CS7NS5 – Security and Privacy

Assignment 1 – Security and Privacy Considerations in Dissertation Topic

By: Pallavit Aggarwal (MSc Intelligent Systems 2022-2023)
Email: aggarwpa@tcd.ie

On Dissertation Topic

Topic Abstract:

The topic for my dissertation is about exploring mobility in IoT devices when they're both producers and consumers of services. IoT devices are usually considered as consumers and at the edge of the infrastructure (edge devices, low powered), receiving or transmitting information across the service mesh and the servers or producers are hosted either centrally or in a distributed manner across the defined infrastructure. But now, with the increase in the compute and the decrease in latency along with some other technical upgrades in terms of power for example, these edge devices can also host services and become producers interchangeably. This provides more flexibility to the entire service grid and the IoT infrastructure.

Though mobility can be explored in multiple ways, my take on it for the dissertation is in the form of Vehicular Fog Computing.

The Professor and Supervisor for my dissertation is Prof. Siobhán Clarke.

Vehicular Fog Computing:

With the evolving nature of vehicles, Internet of Vehicle – based Intelligent transportation systems are expected to become widespread to support real-time video aided navigation, autonomous driving, accident avoidance, traffic and road condition monitoring, infotainment services and sharing of media and other new and upcoming value-added services for vehicles.

A VFC can also be very useful to aid the response to an emergency and orchestration of emergency response in a situation thereby fulfilling the smart city vision as well.

Vehicles and high-computing infrastructures such as roadside units (RSUs) can use vehicle-to vehicle (V2V) and vehicle-to-infrastructure (V2I) communication to contribute their resources to the network via the Dedicated Short-Range Communication (DSRC). The goal of VFC is to relocate communication, computing, and storage resources close to vehicular users. VFC, therefore, plays an important role in addressing the exponential growth in edge device requirements through high bandwidth and low latency.

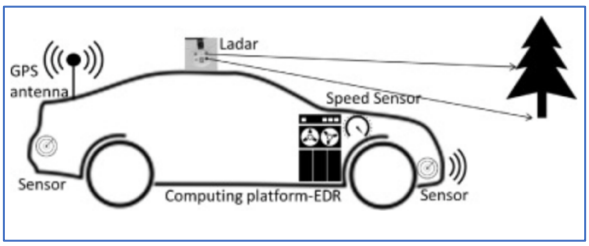

Fig 1: Conceptualization of hardware on Vehicle

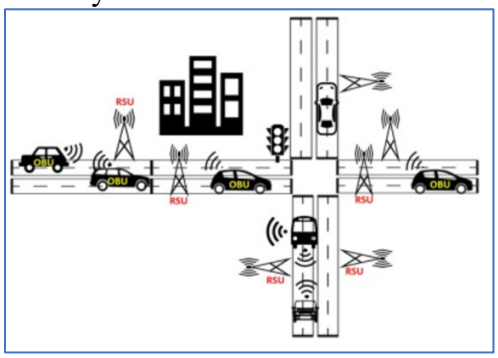

Fig 2: Conceptualization of City Network with different component

On Security and Privacy Considerations

○ Infrastructure Definition:

To discuss the security and privacy aspects of the V2V (vehicle to vehicle) or V2I (vehicle to infrastructure) we first need to understand the actors and define a general architecture for the communication between the devices and the actors in play.

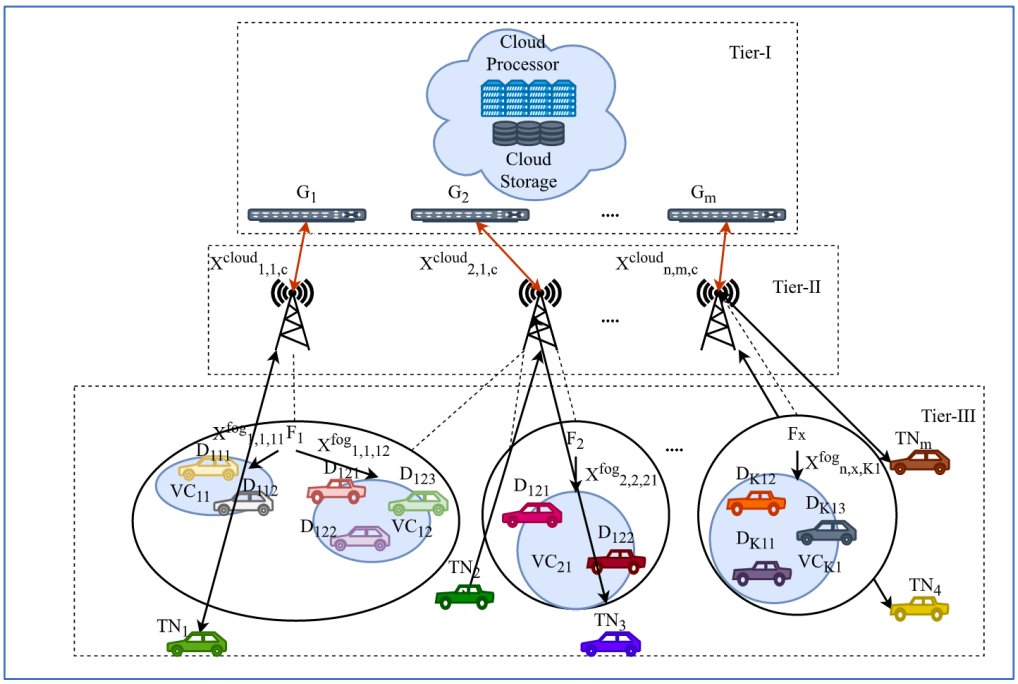

Fig 3: Architecture of a VFC

In the 3-tier architecture above the key components and actors are:

a) *Vehicle/End-User/Terminal* – These are abbreviated as TN. In VFC, vehicular terminals are mainly represented by vehicles. Rather than ordinary mobile nodes, vehicles have the following prominent features: 1) sensing: vehicles can sense the environment from both inside and outside and are able to collect various information using the equipped vehicular devices, including cameras, radars, Global Positioning System (GPS), etc.; 2) communicate: vehicles can exchange and share information with other vehicles or RSUs using V2V and V2R communication manners; 3) computing: in addition to transferring parts of computation tasks to the edge servers or the cloud for processing, vehicles can execute parts of the tasks locally by themselves; 4) storage: the idle storage space of vehicles can be used to cache popular contents for data sharing.

b) *Virtual Cluster of nodes* – The small transparent blue colored circles inside the bigger circle denote the virtual cluster nodes of a TN region that changes dynamically because of nodes entering and leaving it.

c) *RSU nodes* – While there is V2V interaction in the virtual cluster nodes, the entire architecture requires RSUs which finally connect to the main cloud servers. RSUs often act as edge servers in VFC, which are distributed along the road in a city. They have rich communication, computation and storage resources compared to vehicles. RSUs are responsible for receiving the information sent from vehicles, processing these collected information, and even uploading this information to the cloud. By computation offloading and

caching technologies, RSUs are beneficial for handling strict performance requirements. Besides, they can also provide diverse services for vehicles, such as video streaming, traffic control, path navigation.

d) *Main cloud servers*: Cloud services are deployed in a remote cloud. They can get the uploaded information from edge servers. Compared with edge servers, cloud services have rich capacities in terms of computation and storage, and cover a much broader area. By getting the uploaded information from mobile nodes and edge servers, they can have a global view of the covered area. The cloud paradigm can provide global level management and centralized control, which helps in making optimal decisions.

VFC Characteristics – in continuation to the infrastructure definition:
The communication modes in VFC shown in figure above can be categorized into Vehicle to Vehicle (V2V), Vehicle to Infrastructure (V2I) and Hybrid. In V2V, the used communication media is characterized by short latency and high transmission rate. This architecture is used in different scenarios of broadcasting alerts or in a cooperative driving. In V2I, vehicular network takes into account the applications that use the infrastructure points RSUs which multiply the services through internet portals in common. Hybrid mode is a combination of the two previous techniques.

i) VFC characteristics related to Network Topology and Communication Mode:

- *Wireless Communication*: the nodes connection and their data exchange are done via wireless channels. Thus, requires securer communication.
- *High mobility and rapidly changing network topology*: nodes are moving at high/random speed which make harder to predict their position and the network topology. This enhances the node's privacy but also causes frequent disconnection, volatility and impossibility of handshake. It also lacks the long-life context (eg: password) which is impractical for securing vehicular communication. A fast cryptographic algorithm or entity authentication is needed.
- *Reliability* and *Cross Layer* between network and transport layers to support real-time and multimedia applications.

ii) VFC characteristics related to vehicles and drivers:

- *High processing power and sufficient energy*: VANET nodes have no issue of energy and computation resources. They have their own power in the form of batteries and high computing powers to run complex cryptographic calculations.
- *Better physical protection:* The edge devices could be deeply embedded in the car's engine or front dashboard area and breaking into it would require breaking into the car in the first place, which is possible but very tedious without getting noticed.
- *Known time and position*: Most vehicles are equipped with GPS because many applications rely on position and geographical addressing or area. A tamper proof GPS can be used for secure localization to protect node's location against attackers.
- *Central registration with periodic maintenance and inspection*: Vehicles are registered with central authority and have unique id (license plate). Vehicles periodic maintenance is for firmware and software updates. In PKC (Public key Cryptography), maintenance can include updating certificates, keys and obtaining fresh CRL (Certificate Revocation List).

A critical concern is the security of the vehicle in VFC. The concept of intelligent transportation systems, which entails using automated vehicles on public roads, introduces the possibility of hackers gaining access to networked vehicles' controls and causing

accidents. Apart from that, data can be stolen through the interception of network-wide communications, for instance, emergency messages or pooled data used for computation offloading. As a result, safety has emerged as a primary concern of message propagation in a vehicular network.

○ Security & Privacy Definition:

Some common security & privacy requirements are:

- Confidentiality: Confidentiality is a key requirement of fog computing, as it ensures that private data is accessible only to the data owner and authorized users. The protection of private data from unauthorized users is required in VFC whenever it is received on edge, transmitted from the fog networks, and stored in fog or cloud data centers.

- Integrity: When a vehicle offloads a task to the fog, the data must be consistent and accurate during delivery, which means integrity must be ensured from undetected data modification from unauthorized users. If there is the absence of proper auditing, then it may cause compromised users' privacy.

- Availability: The term "availability of fog computing resources" refers to the ability of all authorized parties to access cloud and fog computing resources at any time and from any location specified by users. Additionally, this enables the processing of encrypted user data in cloud or fog data centers in order to comply with a variety of operational requirements.

- Authentication and access control: Authentication is the process of verifying the identity of a user in a vehicular fog environment (such as a service-providing vehicle, service requesting a vehicle, cloud data centers, etc.). Additionally, access control acts as a clearinghouse for all of the control strategies at the 3-tier structure; it establishes fog has access to the tools (authentication) and what types of activities (authorization), such as writing (integrity) and reading (confidentiality), can be performed.

- Availability: by resisting to DoS (Denial of Service), we assure normal functioning because even a delay of a second makes the message meaningless

Threats to the Communication Interface:

- Identity and geographical position revealing (Location Tracking): an attacker tries to get info of the driver and trace him. This exposes a certain node at risk. For example, a car rental company that wants to follow in an illegitimate manner its own vehicles. Users will be tracked and no privacy preserving.

- DoS: an attacker tries to make the resources and the services unavailable to the users in the network. It is either by jamming the physical channel or by "Sleep Deprivation".

- DDoS (Distributed Denial of Service): it is a DoS from different locations.

- Sybil Attack: an attacker creates multiple vehicles on the road with same identity. It provides illusion to other vehicles by sending some wrong messages for the benefits of this attacker.

- Malware: an attacker sends spam messages in the network to consume the network bandwidth and increase the transmission latency. It is difficult to control this kind of attack, due to lack of necessary infrastructure and centralized administration. Attacker disseminates spam messages to a group of users. Those messages are of no concern to the users just like advertisement messages.

- Spam: an insider node transmits spam messages to increase transmission, latency and bandwidth consumption.

- Man in the Middle Attack (MiM): a malicious node listens to the communication established between two other vehicles. It pretends to be each one of them to reply to the other. It injects false information between them.

- Brute force Attack: is a trial-and-error method an attacker uses to obtain information such as a user password or personal identification number or to crack encrypted data, or to test network security.

- Black Hole Attack: a malicious node declares having the shortest path to get the data and then routes and redirects them. The malicious node is able to intercept the data packet or retain it. When the forged route is successfully established, it depends on the malicious node whether to drop or forward the packet to wherever he wants.

Threats to the Hardware and Software:
In addition to DoS, Sybil attack, Malware and Spam, MiM, Brute force mentioned above we can list:

- Injection of erroneous messages (bogus info): an attacker injects intentionally falsified info within the network. It directly affects the users' behavior on the road. It causes accidents or traffic redirection on the used route.
- Message Suppression or alteration: attacker drops packet from the network or changes message content. In addition to Fabrication Attack where new message is generated. Or Replay Attack by replaying old messages or Spoofing and Forgery attacks that consist of injection of high volume of false emergency warning messages for vehicles. Or Broadcast tampering in which attacker injects false safety messages into the network to cause serious problems.
- Usurpation of the identity of a node (Spoofing or Impersonation or Masquerade): an attacker tries to impersonate another node. To receive his messages or to get privileges not granted to him. Doing malicious issues then declaring that the good one is the doer.
- Tampering Hardware: during yearly maintenance, in the vehicle manufacturer, some malicious employees try to tamper the hardware. Either to get or put special data.
- Routing Attack: an attacker exploits the vulnerability of the network layer, either by dropping the packet or disturbing the routing. It includes in addition to the Black Hole Attack:
  - Wormhole attack: Overhearing data; an attacker receives packets at a point targeted via a tunnel to another point. He replays it from there.
  - Greyhole attack: a malicious node misleads the network by agreeing to forward the packets. But sometimes, he drops them for a while and then switches to his normal behavior.
- Cheating with position info (GPS spoofing) and tunneling attack: hidden vehicles generate false positions that cause accidents. GPS doesn't work.
- Timing attack: Malicious vehicles add some timeslots to the received message, to create delay before forwarding it. Thus, neighboring vehicles receive it after they actually require, or after the moment when they should receive it.
- Replay attack: malicious or unauthorized users try to impersonate a legitimate user/RSU by using previously generated frames in new connections.

Research work being done on security issues:

Many groups in Europe and USA build their own security architectures based on PKI. In Europe (EU), ETSI in [1] define its security architecture for ITS (Intelligent Transport System) communications security management.

Many researchers investigated many techniques to maintain participants' privacy within VFC [2]. It can be ensured by a set of anonymous keys changing according to the driving speed or via pseudonyms that cannot be linked to the true identity of the user or the vehicle.

ETSI standard in [3] specifies the privacy management for a node based on anonymity, unobservability, pseudonyms, and unlinkability. The communication between nodes is done using the SA (Security Association) and key management.

Tracking and eavesdropping can be mitigated by encrypting the data. The security architecture for V2V and V2I communication adopted in succeeded to protect privacy of the participants and were very efficient in terms of computing capabilities and communication bandwidth using the asymmetric and symmetric cryptography and tamper resistant hardware.

To prevent DOS attacks Tesla++ [5] is an authentication method used as effective alternative to signatures. It uses symmetric crypto with delayed key disclosure. It secures and prevents memory-based DoS attack. It also reduces the memory requirement at the receiver end for authentication mechanism.

For sybil attacks, [6] uses PKI for key distribution and revocation which validates entities in real time directly or indirectly. For Man in the middle attack use of strong authentication methods such as digital certificates and confidential communication with key or powerful cryptography [7]. Include several authentication schemes mentioned in [8] where anonymity, pseudonyms, trust and privacy are ensured via short-lived keys changing frequently and RSU used for authentication and key distribution.

Use similarity algorithm [9], data correlation and challenge response authentication methods to prove the reliability of the messages. In [9] authors propose a trust and reputation management framework based on similarity algorithm and trust of messages content between vehicles to help driver to believe or not a received message. By calculating the trust value if it surpasses a threshold, they take appropriate action and rebroadcast the message. Otherwise, they drop it.

The RSU-aided message authentication scheme, called RAISE, proposed in [10] offloads the overhead involved in message authentication to RSUs. This requires dense deployment of RSUs. Vehicles establish a shared key with the RSU using Diffie Hellman algorithm.

Most of the research work on secure incentive schemes focus only on cooperative packet forwarding; but due to the high mobility of vehicles, packets could be lost. To address this problem authors in [11] propose a Secure Incentive scheme for Reliable Co-operative downloading in highway VANETs (SIRC) that uses two phases, namely, cooperative downloading and cooperative forwarding which encourage vehicles to cooperate through an incentive scheme; SIRC utilizes aggregated Camenisch-Lysyanskaya (CL) signature to cooperate with others in securely downloading-and-forwarding packets. In this scheme, a reputation system is implemented to reward the cooperating vehicles and punish the malicious vehicles. In addition, a partial prepayment strategy is used to minimize the payment risk to client vehicles. This scheme can resist various attacks such as free riding attack, DoS attacks

and packet injection/removing attack. The performance evaluation of SIRC shows that it has high download success rate, low download delay, and moderate computation and communication overhead. A disadvantage of this approach is that the reputation information about vehicles which have high variability in their spatial distribution need to be calculated and stored.

- **Privacy Definition:**

  Interpretation of privacy is not very different from the above discussion on security. But a separate mention of privacy as a topic is necessary. This is because ensuring the privacy of vehicles is an important issue in VFC. Otherwise, vehicle owners' life could be jeopardized. So, in all communications, a vehicle should not use its real identity. To solve this problem, several solutions have been proposed. A vast majority of the solutions proposed use pseudonyms instead of the real ids of vehicles in the communication. This requires large number of pseudonyms to be loaded into the vehicles OBUs and they need to be kept secret. Moreover, to punish malicious vehicles (i.e., vehicles disseminating malicious messages or modifying the messages sent by other vehicles), vehicles' real ids need to be traced. Thus, even though privacy needs to be preserved, authorities should still be able to trace and punish malicious vehicles.

  Vehicles cannot use the same pseudonym for a long time, because then, based on the path traversed by vehicles, an intruder can associate the pseudonym with the real id. Thus, pseudonyms should be changed frequently. Some authors suggest changing pseudonyms every five seconds to prevent an intruder from linking two messages to the same vehicles and tracking the vehicle. So, each vehicle needs to be assigned millions of pseudonyms during its lifetime and also a scalable mechanism for tracking which vehicle has been assigned what pseudonym needs to be designed and implemented. Moreover, when a vehicle is revoked, the certificates associated with the pseudonyms of the revoked vehicle need to be disseminated to all vehicles/RSUs. This could lead to an exponential growth of CRLs which could slow down the authentication of messages. So, centralized solutions are not scalable. Some solutions proposed for handling this problem allow the distribution of the task of creating and distributing the certificates as well as CRLs to the RSUs. However, more research needs to be done in devising highly efficient, scalable privacy-preserving methods to solve this problem

  Location privacy has been becoming more and more important in vehicular networks due to a large amount of data sharing, especially with the emergence of location sharing applications, e.g., Google Maps. A vehicle can be easily tracked by its adversary based on its communication and movement behaviors. Vehicles need to send their driving information to neighbors for safe driving and expose their location information because of the utilization of location-based services. An adversary is able of locating the vehicle' position once obtaining this information.

On Future Works and Concluding note

The entire concept of Vehicular fog computing relies on the latency of message processing and energy consumption of these devices. These metrics are often characterized under the QoS evaluation of VFC and there is ongoing research to improve the QoS of these devices. I mention this because it is a tradeoff between proper security implementation and the latency and energy consumption and other soft QoS parameters that it might affect due to key size and other headers in the message relays. Providing a flexible security scheme to guarantee the QoS of different applications based on their priorities is the ideal way going forward. Safety applications (e.g., collision avoidance and traffic control) have strict delay requirement, which should be addressed as soon as possible, while several non-safety applications (e.g., multimedia downloading) can tolerant some delay.

Another important aspect is scalability of the infrastructure and security techniques. It is crucial to conduct security management optimally while taking into account the heterogeneous nature of the users, vehicles and networks.

Conventional schemes of providing C-I-A may not be valid in case of FOG and newer faster schemes would be required to enable this infrastructure.

References

[1] Serban, A.C., Poll, E., Visser, J. (2018). A Security Analysis of the ETSI ITS Vehicular Communications.

[2] Kaushik, Sapna S. "Review of different approaches for privacy scheme in VANETs." International Journal of Advances in Engineering & Technology 5.2 (2013): 356.

[3] ETSI TS 102 941 V1.1.1- ITS, Security- Trust and Privacy Management.

[4] Plößl, Klaus, and Hannes Federrath. "A privacy aware and efficient security infrastructure for vehicular ad hoc networks." Computer Standards & Interfaces 30.6 (2008): 390-397.

[5] Dahiya, Arzoo, and Vaibhav Sharma. "A survey on securing user authentication in vehicular ad hoc networks." International Journal of Information Security 1 (2001): 164-171.

[6] Rao, Ashwin, et al. "Secure V2V communication with certificate revocations." 2007 Mobile Networking for Vehicular Environments. IEEE, 2007.

[7] La, Vinh Hoa, and Ana Rosa Cavalli. "Security attacks and solutions in vehicular ad hoc networks: a survey." International journal on AdHoc networking systems (IJANS) 4.2 (2014): 1-20.

[8] Song, Lu, Qingtong Han, and Jianwei Liu. "Investigate key management and authentication models in VANETs." 2011 International Conference on Electronics, Communications and Control (ICECC). IEEE, 2011.

[9] Caballero-Gil, P. "Security issues in VANET." CAR, 2011.

[10] C. Zhang, X. Lin, R. Lu, P. Ho, RAISE: an efficient RSU-aided message authentication scheme in vehicular communication networks, in: Proceedings of IEEE International Conference on Communications (ICC), IEEE, 2008, pp. 1451–1457.

[11] C. Lai, K. Zhang, N. Cheng, H. Li, X. Shen, SIRC: a secure incentive scheme for reliable cooperative downloading in highway VANETs, IEEE Trans. Intell. Transp. Syst. 18 (6) (June 2017) 1559–1574.

SURVEYS:
[12] Liu, L., Chen, C., Pei, Q. et al. Vehicular Edge Computing and Networking: A Survey. Mobile Netw Appl 26, 1145–1168 (2021). https://doi.org/10.1007/s11036-020-01624-1

[13] Keshari, Niharika, Dinesh Singh, and Ashish Kumar Maurya. "A survey on Vehicular Fog Computing: Current state-of-the-art and future directions." Vehicular Communications 38 (2022): 100512.

[14] Chbib, Fadlallah, et al. "A secure cross-layer architecture for reactive routing in vehicle to vehicle (V2V) communications." Vehicular Communications 38 (2022): 100541.

[15] Manivannan, Dakshnamoorthy, Shafika Showkat Moni, and Sherali Zeadally. "Secure authentication and privacy-preserving techniques in Vehicular Ad-hoc NETworks (VANETs)." Vehicular Communications 25 (2020): 100247.

[16] Hasrouny, Hamssa, et al. "VANet security challenges and solutions: A survey." Vehicular Communications 7 (2017): 7-20.