ITEA Office
High Tech Campus 69 - 3
5656 AG Eindhoven
The Netherlands
T + 31 88 003 6136
E info@itea3.org
W www.itea3.org

ITEA 3 is a EUREKA strategic ICT cluster programme

Exploitable Results by Third Parties

ITEA2 11037 CarCoDe

Platform for Smart Car to Car Content Delivery

Project details

Project leader:	Arthur Lallet
Email:	arthur.lallet@airbus.com
Website:	http://www.cister.isep.ipp.pt/itea2-carcode/

An Itinerary Planning application service for Smart Cities		
Input(s):	Main feature(s)	Output(s):
▪ Source address ▪ Destination address ▪ Vehicle brand ▪ Passengers number ▪ Vehicle mass ▪ Traffic information	▪ Based on real time information from the network and data from Internet API's, the fuel consumption of a route is calculated during a trip. ▪ A set of algorithms is proposed to extract and analyze collected data for fuel process calculation aim. ▪ Weather information and temperature are used in the calculation process. ▪ An android IHM is developed to view information for driver.	▪ The most economic route to a destination is given. ▪ Trip duration ▪ Trip cost ▪ Fuel consumption ▪ Route elevations ▪ Service stations in the selected route

Unique Selling Proposition(s):	▪ Various parameters that affect the fuel consumption of a vehicle are considered (air conditioner, engine status, etc.) ▪ A server within the static infrastructure, which has more capabilities, manages the processing complexity. ▪ V2V and V2I communications are deployed. ▪ No need for connection in the client side.
Integration constraint(s):	▪ Apache tomcat server. ▪ Java JDK ▪ Android JDK ▪ Google Maps APIv3 ▪ MySQL database server.
Intended user(s):	▪ Drivers, fleet management companies, police agents, Fire fighters
Provider:	▪ University of Burgundy
Contact point:	▪ Tarek Bouali and Sidi-Mohammed Senouci Sidi-Mohammed.Senouci@u-bourgogne.fr Tarek.Bouali@u-bourgogne.fr
Condition(s) for reuse:	▪ License

AECFV: An accurate and efficient collaborative intrusion detection algorithm to secure vehicular networks		
Input(s):	Main feature(s)	Output(s):
▪ Vehicle's behavior ▪ Vehicles positions ▪ RSUs positions within the road ▪ Data exchanged between vehicles ▪ Data exchanges between vehicles and RSU	▪ AECFV is an accurate and lightweight intrusion detection framework that aims to protect the network against the most dangerous attacks that could occur on such network ▪ This is achieved with a help of the proposed secured clustering algorithm that considers both node's mobility and network vulnerability during cluster formation. Clusters are constructed with a high stability, good connectivity. ▪ AECFV uses three kind of intrusion detection agents, which are: Local Intrusion Detection System (LIDS) running at cluster member level, Global Intrusion Detection System (GIDS) running at Cluster-Head level and Global Decision System (GDS) running at Road-Side-Unit (RSU) level ▪ AECFV has the ability to detect categorize the monitored vehicles into suspected or attacker according to their trust-levels..	▪ A non malicious network ▪ An organized network into stable clusters ▪ Vehicles classification.

Unique Selling Proposition(s):	▪ AECFV is suitable for VANET's characteristics such as high node's mobility and rapid topology change. ▪ It organizes the network into stable clusters that facilitate any application/protocol deployment ▪ It has the ability to detect the most dangerous attacks that could occur in VANETs such as: selective forwarding, black hole, packet duplication, resource exhaustion, wormhole and Sybil attacks.
Integration constraint(s):	▪ NS3 simulation code and need to be adapted for a real implementation in a vehicle ▪ IEEE 802.11p communication capabilities ▪ Need for trusted RSUs with high computation capabilities
Intended user(s):	▪ Researchers ▪ End users (car manufacturers, service providers, etc.)
Provider:	▪ University of burgundy

AECFV: An accurate and efficient collaborative intrusion detection algorithm to secure vehicular networks	
Contact point:	▪ Sid Mohammed Senouci and Hichem Sedjelmaci Sid-Ahmed-Hichem.Sedjelmaci@u-bourgogne.fr Sidi-Mohammed.Senouci@u-bourgogne.fr
Condition(s) for reuse:	Free License

Detection and prevention algorithm from misbehaving intruder in vehicular network		
Input(s):	Main feature(s)	Output(s):
▪ Vehicle's behavior ▪ Vehicles positions ▪ Data exchanged between vehicles	▪ Able to detect and especially predict the future misbehavior of a malicious vehicle. The prediction is based on Bayesian game. ▪ Prevents the occurrence of the Denial-of-Service (DoS) and false alert generation attacks.	▪ Vehicles categorization into the appropriate list (White, Red, Grey or Black) ▪ Malicious vehicles ejection

Unique Selling Proposition(s):	▪ Our algorithm exhibits a high accuracy prediction, faster attack detection, and generates a low communication overhead ▪ Our algorithm has the ability to predict the occurrence of the most dangerous attacks that could occur in VANET such as DoS and false alert generation attacks.
Integration constraint(s):	▪ NS3 simulation code and need to be adapted for a real implementation in a vehicle ▪ IEEE 802.11p communication capabilities
Intended user(s):	▪ Researchers, car manufacturers, application providers, end-users, drivers, passengers, etc.
Provider:	▪ University of Burgundy
Contact point:	▪ Sidi-Mohammed Senouci and Hichem sedjelmaci Sidi-Mohammed.Senouci@u-bourgogne.fr Sid-Ahmed-Hichem.Sedjelmaci@u-bourgogne.fr
Condition(s) for reuse:	▪ No license.

Detection and prevention algorithm from misbehaving intruder in vehicular network		
A secure Intersection-Based Routing Protocol for Data Collection in Urban Vehicular Networks		
Input(s):	Main feature(s)	Output(s):
▪ Road topology ▪ Traffic density per road segment. ▪ Vehicles behavior. ▪ Vehicles positions.	▪ The road topology is get from preloaded maps in vehicles and geographical positions are get using Global Positioning Systems (GPS). ▪ A cluster-based technique is proposed to collect real-time traffic information where the map is divided into segments and small sub-segments in which an elected cluster head counts its neighbor and inform others. ▪ A set of rules and detection algorithms are proposed to monitor vehicles behavior, detect and evict malicious ones from the network. ▪ Detect the Denial-of-Service attacks (DoS).	▪ Optimal routes for packets to destinations ▪ A non malicious network ▪ Vehicles classification

Unique Selling Proposition(s):	▪ The consideration of real-time traffic in the packet routing process. ▪ Packet forwarders are chosen only from confident vehicles. ▪ The use of mutual monitoring between vehicles.
Integration constraint(s):	▪ IEEE802.11p communication capabilities. ▪ Preloaded maps within vehicles.
Intended user(s):	▪ Researchers, car manufacturers, application providers, end-users, drivers, passengers, etc.
Provider:	▪ University of Burgundy
Contact point:	▪ Tarek Bouali and Sidi-Mohammed Senouci Sidi-Mohammed.Senouci@u-bourgogne.fr Tarek.Bouali@u-bourgogne.fr
Condition(s) for reuse:	▪ No license.

A Fuzzy Logic-Based Communication Medium Selection for QoS Preservation in Vehicular Networks		
Input(s):	Main feature(s)	Output(s):
▪ Application class ▪ Vehicle speed ▪ Network density ▪ Service cost ▪ Received signal strength	▪ A set of fuzzy rules is defined to select the best communication medium among available networks. ▪ Information about vehicles and networks are gathered in real-time.	▪ The most adequate network is used for an application.
Unique Selling Proposition(s):	▪ The real-time traffic and network performances are considered. ▪ The framework is lightweight and does not require high processing capabilities.	
Integration constraint(s):	▪ Fuzzy logic library required.	
Intended user(s):	▪ Drivers, fleet management companies, police agents, Fire fighters, service providers.	
Provider:	▪ University of Burgundy	
Contact point:	▪ Tarek Bouali and Sidi-Mohammed Senouci Sidi-Mohammed.Senouci@u-bourgogne.fr Tarek.Bouali@u-bourgogne.fr	
Condition(s) for reuse:	▪ No license required	

Detection and response algorithms to enhance security against lethal cyber-attacks in UAV networks		
Input(s):	Main feature(s)	Output(s):
▪ UAVs behavior ▪ UAVs positions ▪ Data from embedded sensors in the UAVs ▪ Position of the ground stations ▪ Number of UAVs and ground stations	▪ It is a distributed and hierarchical intrusion detection and response scheme, which orchestrates the intrusion detection, decision and categorization mechanisms cooperatively between UAVs and the ground station to detect and eliminate some security threats that may disrupt the network. ▪ The intrusion detection mechanism is running at the UAV node level and the intrusion response mechanism running at the ground station level. ▪ A set of detection and response techniques are proposed to monitor the UAVs behavior and categorize them into the appropriate list according to the detected cyber-attack. ▪ It detects the most lethal cyber-attacks that can target an UAV network, namely, false information dissemination, GPS spoofing, jamming, grey hole and black hole attacks.	▪ UAVs categorization into the appropriate list (Normal, Abnormal, Suspect or Malicious) ▪ Malicious UAVs ejection

Unique Selling Proposition(s):	▪ Our algorithm is fast in terms of attacks detection, lightweight in terms of communications overhead, scalable and achieves a high accurate detection rate. ▪ Our algorithm attempts to secure UAV networks by taking into account the particular characteristics of these networks, such as DTN communications and high node mobility.
Integration constraint(s):	▪ NS3 simulation code and need to be adapted for a real implementation in a drone ▪ Wifi communication with DTN capabilities (memory within the drone) ▪ Need for trusted ground stations with high computation capabilities
Intended user(s):	▪ Researchers ▪ End users (drones manufacturers, Research & Rescue teams, etc.)
Provider:	▪ University of Burgundy
Contact point:	▪ Sid Mohammed Senouci and Hichem Sedjelmaci

Detection and response algorithms to enhance security against lethal cyber-attacks in UAV networks	
	Sid-Ahmed-Hichem.Sedjelmaci@u-bourgogne.fr Sidi-Mohammed.Senouci@u-bourgogne.fr
Condition(s) for reuse:	▪ Free License

Name: Adaptive video transmission application		
Input(s):	Main feature(s)	Output(s):
▪ Analog video streams ▪ IP video streams	▪ Vehicle to control room live video transmission over IP networks ▪ In-vehicle video recording ▪ In-vehicle video display	▪ IP video streams adapted to the network QoS ▪ Exported recorded video streams

Unique Selling Proposition(s):	▪ In-vehicle adaptive video transmission ▪ Features adapted to public safety users
Integration constraint(s):	▪ Works on embedded systems ▪ Proprietary software
Intended user(s):	▪ Public Safety professionals
Provider:	▪ Airbus
Contact point:	▪ arthur.lallet@airbus.com
Condition(s) for reuse:	▪ Licensing

Name: RoutesMobilityModel ns-3 module		
Input(s):	Main feature(s)	Output(s):
▪ Network simulator 3 ▪ API for accessing travel planning service	▪ Mobility module for ns-3 simulator ▪ It imports seamlessly routes from google maps	▪ Vehicular mobility ▪ Public transport mobility ▪ Pedestrian mobility

Unique Selling Proposition(s):	▪ Module for ns-3 that seamlessly download travel plans from external services (e.g.: google maps) and compile them into mobility patterns for ns-3 nodesUsed to assess V2V communication scenarios
Integration constraint(s):	▪ Ns-3 ▪ libcurlpp ▪ Xerces-C++ ▪ GeographicLib ▪ Key for using Google Maps API, acquirable for free from Google website
Intended user(s):	▪ ICT researchers that want to use realistic mobility models for vehicles / pedestrians / public transports, without having to acquire deep knowledge on traffic engineering topics.
Provider:	▪ CISTER/INESC-TEC, ISEP, Polytechnic Institute of Porto, Portugal. Code available from: ▪ - ns-3 main website https://www.nsnam.org/wiki/RoutesMobilityModel ▪ - Bitbucket repository https://bitbucket.org/TiagoCerqueira/routesmobilitymodel
Contact point:	▪ Michele Albano - mialb@isep.ipp.pt ▪ Luis Miguel Pinho – lmp@isep.ipp.pt
Condition(s) for reuse:	▪ Gnu Public License

Content dissemination and synchronisation framework		
Input(s):	Main feature(s)	Output(s):
▪ Cloud server ▪ REST API ▪ High-level libraries ▪ Security features	▪ A framework based on a content server and synchronization agents on mobile devices ▪ This platform is used by business applications and management system. ▪ The system uses a model based content feed containing a coherent set of atomic sub-contents. These sub-contents may refer to each other and integrate multimedia and location data. ▪ The synchronization system is applied transparently based on policies (rights, QoS) when new content is available and when a communication opportunity appears.	▪ Easy to implement applications ▪ Disruption tolerant systems

Unique Selling Proposition(s):	▪ Easy app/service design. ▪ Modern features (synchronisation of content, multi-server, disruption tolerant applications, D2D capabilities) available for use directly in the framework. ▪ Multi-level security. ▪ Multi-language support (JavaScript, Python, Perl, iOS, Android).
Integration constraint(s):	▪ D2D communications are limited to some devices and operating systems.
Intended user(s):	▪ App and service providers
Provider:	▪ Thales Communications and Security
Contact point:	▪ Farid Benbadis Farid.Benbadis@thalesgroup.com
Condition(s) for reuse:	▪ No licence yet

Health Usage Monitoring System (HUMS)		
Input(s):	Main feature(s)	Output(s):
▪ Fleet of vehicles ▪ On-board sensors ▪ On-Board data-logger ▪ On-Board data-transmitter	▪ Collect usage information, environment and health electronic equipment, optronic or mechanical or systems; ▪ Evaluate thanks to gathered data, the health of vehicles during missions; ▪ Operating a scheduling maintenance according to the condition of equipment and its constraints or schedule maintenance operations; ▪ Optimize mission planning phases:	▪ Fleet of vehicles system status evaluation in near real time ▪ Data to plan maintenance phases of vehicles

Unique Selling Proposition(s):	▪ Near realtime vehicle fleet monitoring. ▪ Proactively schedule maintenance and furnitures.
Integration constraint(s):	▪ Compliant on-board units. ▪ Communication system.
Intended user(s):	▪ Fleet of vehicles owners
Provider:	▪ Thales Communications and Security
Contact point:	▪ Farid Benbadis Farid.Benbadis@thalesgroup.com
Condition(s) for reuse:	▪ No licence yet

In-vehicle data collection and transmission		
Input(s):	Main feature(s)	Output(s):
▪ In-vehicle sensors (via OBD2) ▪ Logical inputs ▪ GPS ▪ Accelerometers/ Gyroscope	▪ Recovery and save all data from the inputs ▪ Configuration of the application according to customer needs ▪ Management of two different transmission means (web services and sFTP)	▪ two possibilities to get all the data (vehicle sensors, default codes, localization, inputs, accelerometers) : into a XML file push upload on a sFTP server or through REST web services

Unique Selling Proposition(s):	▪ Vehicle real time monitoring ▪ Compliant with all OBD2 compliant vehicle ▪ Customizable for every need ▪ Respecting the strongest automotive constraints
Integration constraint(s):	▪ OBD2 compliant vehicle
Intended user(s):	▪ For professionals and individuals with a need to monitor a vehicle
Provider:	▪ DUNASYS
Contact point:	▪ Florian THOMAS ▪ Florian.thomas@dunasys.com
Condition(s) for reuse:	▪ Commercial license + support