Digital Forensics Model of Smart City Automated Vehicles Challenges

Xiaohua Feng
School of Computer Science and Technology
University of Bedfordshire
Luton, UK
Xiaohua.feng@beds.ac.uk
Tel. +441234400400

Edward Swarlat Dawam
School of CST
University of Bedfordshire
Beds, UK
Edward.Dawam@study.beds.ac.uk

Saad Amin
Computer Science Department
Coventry University
Csx188@coventry.ac.uk

***Abstract* — The current cyber society is full of complications. Internet has brought so many convenient services to our society but Internet is also a mine field. Mass surveillance from smart phone to PC, from automated car to smart television, any online device seems could be turn to privacy breach toolkit. In order to protect privacy data, including PII, against Cyberstalking and other cybercrimes, a Digital Forensics Model is in progress served for Smart City Automated Vehicles. The proposed development is still on going. Here, an update is reported for discussions.**

Keywords ***–Big data, the Cloud security, Smart City monitoring, IoT*** **(Internet of things),** ***Personally identifiable information (PII) data protection, Cyberstalking, automated car, Digital forensics model***

I. INTRODUCTION

As a new research area, Digital Forensics is a subject in a rapid development. Cyber security for ICT (information communications technology) is getting more and more attentions. Computing breach requires digital forensics to seize the digital evidence to locate who done it and what has been done maliciously and possible risk consequence assessing and many more. In particular, attack on smart city cases, Digital Forensics has been facing even more challenge than original digital breach investigations.

Smart Autonomous Automated Vehicles (AAVs) are the result of decades of research (beginning from the 1980s) into the field of vehicle automation; an application of smart transportation which is a major feature of smart cities. Their relationship involves the communication of sensor data between vehicles to vehicle (V2V) and vehicle to infrastructure (V2I) with a unified data hub in smart cities so as to aid the relevant authorities in decision making; these sensor data make up the lowest level of smart city infrastructure and are accessed through the smart AAVs Electronic Control Unit/Module (ECU/ECM). Since the ECU is an event data recorder and can be used to aid car forensics in cyber-attack or related accident cases, the information coming from these sensors has to be accurate.

In this work, an investigation and analysis of threats specific to smart AAVs within a smart city project were carried out. We used a diagnostic tool to connect a laptop to the on-board diagnostic port of modern vehicle, thereby gaining access to the sensor data on the ECU of two different cars using two different on-board diagnostic software tools. The sensor data was imaged and hashed for data integrity, analysed based on the J1979 standards and encrypted for security purpose. Recommendations were made on how to acquire, preserve and analyses the car sensor data in a forensically manner based on the ACPO guidelines, leading to the proposal of a forensic model for the investigation of smart AAVs in a smart city context.

Smart City technique is making use of ICT to collecting, detecting, analysing and integrating the key information data of core systems in running the cities. The control is making intelligent responses to different requirements that include daily livelihood, PII (Personally identifiable information) security, environmental protection, public safety, industrial and commercial activities and city services. The Smart City data are too sophisticated to deal with easily. This paper has summerised our review on a Digital Forensics model. A case study of Smart City project with the Autonomous Automated Vehicles services to date. Further research is still proceeding at Cyber Security Laboratory, School of CST, University of Bedfordshire. (Abeykoon, et al. 2017)

II. BACKGROUND

Smart city, focuses on the application of the next-generation of information technology to all walks of life, thereby embedding sensors and equipment to power grids, hospitals, roads and railways, bridges and tunnels, dams and water systems, buildings, oil and gas pipelines and other objects in every corner of the world.(Mardacany, 2014). This will enable us to integrate the Internet of things through super computers and cloud computing and will also enable people to manage productivity and life more meticulously and more dynamic manner, leading to global intelligence environment.

Smart autonomous automated vehicles (AAVs) is one fundamental application in the field of intelligent/smart transportation systems (ITS/STS). Smart cities make use of the internet of things, sensor networks and other technological avenues in changing the traditional transport system and establishing the smart traffic management system. Their relationship involves the communication of sensor data between vehicles to vehicle (V2V) and vehicle to infrastructure (V2I) with a unified data hub in smart cities so as to aid the relevant authorities in decision making. These sensor data make up the lowest level of smart city infrastructure and are accessed through the smart AAVs Electronic Control Unit/Module (ECU/ECM). Since the ECU is an event data recorder and can be used to aid car forensics in cyber-attack or related accident cases, the information coming from these sensors has to be accurate as it can potentially lead to a lawsuit and subsequent conviction.

Recently, such lawsuits are increasingly dependent on the sensor and event data recorded on the vehicles' electronic control module or electronic control unit (ECM/ECU). These ECM data includes speed records, airbag and break light sensor data and other event data that can aid accident Reconstructionist to corroborate and classify physical evidence thereby unraveling the true cause of an event. Since these digital data may potentially end up being used as evidence in court, it should be forensically sound. However, practices mostly employed in extracting this information are unprofessional when compared to other areas of digital forensics and therefore require great care on the part of the investigators so as to properly preserve and present evidence.

III. SMART CITY

According to IBM; Smart City is the use of ICT in collecting data and integrating the key information of core systems in running those cities, while also making intelligent responses to different needs that include daily livelihood, environmental protection, public safety, industrial and commercial activities and city services.

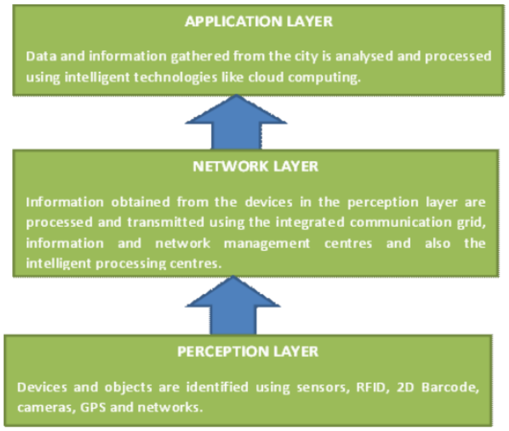
In 2006, Samuel Palmisano, the IBM CEO made a speech in New York to the foreign relations council. In his speech, he released the concept of "Smart Planet: the agenda of the next generation leaders". This concept is to be subsequently discussed in separate meetings in the US and China in 2009, thereby gaining positive responses from president Obama and Premier Wen Jiabao and eventually throughout the world it has gained more acceptances (Su, 2011). However, "Smart City" – initially referred to as wireless city or wireless digital city, has the same approach with "Smart Planet" but only applies to a specific region. It achieves the goal of informational and integrated management of such cities. It is an effective integration of smart planning ideas, smart management methods, smart construction modes, and smart development approaches**.**

III. SMART AUTONOMOUS VEHICLES

According to (Hernandes, 2013) an Autonomous car/ vehicle (in some cases referred to as smart / driverless/ self-driving, car / vehicle) "is a self-driving vehicle with the capability of perceiving its environment and can navigate without human intervention. In order to achieve this, complex autonomous driving algorithms that consist of perception, localization, planning and control are required. Several heterogeneous sensors, actuators and computers are also required to achieve autonomous driving".

Jo K. et al (2014) said that smart autonomous cars have the capability to drive like humans and to make this possible; the car needs to have different components working collaboratively together. These components include; Perception (to evaluate its surroundings), Localization (using the GPS technology), Planning (in order to take the correct action at each step and time.), Control (for the steering, acceleration and breaking) and system management (to supervise the whole vehicle system functionality).

However, the two of them agree that among the many technologies that are required to achieve autonomous automated vehicles are; a combination of actuators and sensors, powerful software executing processors and sophisticated algorithms. It can also be deduced from the both of them, that the sensors and actuators of autonomous cars are categorised into three functions that they aim to achieve: Navigation and guidance sensors – they are responsible for telling you the location, the destination and transportation method. Driving and safety sensors – that are responsible for directing the vehicle to its destination, ensuring that the vehicle acts with precaution in all circumstances and adheres to road and traffic rules. Performance sensors – they manage the basic internal system of the vehicle.



Data and information gathered from the city is analysed and processed using intelligent technologies like cloud computing.

Information obtained from the devices in the perception layer are processed and transmitted using the integrated communication grid, information and network management centres and also the intelligent processing centres.

Devices and objects are identified using sensors, RFID, 2D Barcode, cameras, GPS and networks.

Figure 1 A Smart City Technical Architecture

Smart autonomous automated vehicles is one of fundamental applications in the field of intelligent/smart transportation systems (ITS/STS). Smart cities make use of the IoT, sensor networks and other technological avenues in changing the traditional transport system and establishing the smart traffic management system. The smart traffic management system is an adaptive traffic signal control system with the capability of automatic control of traffic lights in accordance with the flow and time (Su, 2011). The smart traffic management system also integrates urban planning, construction, management and operations and can further provide a comprehensive support for other subsystems like emission control systems in smart vehicles to monitor and control carbon emission, which is a main aim of smart cities.

IV. DIGITAL FORENSICS

According to Feng et al (2012); "Digital forensics is a science of acquiring, analysing, extracting, interpreting and producing evidence from a digital source in civil, criminal or cooperate cases of administrative nature". As a result of the growing use of computers and their networks, digital forensics has become a vital part of forensics science used in hunting down malicious activities whose traces are mostly found in digital form, thereby aiding in the process of identifying the perpetrators. It evolved from computer forensics, developed further to IoTs, Big data, the cloud forensics, bio-informatics, PII and many more area (Hashishi, 2011; Feng, 2012, 2015 and 2016).

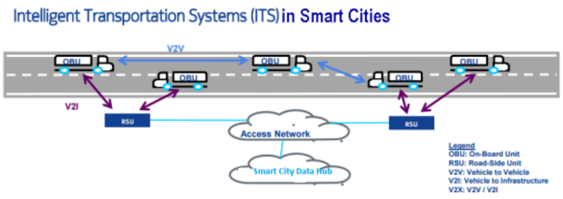


Figure 2 ITS Architecture in a Smart City

V. DIGITAL FORENSIC INVESTIGATION MODEL

A number of digital forensic investigation models have been proposed, some of them are; Computer forensic investigative process – has four phases; Acquisition, Identification, Evaluation and Admission. (Pollitt, 1995). Digital Forensic Research Workshop (DFRWS) Model: Has six phases; Identification, Collection, Examination and Analyses and Presentation (Ismail and Hassan, 2011). Abstract Digital Forensic Model (ADFM): This model was coined out of the DFRWS model and adding three (3) more model phases to it, namely "Preparation, Approach Strategy and Returning Evidence" (Reith and Gunsh, 2002). Integrated Digital Investigation Process (IDIP): consists of five phases, which are; Readiness Phase, Deployment Phase, Physical Crime Scene Phase and Digital Crime Scene Investigation (Ankit, 2011).

From the aforementioned, it can be deduced that all the models share some areas of similarity in the processes of acquisition/collection, preservation, identification, examination/evaluation and presentation. However, the Integrated Digital Investigation Process model has shown features that are more relevant to smart city AAVs as its potential attacks can come from either a physical or cyber source or both and it makes provision for both scenarios**.**

VI. METHODOLOGY

In this research, we have considered the smart city AAV to have both cooperative and automated features as it has a very high level of automation in carrying out dynamic driving task, such that the need of a human driver to monitor threats emanating from the outside environment is not required and it can also perceive its environment using multiple sensors and also make use of the wireless communication technology to perform vehicle-to-X communication (V2X) where X is the smart city road infrastructure which are the stationary road side infrastructures and units that aid smart AAVs. These infrastructure units include traffic signals, map servers and road communication units that broadcast messages like road side alerts (RSA) and signal phase timing (SPAT) which are typical of smart cities.

To summaries the experiments in our project, we could reach a conclusion for AVVs as following Figure 3 shown. The Figure 3 model has demonstrated a proposed digital forensics investigation process model on the smart city automatic vehicle cases, which including the function of preventing data manipulation by hash verification in order to achieve the data evidence integrity as required in principles**.**

VII CONCLUSIONS

This research work has discussed the vulnerabilities of smart AAVs within the context of a smart city, and has identified the possible attack vectors and the point of digital evidence collection in smart AAVs. This leads to the identification of the ECM as a prime tool that collects and stores all relevant data associated with a vehicle's operations. The research went further to apply the ACPO guidelines in the handling of incident data contained in a vehicles ECMs. Other concepts like tamper resistance, standard data meanings, transparency and establishing a baseline for trust were discussed as it relates to the handling of ECM data. A demonstration to describe how acquired ECM data/report can be manipulated is carried out to underpin the research's recommendation that native file formats should not be a trusted format for evidence report.

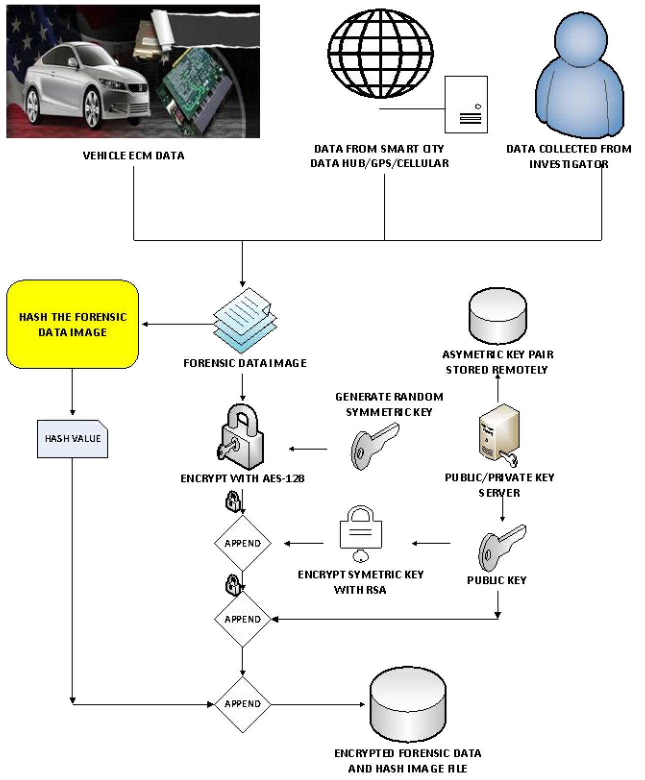

VEHICLE ECM DATA
DATA FROM SMART CITY DATA HUB/GPS/CELLULAR
DATA COLLECTED FROM INVESTIGATOR
HASH THE FORENSIC DATA IMAGE
FORENSIC DATA IMAGE
ASYMETRIC KEY PAIR STORED REMOTELY
GENERATE RANDOM SYMMETRIC KEY
HASH VALUE
ENCRYPT WITH AES-128
PUBLIC/PRIVATE KEY SERVER
APPEND
ENCRYPT SYMETRIC KEY WITH RSA
PUBLIC KEY
APPEND
APPEND
ENCRYPTED FORENSIC DATA AND HASH IMAGE FILE

Figure 3 A Forensics Model to Vehicle Data Investigation

VII CONCLUSIONS

This research has shown that vehicular evidence data can also be extracted, stored and presented in line with the ACPO guidelines using current methods and common tools, but that requires care and diligence from the investigator. The issue as discussed by the research, however, is that when vehicles are away from the incident scene, the data is altered thereby given an inaccurate result from the one that will have been acquired from the point of an incidence. Furthermore, identifying all interested parties at the time of evidence extraction is not feasible in some cases. This poses an issue for an investigator using current practices in the absence of witnesses and thus an issue for first responders as well.

Explanations regarding the standards used by diagnostic software and ELM 327 diagnostic adapter are made in a manner that gives meaning to the raw digital data represented in hexadecimal format in the CarScanner and OBD Auto Doctor diagnostic tools. The level of their compliance with SAE J1979 standard; that defines communication and data interchange between passenger cars, light and medium duty trucks with a wide range of diagnostic test equipment is also discussed and verified. A demonstration of further experimental work and the results regarding the implementation of applying the forensics model to vehicle data details will be provided, represented and discussed at Exeter in June.

Future recommendations on practices to make the forensic processes more reliable and sound were proposed to lead to a development of a digital forensic investigation model on smart AAVs. These recommendations include hashing and encryption of evidence files for integrity purposes, design of diagnostic tools to take activity logs, so as to record an investigators action, using write blockers to prevent message traffic capable of altering digital record and a replay mechanism that replays diagnostic network traffic in order to avoid alteration of the source.

The ease of altering data and evidential files is an issue of concern to vehicle digital data, even though data on clouds and networks can be trusted. Also, the access and integrity of data exposed to adverse and damaging conditions is another issue in the design of vehicle ECMs. That is why designers of these systems ought to implement protective measures against intended and accidental alteration of this network data. A sound solution proposed by this research is to have this network data compared with standard external sources, archived, hashed and encrypted to guard against manipulation. This solution should be adopted by all manufacturers that make use of vehicular networks in transmitting data. Immediately after data extraction, the hash value should be distributed to trusted third parties for storage.

REFERENCES

Abeykoon I. Feng X. and Qiu R. (2017) *“Acquisition and Recovery Robotics Forensics Evidence“*, University of Bedfordshire, Research Conference 2017.

Altschaffel R, Hoppe T, Kuhlmann S, Dittmann J. (2014) “*Beyond mileage”*. IEEE International Conference on Connected Vehicles and Expo (ICCVE). 22 (4), pp149 - 154.

Anderson Ross (2008) Ross Anderson (2008) “*Security Engineering*”, 2nd Ed. Wiley, ISBN-13: 9780470068526.

Connected Vehicles and Expo (ICCVE). 22 (4), pp149 - 154.

Ankit, A., Gupta, M., Gupta, S. and Prof. Gupta . (2011). “*Systematic Digital Forensic Investigation Model”*. International Journal of Computer Science and Security (IJCSS). 5 (1), pp. 1-14.

Carrier, B. (2005): “*Filesystem forensic analysis*”, Indiana: Addison Wesley Professional, 2005, ISBN: 9780321268174

Cohen, R. (2012) '*The past, the present, and the future of cloud computing*', Intel Technology Journal, 16 (4), pp.20-24.

Deekue S.; Feng X. and Liu, E (2013): “*A strategic framework for Nigeria e-government security*”, ARSR2013 Workshop, University of Bedfordshire and Manchester, UK

Delport Waldo M. K. and Olivier Martin S. (2011), “*Isolating a cloud instance for a digital forensic investigation*”, proceedings of the Information and Computer Security Architecture (ICSA).

Dykstra J. and Sherman A. (2011), “*Understanding issues in cloud forensics: Two hypothetical case studies*,” Journal of Network Forensics, vol.b, no. 3, pp. 19–31, 2011.

Fahad Abdullah Al (2015), “*Cloud computing security policy*”, University of Bedfordshire, UK.

Feng X. (2016), “*Forensics and Cyberstalking “*, University of Bedfordshire, UK

Feng X. and Louise, J. (2013), "*MITM attack detection on computing networks*", The International Journal of Soft Computing and Software Engineering [JSCSE], Vol. 3, No. 3, Special Issue: the Proceeding of International Conference on Soft Computing and Software Engineering 2013 [SCSE'13], San Francisco State University, CA, U.S.A., March 2013 Doi: 10.7321/jscse.v3.n3.78 e-ISSN: 2251-7545

Feng X. (2012), "*Cloud computing forensics*", ICFCCT-2012, China, 2012.

Feng, X, et. al. (2012): "*Digital forensics & ethical hacking*", 8th HEA Forensics Workshop, UK.

Feng, X (2011): "*Computer Law in UK*", UCC Data Retriever, Digital Library Workshop, Irland

Feng X. (2011): '*Incidence Response Strategies*", the 7th Annual Forensics Workshop, U.K.

Harshish M and Feng X. (2011): "*Challenges on Forensics, A Cloud investigations reference model*", STAN-2011, IEEE Symposium of Security, Technology and Networks.

Hernandes A, Brito A. S, Roncancio H, Magalhães D. V, Becker M. Sampaio R. C. B, Jensen B. T. (2013). "*GISA: A Brazilian platform for autonomous cars trials*". Industrial Technology (ICIT), 2013 IEEE International Conference. 65 (05), pp. 82 - 87.

Jo K, Kim J, Kim D, Jang C. and Sunwoo, M. (2014). "*Development of Autonomous Car—Part I: Distributed System Architecture and Development Process*". IEEE Transactions on Industrial Electronics. 61 (12), pp. 7131.

Johnson, J. Daily, J. and Kongs, A. (2014). "*On the Digital Forensics of Heavy Truck Electronic Control Modules*". SAE International Journal on Commercial Vehicle. 7 (1), pp72-88

Liu, E and Feng X. (2014): "*Trustworthiness in the Patient Centered Health Care System, Series: Communications in*

Petit J and Shladover S. (2015). "*Potential Cyberattacks on Automated Vehicles*". IEEE Transactions on Intelligent Transportation Systems. 16 (2), pp546-556.

Pollitt, M. (1995). "*Computer Forensics: An approach to evidence in cyberspace*". Baltimore: MD. pp487-491.

Reith, C. and Gunsh,C. . (2002) "*An Examination of Digital Forenisc Models*". International Journal of Digital Evidence, 1 (3), pp1 - 6.

Su K, Li J and Fu, H. (2011) "*Smart city and the applications*". Electronics, Communications and Control (ICECC), 2011 International Conference. 10 (2), pp1028-31.

Wang Z and Liu Y. (2010) "*Design of Road Tracing Navigation Control for Smart Car Use CCD Sensor*". IEEE International Conference on E-Health Networking, Digital Ecosystems and Technologies Design. 10 (3), pp345 - 348.

Woo S, Jin Jo H, and Hoon Lee D. (2015) "*A Practical Wireless Attack on the Connected Car and Security Protocol for In-Vehicle CAN*". IEEE Transactions on intelligent transportation systems. 16 (2), pp. 993.

Zawoad Shams and Ragib H. (2013) "C*loud forensics: a meta-study of challenges, approaches, and open problems*", University of Alabama at Birmingham, USA.

.