is coupled via IEEE 802.15.4 to a sensor note that acts as a gateway to the sensor network. If this node is in the surrounding area of the sensor network, it will receive sensor data, and forward to other VANET nodes nearby using Geo-broadcast.
C. Road Setup and Tests

In the road setup, we have deployed the WSN to cover an area close to a road. The sensor nodes that can potentially communicate with vehicles are put on poles standing about 45 cm above ground. Nodes moving on the ground suffer from not as good as connectivity due to a higher degree of ground reflection and scattering. In this test, a vehicle – equipped with an on-board unit and an 802.15.4 interface – is driving toward the WSN with a Line-of-Sight (LoS) communication path. During the analysis, the vehicle periodically sends requests to recover WSN information. When the vehicle’s OBU receives data from the WSN, the warning is graphically shown to the driver via screen and HMI together with the considered distance between the vehicle and the WSN.

For the demonstration of the accident avoidance service we drove the vehicle in direction of the roadside WSN with changeable velocities up to 70 km/h. Higher velocities could not be maintained safely on our test spot due to the limited road length. We considered approximately the distance at which the vehicle received the safety information from the WSN for the first time, which would determine the time left for a driver to react to the incoming danger. The vehicle sent a message to the roadside WSN each 200 ms. An aggregator node receiving such a message responded by sending the authentic aggregated value of their cluster.

In this measurement operation the four aggregator nodes have been placed 45 cm above the ground. Whereas the antenna type has important impact on the transmission range and thus on the reaction time of a driver the selected velocities in our setting do only effect the measured transmission range to a minor degree. For the setting with the directed antenna we made three measurements per velocity, whereas we did only one for each velocity when using an omni-directional antenna. In turns out that under such condition(surely simplified conditions since no obstacle are in place and only one vehicle is sending ’hello’-messages at one point in time) our measurements defend the design choice to directly communicate linking the roadside WSN and the vehicle’s OBU via IEEE 802.15.4. To recall, in order to keep hardware costs in a real large-scale deployment of roadside WSNs for an IEEE 802.11 enabled RSU per every WSN road side, we determined not to involve any devices on the roadside which are more powerful and costly than sensor nodes themselves.

D. Post-Accident Investigation

As Accident Investigator Node (AIN) we use a standard laptop with a tinyPEDS client to retrieve past data from the WSN. In our setting, sensor nodes have the capability to store data for 50 days, which appears to be enough for a typical post-accident investigation.

In the experiment we let the AIN query the WSN about past monitor values, which was successfully able to recover and decrypt the data. We demonstrated safety features such as DoS resilience using access control mechanisms developed in the UbiSec & Sens project by showing that reader devices that do not possess the key are not able to decrypt the stored data.

IV. CONCLUSION

Hybrid architecture of vehicular ad hoc networks (VANETs) and roadside wireless sensor networks (WSN) that relies on a fully distributed approach without centralized infrastructure elements for coordinating of communication and data storage is presented here. Among the manifold opportunities of such a system here focus on accident prevention and post-accident investigations. The components are well modified to the specific requirements of VANETs and WSN, correspondingly.

We argue that for the consumption of a vehicular communication system, the costs for purchase, installation and protection of the required infrastructure can become a major barrier for the introduction of such a system. A
Entirely distributed approach for the roadside WSNs without a dedicated roadside unit per WSN considerably reduces the costs for the WSN and can therefore leverage the generally system. WSN with dedicated RSUs are still favorable in order to provide full service and connectivity to access networks, but we expect that the majority of the deployed systems will work fully autonomously.

REFERENCES