Trusted Information and Security in Smart Mobility Scenarios: the case of S^2-Move project*

Pietro Marchetta[1], Eduard Natale[1], Alessandro Salvi[1], Antonio Tirri[1], Manuela Tufo[2], and Davide De Pasquale[2]

[1] University of Napoli - Federico II, Via Claudio 21, 80125 Napoli (Italy)
{pietro.marchetta, alessandro.salvi}@unina.it
{ed.natale, an.tirri}@studenti.unina.it
[2] University of Sannio, Piazza Guerrazzi 1, 82100 Benevento (Italy)
manuela.tufo@unisannio.it, davide.depasquale@studenti.unisannio.it

Abstract. Smart cities and smart mobility represent two of the most significative real use case scenarios in which there is an increasing demand for collecting, elaborating, and storing large amounts of heterogenous data. In urban and mobility scenarios issues like data trustiness and data and network security are of paramount importance when considering smart mobility services like real-time traffic status, events reporting, fleets management, smart parking, etc. In this architectural paper, we present the main issues related to trustiness and security in the S^2-Move project in which the contribution is to design and implement a complete architecture for providing soft real-time information exchange among citizens, public administrations and transportation systems. In this work, we first describe the S^2-Move architecture, all the actors involved in the urban scenario, the communication among devices and the core platform, and a set of mobility services that will be used as a proof of the potentialities of the proposed approach. Then, considering both architecture and the considered mobility services, we discuss the main issues related to trustiness and security we should taken into account in the design of a secure and trusted S^2-Move architecture.

1 Introduction

Today more than 50% of people around the world live in an urban area and by 2050 this percentage will grow up to 70%[1]. While cities are becoming more and more the center of the economic, political and social life, an efficient, effective and secure mobility remains a non-trivial key challenge to face. In this new social scenario, the citizen has the opportunity to share geo-referenced information acting such as human sensors network thanks to a deep interconnected network. This innovative citizen-centric vision of the city is behind S^2-Move [2, 3], a 36-months long project funded by MIUR, started in June 2012. The aim of the

* The activities described in this paper are funded by MIUR in the field of Social Innovation of the program with the grant number PON04a3_00058. We would like to thank (i) University of Napoli Federico II for providing SincroLab and ArcLab laboratories for lodging some S^2-Move activities; (ii) the industrial partners collaborating in the project; (iii) Dario Di Nocera, Antonio Saverio Valente, and Luca Iandolo for their valuable work and support.

project is to create a link between the digital and the real world, changing the way in which cities interact with the population. To provide the previous opportunity a number of challenges arose when considering trustworthiness and security of a smart mobility scenario both as a black box and as related to each technological brick [4]. For example, issues related to users privacy [12], secure communications among all the entities involved in the S^2-Move scenario (users, cars, devices, etc) [9, 10], vehicular and ad hoc networks security [25–32], cyber attack events involving malware/worms [5, 6] and botnets [7, 8], cloud infrastructures [11]. In this architectural paper, we first briefly describe the S^2-Move architecture, then considering both architecture and mobility services, we discuss the main issues related to trustiness and security we have taken into account in the design of the S^2-Move architecture.

2 S^2-Move

The main idea of S^2-Move is to supply soft real-time information exchange among citizens, public administrations and transportation systems. S^2-Move uses customized maps as the most user-friendly and intuitive approach to supply urban mobility services based on urban probes real-time information.

Urban probes represent a heterogeneous set of devices/sensors deployed in the urban environment to detect different real-time information. They range from simple sensors to sophisticated devices, such as smartphones or tablets. S^2-Move exploits urban probes as well as a new prototype of On Board Unit (OBU). This is a smart electronic device, connected with the vehicle CAN bus, able to collect in-vehicle information (e.g. speed, pedals pressure, fuel consumption, etc.) as well as to process data and to communicate with a Central Processing System (CPS)[3]. The OBU is also responsible for both vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications. Crossing the data provided by multiple sources of information the S^2-Move system can both monitor the urban environment and provide services to the citizens and the social community. CPS is the S^2-Move architecture core and it is composed by three main layers: *data layer* (responsible for data storage and low-level computation); *core layer* (to manage user authentication, customized maps, data exchange with the urban probes and raw data preservation); *presentation layer* (for the interaction among final users and administrator).

While the platform can be easily used to provide a widespread of urban information-based services, the project currently focus on two exemplar case of study: traffic monitoring and fleet management. Traffic monitoring aims at determining real-time knowledge of traffic jam exploiting the information collected from the urban environment. Note that, traditional traffic monitoring systems are based on data collected through heterogeneous sensors [13] (inductive loops, magnetic sensors, video cameras, infrared sensors, etc.). The usage of those sensors is very expensive, hence new monitoring technologies, based on GPS have

[3] While the CPS represents a single logic unit, it is distributely implemented for coping with scalability and robustness issues

been recently proposed [13, 14]. The S^2-Move aims to implement traffic monitoring services by using GPS and information provided by the OBU devices to infer the traffic condition by observing the speed of the monitored vehicles along the urban routers. To this end, a data collection module hosted on the OBU device samples and filters kinematics information coming from the CAN bus. Once collected and filtered, data is sent to the CPS where they are processed to infer the traffic information [14]. Fleet management has two main aims: Fleet Monitoring and Fleet Control. Fleet monitoring can be meant as the tracking of a group of vehicles moving in the urban environment. Fleet Control allows the coordinate motion of a group of vehicles traveling with a common velocity and a predefined intra-vehicular distance (platooning [15]). Platooning is based on the design of decentralized control algorithm that funds on reliable V2V and V2I communication. To this aim heterogeneous wireless communication technologies and their performance must be carefully taken into account [16–19]. A first attempt to platooning design within the S^2-Move context is described [2, 3], while the design of more sophisticated control approaches embedding adaptive mechanisms [20–23] is currently under development.

3 Trusted Information and Security in S^2-Move: an architectural view

In this section we first review both (a) secure and trusted fleet and traffic management and (b) users and vehicles communications privacy, then we describe an architectural solution we should follow in the S^2-Move project.

Secure and Trusted Fleet and Traffic Management. There are different kinds of attacks, performed against the exchanged messages. In [25], authors analyzed different types of attacks, including *Fabrication Attack*, *Replay Attack* and *Sybil Attack*. During a *Fabrication Attack*, false information is transmitted. In this case, for example, a vehicle belonging to the fleet can change the speed of the fleet itself or other parameters of cruise. In addition, a malicious agent can create problems in traffic management reporting vehicle collisions that are not true, or signaling a free road, in presence of an incident, to aggravate the situation. In [24], authors described the IEEE 1609.2 protocol for message authentication and security at the data link layer. This protocol uses IEEE 802.11p protocol for data transmission, which does not provide any kind of security, since it is based on a communication outside the BSS (Basic Service Set) context. The IEEE 1609.2 protocol uses a Public Key Infrastructure (PKI). To allow the physical implementation of this type of infrastructure, each vehicle will come with a Trusted Platform Module (TPM) that works with the OBU. In the PKI paradigm, each vehicle is equipped with two keys, one public and one private, and a certificate that proves its identity, validating the public key held. Since TPMs are resistant to software attacks (but not to physical tampering), they are used to ensure the storage of cryptographic keys and certificates, and to implement the required cryptographic mechanisms. In addition to this new hardware device, the implementation of the PKI requires the presence of a Certification Authority (CA) that deals with the release and management of

certificates to the members of the network, vehicles in the case of S^2-Move. This type of infrastructure is able to ensure *Authenticity*, *Integrity* and optionally *Confidentiality* to the messages that are in transit in the network. Moreover, it is possible to prevent different kinds of attacks (like the *Sybil* attack) that may make unusable the traffic management system presented in this work. In fact, in order to perform a *Sybil* attack, a malicious vehicle pretends the presence of a traffic jam, sending out at the same time several messages and using for each of them a different identity. But for each of these identities there is the need to use a valid certificate, making very complex and virtually impossible this type of attacks. The authentication procedure provided by the IEEE 1609.2 protocol operates as follows. If a vehicle wants to send a message in the network, it has to sign it with its private key and then it attaches its certificate provided by the CA. This certificate contains the public key associated with the private key used. In order to sign the message is used the *Elliptic Curve Digital Signature Algorithm (ECDSA)*, an encryption algorithm with 224 or 256 bits asymmetric keys. This algorithm requires a heavy use of computational resources, guaranteed on the vehicle by the TPM mentioned before. The recipient of the message will reach the sender's public key using the certificate attached to the message. To verify the authenticity of the certificate, the recipient will see, using the public key of the CA, the signature contained in the authentication of the certificate, signed by the CA with its private key. In the case of information needed for the traffic management, there is no need to make the transmissions confidential, as it would introduce only overhead. The confidentiality of information can become crucial in the implementation of additional features such as vehicle platooning or an online payment system for parking. In this regard, the IEEE 1609.2 protocol also provides an encryption algorithm, given by a combination of symmetric and asymmetric encryption. The symmetric encryption algorithm used is the AES-CCM, while the asymmetric one is the *Elliptic Curve Integrated Encryption Scheme (ECIES)*. [24] However, the use of the IEEE 1609.2 protocol does not guarantee the solution to all the security problems listed above and that arise from the implementation of our project. In fact, the possession of a certificate by a vehicle does not necessarily imply its correct behavior. Moreover, there are also privacy issues. In fact, the use of certificates, even if multiples, makes the vehicle recognition and tracking even easier. As widely reported in [25] it is necessary to combine the IEEE 1609.2 protocol with other mechanisms that can adequately identify suspicious vehicles in order to protect the privacy of the users. In cases in which a vehicle performs suspicious actions, the CA has the power to revoke its certificate. To do this, it can submit a *Revocation of the Trusted Component (RTC)* to a vehicle requiring the deletion of all the cryptographic material that it keeps in its TPM. In cases where this message does not reach the TPM because the attacker is able to block it, the CA recurs the use of *Certificate Revocation List (CRL)*, a list of all revoked certificates. The CPS will also preserve the CRL and will send it periodically to the *Road Side Unit (RSU)*. Then the RSU will forward it to the vehicles. A vehicle will discard a received message if signed with a revoked certificate.

Users and Vehicles Communications Privacy. Another key issue is to protect the privacy of users that moves in the city and that use S^2-Move vehicles equipped with OBUs. In this case it is possible to follow two different paths: use of aliases or adopting the group keys (signatures) that may be especially effective in the fleet management [26]. The first solution is to associate the certificates to aliases associated with vehicles. Each alias must still be due to the vehicle to enable the authorities to any checks. To ensure this form of anonymity, vehicles must be equipped with the *Electronic License Plate (ELP)* and the CA will associate aliases to the ELP. Therefore, the authorities will be able to trace the identity of the owner of the vehicle through the ELP. The creation of aliases with the associated keys can occur both by the CA and by the vehicle itself. In the first case, the CA will create offline all the necessary information that will be transferred to the vehicle during annual revisions, while in the second case the vehicle will create all the necessary information thanks to the TPM. In fact, the TPM will send the alias and the public key of the CA, which will reply by sending the certificate to the vehicle. The second approach is preferable because the aliases can be changed more frequently and, in addition, the security offered will be greater, as the private key related to the alias will never be disclosed by the TPM. Each vehicle will not be equipped with an individual certificate, but with a large number of certificates, each valid only for a short period. Changing certificate frequently (every 5-10 minutes) ensure greater privacy to the user because the messages appear to come from different sources. Moreover, if an attacker could take the cryptographic information in the TPM of a vehicle, he would have access to a large number of certificates (in the order of 10^5) and could easily lead to a *Sybil* attack without this kind of trick. The second solution is, as previously mentioned, the use of signatures group [27]: the vehicles of the network are divided into groups and each group member has its own secret key together with the public key of the group. A vehicle of the group, instead of authenticate their messages using their private key associated with the certificate, will use its secret key group member. This will protect the anonymity to the members of the group, anonymity that must still be resolved by the competent authorities. To make the anonymity resolvable, there are entities called Group Manager. The Group managers have a group manager secret key, which allows the identification of the message sender. As proposed by [31], a solution can be the use a symmetric structure key to reduce the overhead due to the asymmetric encryption algorithms and eliminate the need to contact the CA for the establishment of asymmetrical group keys. In this approach the group leader (that is the leader of the fleet in our case) is responsible for generating a symmetric key and distribute it to each of the members of the group by encrypting it with their corresponding public keys (previously sent in broadcast with the relevant certificate). At this point, all the members can sign messages with the public key of the group, so that they can make confidential communications. To allow the propagation of the messages between the S^2-Move fleets and provide a mechanism for checking the validity of the information contained in the message, it is necessary that the geographic areas of the groups overlap. In that way, a vehicle

placed in the shared area (the first and the last of the fleet) has the keys of both groups and will send the message to the next group using its key. This is a solution based on symmetric keys and does not provide the message non-repudiation and it is not designed to protect the privacy of users as it allows communication only within the group or with adjacent groups. On the other hand, it allows the management and the creation of groups without the need to contact the CA. To ensure a wide non-repudiation policy for the message, it is necessary to create a unique group key pair (public and private keys) for the whole group by contacting the CA. In that way, the CA will assign each vehicle of the fleet with a recognition ID, which will be included in the message signature. Since the ID is sent in the signature of a message, this kind of implementation does not guarantee the privacy of users, that can only be ensured by the approach previously presented and proposed in [27]. The CA can revoke the certificate to a vehicle in the event of its suspicious behavior. It is necessary, however, an additional security mechanism that allows all vehicles to decide autonomously whether the information received from a vehicle are correct, or if they should be discarded even if it has a valid certificate. They are used trust models that, in vehicular environments, such as the present, which must take into account some factors due to the particular structure of vehicular networks. In [32], authors proposed the assignment of this trustiness value directly to the groups rather than to the individual entities. However, this is not possible as the groups (fleets) in the case of S^2-Move can be short-lived. In practice, data-oriented trust models are used to assign the value of trust directly to the received message and to the information contained therein. In assigning this trust value, it will consider two kinds of factors: a type of factors of the static type, such as a trust value that can be assigned a priori to the sender entity based on the type of vehicle (police car, bus, etc.) and a type of factors of the dynamic type, such as the spatial or temporal proximity to the logged event. By grouping different reports about the same event, and applying the theory of *Dempster-Shafer* taking into account the factors listed above, it will be possible to assess the level of trust of the event in question. Considering separately each event shows off the downside of this approach: as the trust relationships must be evaluated from the scratch for each event, if the network is sparsely populated this model will be inapplicable, having an insufficient number of alerts [28, 29], c. However, it is possible to use hybrid trust models, which mostly provide a mechanism of opinion piggybacking [28, 30].

The case of S^2-Move. The solutions previously described could be profitably applied in S^2-Move. Since the CPS is always available, it can be used as a certification server, in addition to the functionalities of data collection and processing. It would be possible to assign a group key to the fleets that are formed over time. At the same time, the Group Manager (which does not correspond to the leader of the fleet, but acts only as a secure entity) could handle multiple group keys and different fleets in the reference area (via the RSU), allowing the establishment of group member secret keys for each member of the fleet. S^2-Move has been designed in such a way to make the architecture independent from the possible presence of the RSU. While this design choice has brought significant advantages

in terms of extensibility of services offered by the platform freeing the interaction between the actors of the urban landscape by the presence of RSU, the solution proposed in literature based on the RSU, regarding the conservation of CRL lists but also for the groups management, is not currently applicable. An alternative approach would be the preparation of the CRL lists by the CPS (that will be sent to all the vehicles) and the embedding of the Group Management logic within the CPS itself. Moreover, the benefits of an approach based on symmetric-key communications are significant when compared to other implementations presented. In S^2-Move the RSU are not necessarily present, and then the connection to the CPS may not be constant due to the availability of a cellular network. Therefore, in this case, an implementation based on asymmetric keys may create problems in the management of the security of the fleet, which may not be able to get a pair of valid key (being not able to contact the group manager). For this purpose, the following resolving hypothesis is considered: when the network is not available, it is possible to use symmetric keys to ensure the authenticity and integrity of messages transmitted within the fleet. In this way, vehicles not belonging to the fleet cannot send invalid information to the fleet vehicles. At the time when the network becomes available again, matching the Group Manager with the CPS (and consequently with the systems CA), it is possible to ask for the establishment of a group key and private keys for the members of the group, ensuring the anonymity and security in the transmissions.

4 Discussion and Conclusion

Trusted information and security (at different layers) represent really important aspects to carefully consider when designing and planning smart mobility platforms. In this architectural paper we have discussed the S^2-Move architecture, its main components and applications, and we have provided a review of the main challenges related to trusted information and security of the entire architecture. Finally, we have reported some potential solutions to trusted communications and privacy in the S^2-Move architecture and services. Experimental evaluation is left for future work.

References

1. United Nations Department of Economic and Social Affairs Population Division, *World Urbanization Prospects: The 2011 Revision*, 2012.
2. P. Marchetta, et al., *S^2-MOVE: Smart and Social Move*, In IEEE GIIS, 2012.
3. P. Marchetta, et al., *Social and Smart Mobility for Future Cities: the S2-Move project*, AICA 2013.
4. A. Abdullahi, I. Brown and F. El-Moussa, *Privacy in the age of Mobility and Smart Devices in Smart Homes*, PASSAT, SocialCom 2012.
5. Dainotti A., Pescapé A., Ventre G., *Worm traffic analysis and characterization*, IEEE Inter. Conference on Communications (ICC), 2007.
6. S. Colleen and D. Moore, *The spread of the witty worm*, Security & Privacy, IEEE 2.4, 2004.
7. Dainotti A., King A., Claffy K., Papale F., Pescapé A., *Analysis of a /0 stealth scan from a Botnet*, ACM IMC, 2012.

8. Barford P. and Vinod Y., *An inside look at botnets*, Malware Detection, Springer US, 2007
9. Landman M. *Managing smart phone security risks*, Information Security Curriculum Development Conference. ACM, 2010.
10. Chourabi H., et al. *Understanding smart cities: An integrative framework*, HICSS, 2012.
11. J. Wayne and T. Grance, *Guidelines on security and privacy in public cloud computing*, NIST special publication, 2011.
12. Armac I., et al. *Privacy-friendly smart environments*, NGMAST, 2009.
13. B. Barbagli, et al., *A real-time traffic monitoring based on wireless sensor network technologies*, IWCMC, 2011.
14. A. Hadachi, *Travel time estimation using sparsely sampled probe GPS data in urban road network*, Ph.D. Thesis, Normandie University, 2013.
15. J.K. Hedrick, M. Tomizuka and P. Varaiya, *Control issues in automated highway systems*, Control Systems, IEEE 14.6, 1994.
16. M. Bernaschi, F. Cacace, A. Pescape' and S. Za, *Analysis and Experimentation over Heterogeneous Wireless Networks*, TRIDENTCOM '05, 2005, Trento (Italy).
17. G. Iannello, A. Pescape', G. Ventre and L. Vollero, *Experimental Analysis of Heterogeneous Wireless Networks*, WWIC 2004: 153-164.
18. R. Karrer, I. Matyasovszki, A. Botta and A. Pescape', *Experimental evaluation and characterization of the magnets wireless backbone*, WINTECH 2006: 26-33.
19. A. Botta, A. Pescape' and G. Ventre, *Quality of Service Statistics over Heterogeneous Networks: Analysis and Applications*, EJOR, Volume 191, Issue 3, 2008.
20. M. di Bernardo, et al., *Model reference adaptive control of discrete-time piecewise linear systems*, International Journal of Robust and Nonlinear Control 23 (7) , 2013.
21. M. di Bernardo, U. Montanaro, S. Santini, *Canonical forms of generic piecewise linear continuous systems*, IEEE TAC 56 (8), 2011.
22. M. di Bernardo, et al., *Experimental implementation and validation of a novel minimal control synthesis adaptive controller for continuous bimodal piecewise affine systems*, Control Engineering Practice 20 (3), 2012.
23. M. Di Bernardo, U. Montanaro, S. Santini, *Novel switched model reference adaptive control for continuous piecewise affine systems*, CDC 2013, 2008.
24. J. B. Kenney, *Dedicated Short-Range Communications (DSRC) Standards in the United States*, 2011.
25. M. Raya, P. Papadimitratos, I. Aad, D. Jungels, J.-P. Hubaux, *Eviction of Misbehaving and Faulty Nodes in Vehicular Networks*, 2007
26. J. M. de Fuentes, A. I. Gonzalez-Tablas, A. Ribagorda, *Overview of Security issues in Vehicular Ad-hoc Networks*, 2010.
27. L. Malina, J. Hajny, *Group Signatures for Secure and Privacy Preserving Vehicular Ad Hoc Networks*.
28. M. Raya, P. Papadimitratos, V. D. Gligor, J. Hubaux, *On Data-Centric Trust Establishment in Ephemeral Ad Hoc Networks*, 2007.
29. J. Zhang, *A Survey on Trust Management for VANETs*, 2011.
30. F. Dotzer , et al., *VARS: A Vehicle Ad-Hoc Network Reputation System*, 2005.
31. M. Raya, A. Aziz, J. Hubaux, *Efficient Secure Aggregation in VANETs*, 2006.
32. A. Tajeddine, A. Kayssi, A. Chehab, *A Privacy-Preserving Trust Model for VANETs*, 2010.