Adaptive Traffic Management for Secure and Efficient Emergency Services in Smart Cities

Soufiene Djahel[∓], Mazeiar Salehie[±], Irina Tal[‡] and Pooyan Jamshidi[‡]
[∓] Lero, UCD School of Computer Science and Informatics, Ireland
[±] Lero, University of Limerick, Ireland
[‡] Lero, Dublin City University, Ireland
soufiene.djahel@ucd.ie, mazeiar.salehie@lero.ie, irina.tal2@mail.dcu.ie, pooyan.jamshidi@computing.dcu.ie

***Abstract*—Rapid increase in number of vehicles on the roads as well as growing size of cities have led to a plethora of challenges for road traffic management authorities such as traffic congestion, accidents and air pollution. The work presented in this paper focuses on the particular problem of traffic management for emergency services, for which a delay of few minutes may cause human lives risks as well as financial losses. The goal is to reduce the latency of emergency services for vehicles such as ambulances and police cars, with minimum unnecessary disruption to the regular traffic, and preventing potential misuses. To this end, we propose to design a framework in which the Traffic Management System (TMS) may adapt by dynamically adjusting traffic lights, changing related driving policies, recommending behavior change to drivers, and applying essential security controls. The choice of an adaptation depends on the emergency severity level announced by the emergency vehicle(s). The severity level may need to be verified by corresponding authorities to preserve security measures. We discuss the details of our proposed framework and the potential challenges in the paper.**

***Keywords* – Traffic Management Systems (TMSs), Vehicle to Vehicle (V2V), Vehicle to Infrastructure (V2I), Adaptive Security, Adaptive Software, Emergency Service, Smart Cities.**

I. Introduction and motivation

The number of cars using the limited road networks infrastructure has seen a tremendous growth recently. One major consequence of this increase is the arisen management problems that range from traffic congestion control to driving safety and environmental impact. Over the last years, researchers from both industry and academia were focusing their efforts on exploiting the advances in sensing, communication and dynamic adaptive technologies to make the existing road Traffic Management Systems (TMSs) more efficient to cope with the above issues in future smart cities. One of the most critical consequences of traffic congestion is the delay of emergency services, such as police intervention, fire and rescue operations as well as medical services. Indeed, human lives and the amount of financial loss in case of incident or criminal attack depend on the efficiency and timely response of emergency services.

In addition to the delay issue, recent road traffic statistics reveal another extremely serious concern which is emergency vehicles crashes. According to the statistics published in [1], the crashes involving emergency vehicles using the physical emergency signals led to 60 deaths and 918 total injuries in USA only, in 2009. Moreover, in this case, the impact on the emergency area which is the target of the crashed emergency vehicle is exacerbated due to the large delay that other emergency vehicles may experience before reaching this area. Besides traffic congestion, another cause of such crashes and delay is the failure to yield the right-of-way to an approaching emergency vehicle [5]. This failure is usually due to drivers not being able to timely recognize the approaching emergency vehicle and react appropriately.

Adding to above concerns, security is also important in emergency response. Security has twofold in this problem. First, traffic privileges for emergency vehicles might be misused by criminals, hackers and other threat agents. A fake ambulance may benefit a "green passage" through intersections to handle a fake emergency case. Second, the emergency case itself may have some security impacts on citizens. An area affected by a robbery, police car chasing or hostage-taking situation is often dangerous for people, and TMS must keep away non-emergency vehicles from the scene.

To address all these aspects of emergency response services, TMS should be able to control the behaviour of non-emergency vehicles to ensure fast emergency service delivery with minimum number of crashes, minimum disruption to the regular traffic flow, and satisfaction of security requirements. These objectives should be achieved in the dynamic environment of a city by considering uncertainty in emergency cases and spatiotemporal factors of the traffic flow. We propose an adaptive traffic management framework that dynamically adjust infrastructure actuators and steer drivers to fulfill specified requirements.

The remainder of this work in progress paper is structured as follows. Section II gives an overview on the proposed adaptive TMS. Next, we describe the proposed architecture in section III. In section IV, we discuss our research plan. Finally, we present the literature in Section V.

II. Solution overview

The problem we tackle in this work is the lack of an architecture or design of a TMS to ensure secure and efficient emergency service delivery in smart cities. Here, smart cities refer to the cities equipped with intelligent infrastructure and in which most of vehicles are equipped with advanced communication technologies.

A. System objectives

To make our framework viable and valuable in real road environment, a tradeoff between the following three key objectives should be carefully considered at design and runtime: i) achieving minimum response time for emergency services, ii) achieving minimum disruption of the regular road traffic flow, and iii) satisfying the security requirements of the road network authorities. Security requirements are often authenticating emergency vehicles and authorizing them to access a proper privilege level. These three objectives should be satisfied considering the emergency sensitivity level.

Our system considers three emergency levels: high, medium and low. The high emergency level has the highest priority for changing behaviors or policies of system components. For the high level, the behavior of traffic lights, traffic policies (speed limit, one-way/two-way traffic, turning rules, reserved lanes) can be changed and traffic may be rerouted. A highly emergency traffic service request needs to be strongly authenticated, authorized and verified by a trusted authority. For medium and low-level emergency cases only changing traffic lights and rerouting traffic are allowed with weaker security

controls. In the low-level except the traffic light manipulation, other behavior changes are recommended to drivers.

B. Why an adaptive TMS?

We have chosen to design an adaptive TMS (i.e. security and driving rules adapt to the emergency level and traffic conditions) due to the following facts. The maximum tolerable response time of emergency service could differ according to the type of incident (e.g., fire, car crash, robbery, riot, etc), its severity and the assets required to be protected (e.g., people, cars, affected locations such as banks and abandoned warehouse). For example, if there is a serious injury due to a riot in a part of the city, the ambulance should access to this area in a short time, while other vehicles should be rerouted to avoid this dangerous area.

Furthermore, in road networks, especially in big cities, the reaction of a TMS to create green passages for the emergency vehicles may depend on real-time traffic conditions and prediction. If the traffic congestion around the fastest route assigned to the emergency vehicle is low then traffic lights timing change and inter-vehicles coordination are sufficient to ensure short response time. If the congestion is medium then the TMS may also adapt the driving policies accordingly. Finally, in case of very high congestion level re-routing the traffic and closing some road segments may also be needed.

An adaptive TMS should take into account both traffic congestion and incident emergency levels to set the adaptation level required to ensure the efficiency of the emergency service. In this way, comparable incidents may require different traffic adaptation actions due to the traffic conditions. Using the proposed adaptive TMS, a life-and-death scenario in which an ambulance carrying injuries needing urgent attendance in a hospital being stuck in a congested intersection or road segment would be avoided.

C. Interaction between the TMC and its environment

A TMS in a city (Dublin for example) usually consists of a set of Traffic Management Controllers (TMCs), each of them controls and manages the traffic in a given area (e.g., Dublin 4). The role of the TMC component in our framework is threefold, as illustrated in Figure 1. First, upon reception of the emergency level notification announced by an emergency vehicle, the TMC requests the corresponding authority (e.g., hospital, rescue department etc) to authenticate the vehicle if the advertized emergency level requires that. Second, once the emergency vehicle identity is authenticated and its emergency level is confirmed, the corresponding adaptation to the traffic control equipments and driving policies should be approved by the road network authority. Finally, the TMC should provide to the emergency vehicle the best route (fastest route) to speed up its access to the emergency area. Moreover, this route must be updated during the vehicle journey as traffic conditions and congestion level change rapidly. To calculate the best route, the TMC uses the emergency vehicle characteristics (e.g., vehicle category, height, weight etc), current traffic conditions in addition to the traffic prediction forecasts during the estimated duration of its journey.

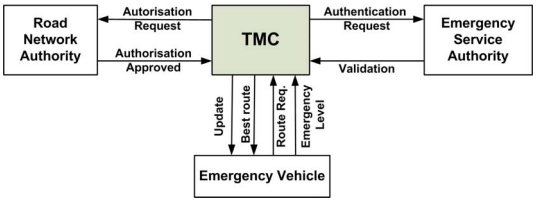

Figure 1: TMC and the environmental interactions

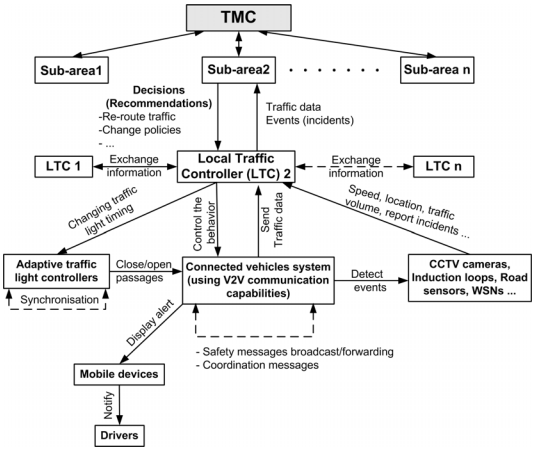

Figure 2: Architecture of the proposed adaptive TMS

III. The proposed framework

A. Architecture of adaptive TMS

In this section, we describe the architecture of the adaptive TMS and the role of each of its components. As shown in Figure 2, the proposed dynamic adaptive TMS consists of separate coordinated components such as Traffic Management Controller (TMC), Local Traffic Controller (LTC), Adaptive Traffic Light Controllers, Environmental Sensor Controllers and Connected Vehicle System. This latter system is usually equipped with advanced wireless communication capabilities, on-board processing units, GPS navigation and smart applications. The TMC is gathering the traffic data from all the LTCs in each sub-area in order to acquire a global view on the traffic conditions within its area, then provides recommendations/decisions about the most appropriate adaptation to satisfy the emergency service request and minimize the incurred disruption of the regular traffic flow.

The traffic data sent to the TMC is collected by the LTCs from heterogeneous sources like, CCTV cameras, road sensors and induction loop systems. Additionally, the vehicles which are usually organized in clusters, report traffic information through V2I (vehicle to infrastructure) communication capabilities. Each LTC manages a set of adaptive traffic light controllers that need to be synchronized in order to lead the vehicle. Moreover, the TLC sends them the instructions about the adaptation level of the traffic light timing, as appropriate. Depending on the emergency level, the LTC may also broadcast new driving policies (e.g. speed limit, reserved lanes, turning rules, etc) towards the non-emergency vehicles which then use coordination protocols to safely apply the new policies. In this case, the LTC should also notify the driver about these new policies, as well as all the necessary details about the emergency case, including location and direction of the emergency vehicle, although in some cases, such as police missions, confidentiality issues should be considered. The notification can be performed in different ways. The entertainment system may display a message or play an alarm. The system can also send a SMS to the drivers mobile phone, which of course is not safest way because of the distraction. Besides, connected vehicles system provides the capability to identify threats and hazards on the roadway and exchange this information over wireless networks to ensure early notification of the drivers.

In this architecture, each component has different levels of dynamicity and adaptability. For example, in traffic light controller, the lights and the related timing constraints change dynamically according to the congestion and the emergency levels. For vehicles, the minimum/maximum speed control and notification alarms are dynamically adjusted by the LTC. Finally, for LTC, the security policies can be changed according to the emergency level.

As an illustrative example, Figure 3 shows a road intersection

controlled by traffic lights and an ambulance announcing its approach to the LTC as well as to the traffic light controller in order to clear the route ahead. The purpose of this double notification is to switch the traffic light to green when the ambulance reaches the intersection and also to allow the LTC to spread this notification to the LTCs of the nearby sub-areas, as shown in Figure2. In this way, the vehicles in the road segments ahead will be notified earlier and thus a safer inter-vehicles coordination is ensured. Upon reception of the emergency notification from the ambulance, the LTC authenticates it in accordance to the emergency level and might make use of corresponding authorities databases. If the emergency message is authenticated, the LTC broadcasts the required adaptation actions towards the traffic lights as well as the vehicles within its transmission range. The receiver non-emergency vehicles will yield the road to the ambulance and apply the requested adaptation (speed, lane and direction change) through the exchange of cooperative safety messages between each other to coordinate their actions.

B. Inter vehicles communication

The role of inter vehicles communication in our framework is to ensure wide spread of the emergency vehicle notification as well as the coordination between the vehicles to ensure efficient application of the new driving policies advertized by the LTC. Moreover, a crashed or stalled vehicle in the best route of the emergency vehicle may use V2I or (V2V+V2I) communication capabilities to notify the LTC which in its turn will reroute the emergency vehicle to avoid this bottleneck.

The efficiency of V2V and V2I communication depends mainly on the robustness of both IEEE802.11P [6] and the broadcast protocols used to disseminate the emergency/safety messages among the vehicles and among the vehicles and the infrastructure. Hence, as part of our framework, we need to achieve the following goals. First, improve IEEE802.11P MAC protocol by proposing a set of mechanisms to control beacon transmissions when the vehicles density gets higher, and thus prevent the congestion state [16]. Notice that the congestion state may cause a significant delay for the exchanged coordination messages as well as the messages disseminated by the LTCs, leading to vehicles collision. Second, design robust and scalable protocols for data dissemination for both V2V and V2I communication scenarios in urban and highway environments. The main feature of this protocol is its ability to support real time critical information dissemination among the vehicles and among the vehicles and the infrastructure. This protocol will complement the improvement brought by the congestion control mechanism set at MAC layer, hence we ensure that the messages sent by the infrastructure can reach the whole set of vehicles in the road segment in a short delay.

C. Security adaptation

Emergency services are susceptible to several threats and misuses. First, unauthorized drivers may announce a false emergency case to benefit from "green passage" through the city for different purposes. Second, The false emergency case may aim to block specific roads to prepare a context for a crime (e.g., robbery or terrorist attack). Third, a genuine emergency vehicle may claim to be in a mission for a false emergency case. To prevent these misuses, security adaptation can be applied through several effectors: i) Emergency cars are authenticated by the infrastructure through V2I and I2I (Infrastructure to Infrastructure) communication. This can be applied by traffic manager and traffic light controllers. ii) The emergency case might need to be verified by the corresponding authority for medium and high severity levels through V2I and I2I communication. Appropriate traffic adaptation actions then should be authorized accordingly by traffic manager and traffic light controllers. iii) Emergency car and the case might be authenticated and verified by non-emergency vehicles through V2V and V2I communication. Vehicles can report any suspicious case to each other and the infrastructure. Of course, this source of information is not completely trustful.

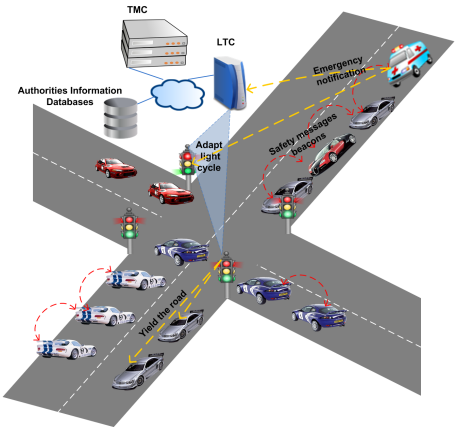

Figure 3: An emergency scenario

Note that different effectors may be applied in each context, particularly depending on the emergency case and its sensitivity level. For example, a low-level emergency case with slight traffic impact may not need a strong authentication method and verification. Other than preventing the misuse of traffic privileges given to emergency services, the affected area by incidents may need to be closed to drivers. For example, because of some valuable assets or security threats in a crime scene vehicles need to be kept away from that area.

IV. Research Vision

The details of our research plan to realize the proposed framework, evaluate its efficiency and investigate the potential challenges are discussed below.

Developing protocols and security controls- We will initially design fast and reliable V2V and V2I communication protocols to enable real-time interactions between the TMC and the vehicles. Security controls should also be developed to prevent misuse of the emergency service. These controls need to be configurable to be adjusted depending on the context, especially the emergency level.

Providing the simulation environment- In order to evaluate the effectiveness of the proposed architecture we utilize iTETRIS [2], an open source simulation platform that integrates ns-3 [3] and SUMO [4], in which ns-3 is used to implement the core functionality of the framework. We then apply a set of mobility scenarios using SUMO to simulate different roads environment (Highway, Urban area) under varying levels of traffic congestion, and roads segments with various lengths to measure the dissemination delay and evaluate the scalability of our scheme. To have a realistic simulation, we should consider that some vehicles may lack communication capabilities and assess their impact on the efficiency of inter-vehicles coordination to clear the road for the emergency vehicle.

Investigating alternative data sources- In a realistic test platform, we should consider that there might be faulty sensors or failed traffic control equipment in the TMS. Therefore, the system needs to consider alternative ways to glean domain data. One idea is to use a mobile sensing approach in which a mobile application can send traffic data to the TMS. Data collection, in this context, can be opportunistic or participatory. In the former, the application is allowed to send information automatically, while in the latter users decide to report events voluntarily.

Alternative data sources are also useful in adaptive security. For instance, sometimes the system may not be able to verify an emergency case from corresponding authorities in a reasonable time. In this case, the system may match location and other data from user profile with the car data and other information to verify the emergency case. This is certainly a weaker verification, but it is better

than rejecting the request, which may be genuine, or allow the driver to benefit from traffic adjustment without any verification.

Investigating system and human adaptation scenarios- The proposed framework of traffic management for emergency services is sociotechnical. Therefore, to satisfy security and performance requirements, not only the system but also drivers should adapt their behaviour. System adaptation is actuated through traffic lights and other elements of TMS, and drivers are steered by recommending to change their route, speed or pulling over. We plan to investigate how these two types of adaptation actions could complement each other, or in other words, how we can gain maximum benefit from the combination of these two.

Selecting a proper decision-making mechanism- Recommending an alternative route to drivers is not a new problem, but in this paper we are looking for a fast mechanism that takes into account real-time contextual factors and security constraints to apply and recommend a variety of adaptation actions. We plan to investigate optimization techniques and Artificial Intelligence search algorithms to find the best possible solution.

Two significant points should be taken into account when adapting the behavior of TMS and people: first, the emergency incident response is not just speeding up the emergency team access to the affected area. The affected area may also need traffic regulation to protect citizens and their valuable assets in case of fire or security incidents (e.g., hostage taking). Second, the emergency affected area may not be fixed. For example, consider when police cars chasing a car in the city. In this case safety and security of citizens on the route are also important.

V. Related work

A recent survey points out that the efficiency of emergency services can be improved by V2V and V2I communications [17]. In this context, a number of approaches have been proposed, such as the proposals reported in [20] and [21], in which the main focus was on incident detection, alert message dissemination, and emergency notification, whereas the secure mechanisms ensuring in-time emergency service delivery were out of consideration. In [18], the authors have proposed an adaptive system, for disseminating warning messages, which can dynamically update the key parameters by taking into account the features of roadmap, so that dissemination latency can be minimized. Other approaches have been also designed to disseminate traffic information in vehicular networks through multi hop broadcasting. This latter technique is very appropriate for safety applications, such as inter-vehicles coordination in which non emergency vehicles change road lanes to clear one specific lane for an emergency vehicle, or adapt their speeds according to the new driving policies advertised by the LTC.

In [7], a broadcasting algorithm that relies only on the local topological knowledge is designed to deal with network disconnection and broadcast storm problems. A cooperative forwarding scheme is also introduced in [8] where multiple forwarding vehicles with different delays are proposed to ensure wide and fast spread of an emergency message in a given area. In addition, 2-hop beaconing mechanism has been proposed, where a vehicle has to learn the topology in its surrounding in order to perform an opportunistic forwarding. This forwarding technique is based on the chosen best target forwarder as described in [9]. Furthermore, a reliable beaconing technique has been investigated in [10]. The main challenge for all of these beacon systems is their sensitivity to environmental conditions like vehicle density and network load. Besides, the scalability criterion must be investigated in order to make the system viable in real scenarios [11].

Adaptive software research body offers different solutions for dynamically changing architecture [19], behaviour and parameter in software systems at runtime [14]. These solutions address performance, reliability and security issues of variety of applications. In particular, adaptive security and self-protection research has considered two aspects [13]: defending against malicious attacks and cascading failures, and anticipating problems and avoiding them. In this paper, we focus on "proactive security" that is related to the anticipation and prevention aspect. Proactive security has been addressed by few efforts on risk-adaptive approaches (e.g., [15]), but risk is not the only factor influencing the selection of an appropriate security configuration. The authors of [12] proposed a requirements-driven approach to represent security, performance and other quality requirements at runtime in addition to risk and to adapt security controls.

VI. Acknowledgement

This work was supported, in part, by Science Foundation Ireland grant 10/CE/I1855 to Lero - the Irish Software Engineering Research Centre (www.lero.ie).

References

[1] National Highway Traffic Safety Administration, www.nhtsa.gov
[2] iTETRIS project, http://ict-itetris.eu/
[3] ns-3 network simulator, http://www.nsnam.org/
[4] SUMO: microscopic traffic simulator, http://sumo.sourceforge.net/
[5] P. Savolainen, T. Datta, Evaluation of an Innovative Vehicle Alert System (EVAS), Report to Federal Highway Administration, Washington DC, 2007.
[6] 802.11p-2010 - IEEE Standard for Information technology– Local and metropolitan area networks– Specific requirements– Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments.
[7] O. K. Tonguz, N. Wisitpongphan and F. Bai, DV-CAST: A Distributed Vehicular Broadcast protocol for Vehicular Ad hoc Networks, IEEE Wireless Communications, vol. 17, no. 2, pp. 47-57, April 2010.
[8] S. Bai, Z. Huang , D. Kwak, S. Lee, H. Oh and J. Jung, Vehicular multi-hop broadcasting protocol for safety message dissemination in VANETs, In Proc. of the 70th IEEE Vehicular Technology Conference Fall (VTC 2009-Fall), Anchorage , AK, 2009.
[9] K. Lee, U. Lee, and M. Gerla, Geo-Opportunistic Routing for Vehicular Networks, IEEE Communications Magazine, vol. 48, no. 5, pp. 164170, May 2010.
[10] F. J. Ros, P. M. Ruiz, and I. Stojmenovic, Reliable and Efficient Broadcasting in Vehicular Ad Hoc Networks, In Proc. of IEEE VTC2009-Spring, Barcelona, Spain, April 2009.
[11] B. Scheuermann, C. Lochert, J. Rybicki, and M. Mauve, A Fundamental Scalability Criterion for Data Aggregation in VANETs, In Proc. of ACM MobiCom09, Beijing , China, September 2009.
[12] Salehie, M., Pasquale, L., Omoronyia, I., Ali, R., and Nuseibeh, B. (2012) Requirements-driven adaptive security: Protecting variable assets at runtime. In: 20th IEEE International Requirements Engineering Conference, 24-28 Sept 2012, Chicago, ILL, USA.
[13] Kephart, Jeffrey O., and David M. Chess. "The vision of autonomic computing." Computer 36, no. 1 (2003): 41-50.
[14] Salehie, Mazeiar, and Ladan Tahvildari. "Self-adaptive software: Landscape and research challenges." ACM Transactions on Autonomous and Adaptive Systems (TAAS) 4.2 (2009): 14.
[15] Covington, Michael J., et al. "Securing context-aware applications using environment roles." Proceedings of the sixth ACM symposium on Access control models and technologies. ACM, 2001.
[16] S. Djahel and Y. Ghamri-doudane, "A Robust Congestion Control Scheme for Fast and Reliable Dissemination of Safety Messages in VANETs", *In Proc. of IEEE WCNC*, Paris, France, April 1-4, 2012.
[17] F.J. Martinez, C.-K. Toh, J.-C. Cano, C.T. Calafate, P. Manzoni, "Emergency Services in Future Intelligent Transportation Systems Based on Vehicular Communication Networks", *IEEE Intelligent Transportation Systems Magazine*, vol. 2, no. 2, pp. 6-20, 2010.
[18] M. Fogue, P. Garrido, F. J. Martinez, J.-C. Cano, "An Adaptive System Based on Roadmap Profiling to Enhance Warning Message Dissemination in VANETs", *IEEE/ACM Transactions on Networking*, 2012.
[19] P. Jamshidi, M. Ghafari, A. Ahmad and C. Pahl, "A Framework for Classifying and Comparing Architecture Centric Software Evolution", *CSMR*, Genova, Italy, March 5-8, 2013.
[20] European Commission eSafety Initiative, http://ec.europa.eu/information_society/activities/esafety/index_en.htm
[21] OnStar by GM, http://www.onstar.com/xl