A Safe Traffic Network Design and Architecture, in the Context of IoT

Angeliki Kalapodi [I], Nicolas Sklavos [I, II], Ioannis D. Zaharakis [II, III], Achilles Kameas [II, IV]

[I] SCYTALE Research Group, Computer Engineering & Informatics Dept. (CEID), University of Patras, Hellas

[II] Computer Technology Institute & Press – "Diophantus" (CTI), Patra, Hellas

[III] Computer & Informatics Engineering Dept., Technological Educational Institute of Western Greece, Hellas

[IV] School of Science and Technology, Hellenic Open University, Patra, Hellas

***Abstract*— Today's life has been simplified by the advent of IoT technology. Smart Homes and Smart Cities tend to be the most frequent subject of study, on this field of science. This work is concentrated on the design and implementation of an IoT network, over smart roads. Car accidents' rate gets higher over the years. A smart road network might offer very useful data for the construction of a real-time accident and traffic preventer. Hardware implementations are also included. The architecture, security and privacy preservation of the network are highlighted. Cryptography could be the tool to the creation of a safe and useful IoT application. A concluding solution to the Road Tragedy phenomenon may be offered by the Academic study and research. Safe and effective smart networks' research and development may simplify daily life and eliminate fundamental issues. All these solutions may be applied to the human society, as very useful and trustworthy approaches.**

Keywords—IoT, Smart Cities, Mobile Ad-hoc Networks, Privacy, Security, Encryption, Tesla Cars.

I. INTRODUCTION

The aim of this research is to study and develop an 'intelligent' Mobile Ad-hoc Network for the detection, identification and recording of events on a given traffic network. The data provided to the manager by the network may lead to case studies, from traffic frequency to accident prevention statistics. In particular, the modern electric cars are equipped with sensors, which could transmit the data to a cloud. Thus, the data could be converted into useful information, under appropriate processing, with the goal of creating secure traffic networks in the cities.

Internet of Things (IoT) is the wide concept of vehicles, home devices etc, which could be connected via software, sensors, activators and networks, that allow these objects to exchange data [1-3]. IoT forms a concept that relates to daily objects, that use built-in sensors to collect data and act on them within a network. In brief, the IoT is the technological future that will make our lives easier [1-3].

Ad-hoc Networks are one of the most modern and challenging research sectors in automation industry. A wide range of applications, such as safety, mobility and connectivity for both the driver and passengers, transport systems in a smooth, efficient and secure way could be exploited by the presence of such networks.

More specifically, this study focuses on the interaction and integration of various critical elements of an Ad-hoc Traffic Network. An Ad-hoc Traffic Network is a wireless network where the communicating nodes are mobile, and the network topology is constantly changing. Wireless sensors can detect any events such as accidents, as well as frozen roads and can forward rescue /warning messages via intermediary vehicles for any necessary help. We therefore propose an Ad-hoc network architecture that uses wireless sensors to detect events and effectively transmit security messages using different service channels. Moreover, a control channel with different priorities may be built.

The purpose of designing this system is to increase driving safety, prevent accidents and effectively use channels by dynamically adjusting the control and service channels' time slots. We will propose a method that can select some driver nodes between vehicles running along a national highway to efficiently transmit data. The method followed can be a guide to managing traffic issues and preventing accidents. The generality of the methodology lies in the fact that the traffic frequency, in existing traffic networks, road behavior, and the availability of electric cars vary by region. However, this work could help in the implementation of a "smart" Ad-hoc traffic network that would be applicable in every state.

This work is organized as follows. First and foremost, the theoretical background is sited. Trust, authentication and Ad-hoc Networks are the necessary terms to be analyzed. MANETs (Mobile Ad hoc NETworks), and more particularly their sub-category VANETs (Vehicular Ad hoc NETworks), are the theoretical model to be implemented. The proposed model, a safe traffic network, is introduced. The network components, as well as the algorithm implemented are shown in detail. Last but not least, the benefits and drawbacks of the proposed model in our daily life are listed and highlighted. The positive effect of the implemented model and the significance of academic research in human life issues are underlined. Online simulations and implementations are included.

II. TRUST MANAGEMENT INFRASTRUCTURES

The significance of trust management infrastructures is highlighted. Trust models are implemented only in small, static networks due to their management constraints and memory requirements. A peer-to-peer validation is required by a web-of-trust model [4]. However, it lacks feasibility for non-static networks. At least one trust anchor, that organize on-the-fly connection requests, between network nodes, manages a hierarchical trust model. This system is supposed to be appropriate for static networks. The categorization of hierarchical trust models exists as follows: Trust Center Infrastructures (TCI) (system Kerberos) and Public Key Infrastructures (PKI) (X.509, Card Verifiable Certificates (CVC) [5].

The most vital part of a digital identity certificate is the identification of both peers. The name of a web resource can only be identified by the Uniform Resource Identifiers (URI). Notwithstanding, the URI may be considered as futile, depending on the expected number of IoT devices. Thus, we use IPv6 address as its unique device identifier. Public Key Cryptosystems, are based on a pair of keys, which is authenticated by both peers, each time. Two of the most famous public key cryptosystems are:

- ✓ *Rivest–Shamir–Adleman (RSA): based on the difficulty of factoring the product of two large prime numbers.*
- ✓ *Elliptic Curve Cryptography (ECC): a quite fresh approach to public key cryptography based on the algebraic structure of elliptic curves over finite fields.*

ECC is considered as faster than RSA and has been established as the leading public key cryptosystem of choice, for resource-constrained embedded systems. Therefore, an IoT device contents a single universal certificate, that lasts the same as the expected operational life span of the device [1].

Customized domain-specific Object Identifier (OID) extensions should be defined due to the lack of a standardized framework for the encoding of device attributes entailing authorization credentials in a certificate. Concerning the Trusted Authentication Protocols, one or more nodes may be connected by a device with multiple simultaneous peer-to-peer connections. Transmission Safety Protocol (TLS) refers to the application level protocol in an IP-based environment [6].

A. Trust in the Internet of Things

The individual devices of any trust management system should be protected by the IoT (Figure 1). Encapsulation via memory virtualization, usually fails to be processed by a trustworthy firmware. Consequently, the individual components firmware trustworthiness determination, are not enough. Thus, the firmware overall image should be validated. An integral component to maintain security may overpass the obstacle of the lack of a secure device firmware updating or patching mechanism. Otherwise, several systems can be compromised by a foible. A network-wide update mechanism should be included in an effective patching process. By this mechanism, integrity robustness and authenticity checks, service outages minimization, and a version rollback permission -if necessary- may be goaled.

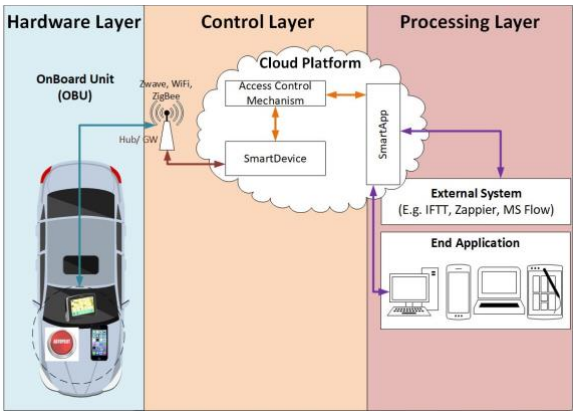

Figure 1 Visualization of an IoT Network

The system should process as follows:

- ✓ *Trust tokens exchange and validation or new session tokens creation.*
- ✓ *Data integrity assurance, optionally combined with data confidentiality via encryption, for the data suggested trustworthines.*
- ✓ *Implementation of data confidentiality via symmetric encryption, often directly in hardware; usually, data integrity is provided via message authentication codes, or cryptographic hashes, attached to the payload data.*

In this way, we reassure the construction of a viable mechanism, protected against fabrication [7-8].

B. Security Protocols for IoT Access Networks

Nowadays, the main pillars that represent the basic technologies are listed as four. They preserve the most common vertical applications related to automation or machine interaction formulate IoT architecture [9]:

1. Radiofrequency ID (RFID); with target to the objects' identification and tracking through tags, spared in the environment or attached to an object, is considered to be the most disseminate technology.
2. Machine-to-Machine (M2M) communications.
3. Wireless Sensor Networks (WSN); a constitution of several sensors widely split in the environment, with the ability of monitoring physical values and wireless communication in a multi hop mode. Its reference standard is the IEEE 802.15.4 [10].
4. Supervisory Control and Data Acquisition (SCADA); a real-time smart monitoring autonomous system. It preserves heterogeneity of terminals and the necessary guarantee for the data security [11].

The analysis would be incomplete, with the elimination of the vast amount of data management, due to the billions of information, from the environment to the Internet. A cloud platform's responsibility includes data storage, computation, visualization, and transforming into useful information. The providence of specific services and the necessity of each object's address could be preserved by a standardized platform. Some

issues arising from the diffusion of an IoT are the heterogeneity of terminals, and the need for data security guarantee, from their collection to their transmission.

Finally, the cognitive security is introduced and applied to the time-based security solution. It highlights the main parameters that need to be monitored and measured by actors to strengthen the security in a parti-colored and variable scenario like the IoT [12].

C. Authentication in IoT Networks

The parties involved in the entity authentication are:

- ✓ *Claimant (that declares its identity as a message).*
- ✓ *Verifier (that is preventing impersonation).*
- ✓ *Trusted Third Party (mediates between two parties to offer an identity verification service as a trusted authority).*

Transferability and impersonation are included in the entity authentication objectives. The factors of entity authentication are classified, as follows: something known, something possessed and something inherent. These techniques have now been extended beyond authentication of human individuals to device fingerprints. The levels of entity authentication are categorized as weak authentication, strong authentication and Zero-Knowledge (ZK) authentication.

The reciprocity of identification, the computational efficiency, the communicational efficiency, the third party and the timeliness of involvement entity, are the authentication properties that are of interest to users. A central authority (CA) often runs offline to edit public-key certificates. The nature of trust, the nature of security guarantees and the storage of secrets, constitute the most important components.

D. Ad-hoc Networks

Hereby, we are focused on the interaction and integration of various critical elements of a Mobile Ad-hoc Network (MANET). A MANET is a wireless network, where the communicating nodes are mobile, and the network topology is constantly changing. Wireless sensors can detect any events such as accidents and can proceed warning messages, via intermediary vehicles for any necessary assistance. The proposed architecture is an ad-hoc network that incorporates wireless sensors to detect events and effectively transmit security messages, using different service channels and a control channel with different priorities. [13].

For security applications, the best routing protocol should be selected. The three most common routing protocols used in the MANET are: Dynamic Source Routing (DSR), Ad Hoc On-Demand Distance Vector (AODV) and Destination-Sequenced Distance Vector (DSDV). Indeed, it is important and necessary to test and evaluate the different routing protocols related to the MANET, before implementing them in the real environment. This can be done through MANET simulation tools. Our goal is to measure the performance of the routing model, for city scenarios. The main objective is to find the appropriate routing protocol, in a high-density traffic area.

A MANET is a self-tuning and wireless network of mobile devices, connected via wireless links, (Figure 2). Every device in a MANET is free to move to any direction, and therefore often changes its links with other devices. Each of them should promote the data circulation, that is not related to its own use, and thus act as a router. The main challenge for building a MANET is to supply each device, so that it always maintains the necessary information to proper route traffic. These networks can either operate autonomously or connect to the Internet. MANETs are a kind of wireless ad-hoc network with a routable network environment at the top of the Open Systems Interconnection (OSI) Reference Model Data Link Layer.

One of the main types of MANETs is Vehicular Ad-hoc NETwork (VANETs). VANETs are used to ease the communication among vehicles and among vehicles and equipment en route. More specifically, this work will be dealt with by InVANETs (Intelligent Vehicular Ad hoc NETworks - Intelligent VANETs). It is a kind of artificial intelligence that helps vehicles behave intelligently during vehicle-related crashes, accidents, driving under the influence of alcohol, etc. The node eviction in VANETs forms the main cause of interest thereby [16]. A Vehicular networking features include high-speed mobility, short-lived connectivity, and infrastructureless networking constitute the formation of a VANET.

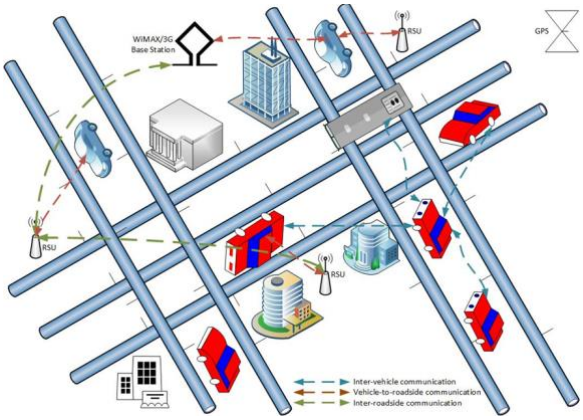

Figure 2. Visualization of a VANET

VANETs consist of vehicles equipped with wireless gadgets [14]. Communication in VANET occurs between vehicle and vehicle operation, and the road with which an intelligent traffic system gets formed. Routing plays an important role in promoting the required data to nodes or vehicles. Some reactive routing protocols, such as AODV and DSR protocols and proactive routing protocols such as Optimized Link State Routing (OLSR) in urban traffic scenarios are examined. Simulation of Urban Mobility (SUMO) and network performance using Network Simulator 3 (NS3) to find an appropriate protocol using network parameters, and delay are being used. The simulations have shown that AODV proceeded well with other routing protocols in VANET scenarios [15].

III. PROPOSED MODEL

VANET is an exemplary IoT, with vehicles as things connected to the IoT [17]. Intentionally, faulty messages get inserted to VANET with the potential of massive destruction by malicious

nodes. Other than faulty nodes, malfunctioning Onboard Units (OBU) with fatal aftermaths in safety applications obstruct VANET's performance [18]. Moreover, massive destruction may be caused by faulty messages inserted to VANET by malicious nodes. Errant nodes should get removed anyway from VANET as fast as possible. Traditionally, an errant node's certificate gets revoked by a centralized CA. Nevertheless, CA-based approaches become ineffective due to the nature of VANET. Nodes are allowed to decide and act against other errant nodes both distributed and locally by current node-eviction schemes in VANET (Figure 3). Local node-eviction schemes can be classified into four categories: Reputation, Vote, Suicide Abstinence and Police. Various factors may affect the performance of node-eviction schemes. It gets strong in model behaviors and goals of single nodes by the richness in flexibility and emergence of an agent-based simulation. The simulation scenario is formed by a circular road setup in the grid, where vehicles at different speeds cycle around the road and communicate with each other or with the RoadSide Unit (RSU) when nearby.

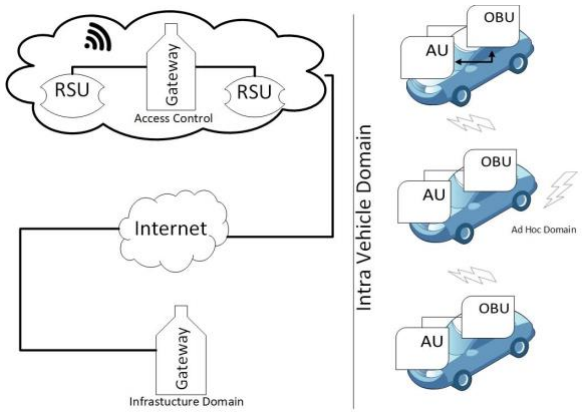

Figure 3. Visualization of a VANET

The RSU transfers the information to the CA. In our model, the node-eviction scheme and frequency of contact are implicit. Any node eviction scheme should be able to optimize the average time, risk, and utility measures under dynamic environment conditions. The node eviction process gets modeled as a set of states and transitions. Eventually, two subnets get formed, separating all nodes, depending on their good or bad state. A state transition occurs as long as a node moves from Subnet I to Subnet II. Finally, Subnet I or Subnet II will converge into the same kind of nodes. A network message exchange, certificate-controlled model, form the final system. Each node formulates a List of other nodes' Valid Certificates (LVC). As long as good and bad nodes are separated with insignificant risk, the procedure terminates. However, it gets complicated the individual police node to capture all the bad nodes on time. In parallel, as the percentage of bad nodes increases, multiple bad nodes pop up simultaneously at different spots. Moreover, possibly some of the bad nodes never being caught, meaning a high risk [9].

The VANET applications are based on the precise information, providence to the drivers. Nevertheless, VANET content delivery includes serious security threats. Common metrics cannot be precisely measured, according to the effectiveness of different techniques. Thus, consumers cannot be reassured, especially with regards to the critical road safety concerns. However, security measurement is difficult and differs from other kinds of measurement, like quality of service in wireless multimedia. An Asymmetric Profit-Loss Markov (APLM) model, constructs a security metric. Briefly, profits are considered to be incidents of detecting data disasters, and the ones of accepting corrupted data as damages.

A. Case of Study

Houston is the capital of the American State of Texas, located southeast and bordered by the Gulf of Mexico. It has population of over 6,000,000 inhabitants and an expanse of 1,558 km^2. It is chosen, as the area of study, because it is in the 2nd place of the traffic congestion table, but also in the 6th place of the fatal accidents chart among the USA.

It is very important to bear in mind that in Houston, according to the recorded car events of 2016, a man was killed every 2 hours and 20 minutes. One person was injured every 1 hour and 59 seconds, and a recorded incident took place every 57 seconds [19]. In total, for 2016, the privately-owned vehicles registered by the U.S. Service vehicle registration statistics reach 261.8 million. The daily statistics of Houston's traffic congestion are shown in Figure 4.

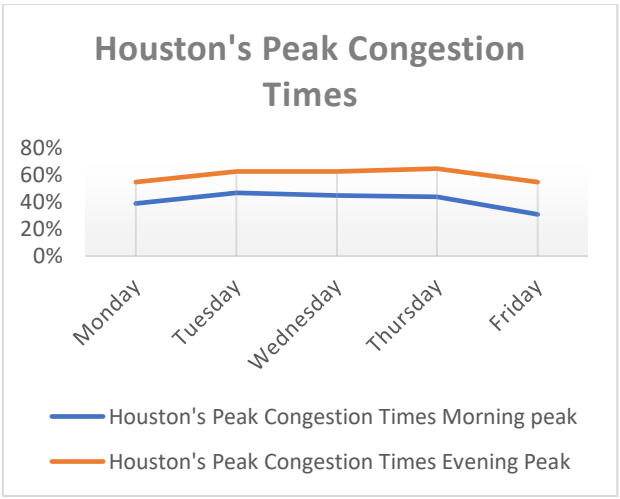

Figure 4. Houston's Peak Congestion Times

The yearly statistics of Houston's traffic congestion are shown in the below Figure 5.

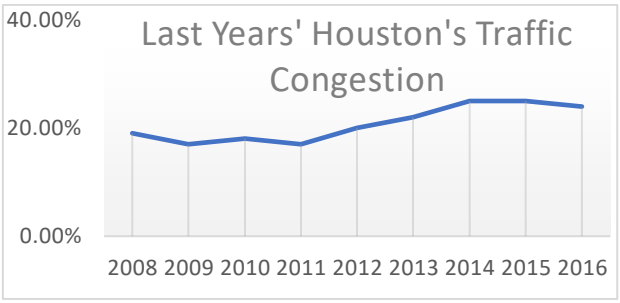

Figure 5. Houston's Congestion

All the mentioned above, prove the usefulness of a smart application for traffic regulation in a state with increased traffic issue. The rate of injuries and deaths in the area of study, necessitate the creation of an ad-hoc network that can provide real-time data for the study, prevention and rehabilitation of the traffic network.

B. Tesla Cars

Tesla cars, with their advanced technology, can provide us with information transfers about what is going on in the street. They are the only candidates to perform the OBU role [23].

Specifically, the Tesla S was designed from the beginning as the safest, most exciting sedan on the road. With outstanding performance delivered through Tesla's unique electric engine, the S-Series accelerates from 0 to 60 mph in just 2.5 seconds. The S model incorporates an Autopilot feature that is designed to make a motorway drive safer, (Figure 6), [23].

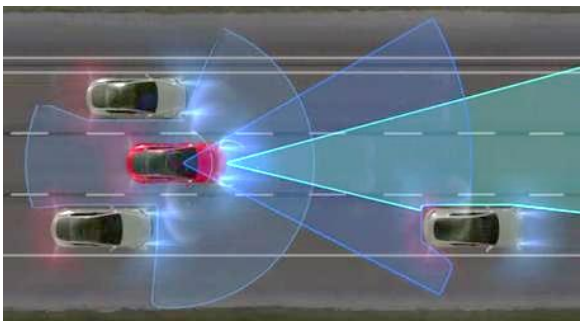

Figure 6. Tesla Autopilot System

The driver's safe driving system is based on the following:

1. *Eight peripheral cameras offer 360 degrees of visibility around the car up to 250 meters.*
2. *Two-time ultrasonic sensors complement this vision, allowing the detection of hard and soft objects almost twice the distance of the previous system.*
3. *A forward-looking radar with improved processing, providing additional data for the world at an unnecessary wavelength that can be seen through intense drop, fog, dust and even the car forward.*

C. The Algorithm

The basic idea of the algorithm is that the essential data are used, to alert the driver for any possible events, throughout the road network. The loop keeps on until there are not essential data to keep the driver vigilant. The following simple algorithm can lead the information of the system to the administrator and each driver for the criticalness of the road events (Figure 7). The daily use of the data produced, may offer useful statistics concerning the special roads, or crucial parts of the street that need attention. Repeating the algorithm, big data can be produced for any necessary road construction works. The algorithm is visualized in Figure 8.

Applying the algorithm, the vehicle data may be collected by the RSU, be processed and used equally. In this way, the driver may be alerted for any kind of danger appearing and the system administrator may be notified to intervene, if necessary. The daily collection and processing may highlight the need for road works or speed limitation for the elimination of road traffic or accidents rate minimization.

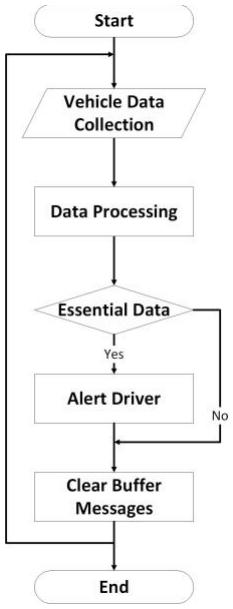

Figure 8. Visualization of the Algorithm

D. A Traffic Simulation Framework

An online simulation was implemented to justify the proposed system. Given real-time data collected from the distributed online simulations, necessary information for near real-time traffic decisions get provided by the IoT traffic system. The traffic IoT network is divided into dynamic overlapped sections, and a simulation processor mapped to each section. Nearby RFIDs and sensors supply each simulation with real-time data, enabled to run continuously. A collection of segment simulations formulates the overall distributed simulation. In this, each small segment of the overall traffic IoT network is modeled based on local criteria. The information exchange among vehicles moving from one simulation segment to another is allowed in the simulation. Each simulator's segment locally models current traffic conditions and shares its predictions with other simulation segments. Altogether, they create an aggregated view of both the individual segment ‘s area of interest and the overall of traffic system. current traffic state information and their predictions to the simulation server are published by the simulators' segments. An accurate estimation of a future state of the system is provided by an aggregation of all simulation segments provides. All the mentioned above are reflected in Figure 7, [21].

Significant network bandwidth and amount of computation by each simulator host are required by the current large-scale distributed simulation methodologies. The communications loads placed in the network can be reduced by mobile agents. Agents communicate with a specific simulation segment, providing all the state information sent to the simulator server.

For modeling a collection of adjacent intersections, NetLogo simulator has been used. Different network features are represented by static and mobile agents. Motor vehicles have been modeled individually within NetLogo using mobile agents.

By NetLogo, instructions can be given to many independent agents which could all operate at the same time. Four types of agents are used in NetLogo: patches represent the static agents, turtles represent the mobile agents; links make connections between turtles; and the observer oversees everything going on in the simulated environment [21].

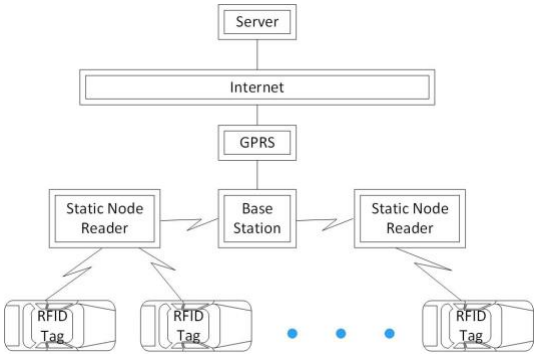

Figure 7. Distributed Online Traffic Simulation Framework

Java is the programming language of the NetLogo environment. In this simulation, the agent entities are vehicle, traffic lights, and sensors of intersections and lanes. Agents are created and randomly distributed over the network of intersections. A random number of vehicles are set to limits defined in the model. Sensors recorded the number of passing vehicles. The traffic lights' action is based on vehicles' waiting time minimization and vehicles successful pass through intersections throughput increase. The following indicators are bore in mind per run: not moving vehicles, average waiting time and average speed of the vehicles in a time step. Usually, the driver's behavior is unpredictable. Drivers' behavior modeling has been performed based on techniques proposed by. The simulation has 'setup' and 'go' switches. The 'setup' switch sets a procedure to reverse the model to the initialization state. The 'go' switch initiates a procedure that carries out all the necessary actions for each simulation. The interface and performance evaluation of the simulation results are shown in Figure 8 [21].

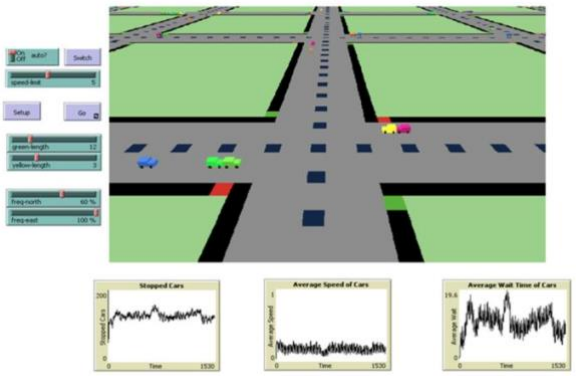

Figure 8. Interface And Performance Evaluation of the Simulation Results

IV. Efficient Hardware Implementations

The system proposed may be implemented by Udoo Kits. Their technologies form a full IoT implementation platform [24]. Actually, it is a single-board computer, Arduino-compatible, that can perform Android or Linux OS. Its benefits are its ease-to-use, with minimum knowledge requirements (Figure 7). Different computing methods, emphasizing on the proper and weak points of each are combined. Educational purposes are the basic reason of Udoo Dual/Quad [23]. A well-trained team that can built-up new applications and projects, using a low-cost and user-friendly platform, may be created for its use. Thus, a useful tool for high-standards implementations may be provided to institutions and companies.

Following the rules of trust and authentication, IoT may be successfully implemented. As the technology evolves, more and more requirements are necessary to networks and systems. IoT systems, are representative of bridging and maintaining complex systems at every appearance of real life.

Figure 9. Udoo Kit: An IoT Implementation Platform

Udoo kits basically consist of touch displays of 7-15 inches, featuring high resolution that makes the content easy to be read, USB gates, USB cables for additional gates and LCD board adapters. The main representative, integrated systems suggested by Udoo are Udoo KIT LCD 15,6" Touch and Udoo KIT LCD 7" - Touch for QUAD/DUAL. The Udoo kits include WiFi technology (as well as ethernet), camera connectors and their capacity may reach up to 2,5 GHz (CPU), 700 MHz (GPU) and 8GB (RAM) [24].

V. Advantages of The Proposed Model

VANETs offer innumerable benefits to organizations of any size. High speed internet access of cars will transform the vehicle's computer from an elegant gadget, into a basic productivity tool, making almost any web technology available in the car. While such a network creates some security concerns, it does not limit the VANETs' dynamics, as a productivity tool. It allows the "dead time", that is lost while waiting for something, to be transformed into "useful time", time used to perform tasks. A passenger can turn a traffic congestion into a productive working time. Even GPS systems can benefit as they can be integrated with traffic reports, to provide the fastest route to run. Finally, it would allow free VoIP services, among the converters, reducing the cost of telecommunications.

On the other hand, while Internet can be a useful productivity tool, it can also turn out to distract enough attention, resulting in security and real-time consuming concerns. Checking emails, surfing the web, or even watching videos, can distract a driver's attention from any danger in the street.

VI. Conclusions & Outlook

While still years away, VANET is a technology that could significantly increase productivity in times that are usually not productive. However, to achieve this, VANET users must first

overcome the loose temptations and distractions of Internet. Recent developments in wireless communications technologies and in the automotive industry have generated significant research interest in VANETs in recent years. VANET consists of vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) technologies supported by wireless access technologies such as IEEE 802.11p.

This innovation in wireless communication, is designed to improve road safety, and traffic efficiency, to the close future through the deployment of Intelligent Transport Systems (ITS). As a result, the government, the automotive industry and academia, cooperate to a large extent through various ongoing research projects to establish standards for VANETs. The typical set of VANETs application areas, have made VANETs an interesting wireless domain. This document provides an overview of the current research situation, challenges, VANETs capabilities and the path towards achieving the long-awaited ITS [24-25].

The innovative safety systems such as ABS, seatbelts, airbags, backlight cameras, electronic stability control (ESC) have not reduced the car accidents' rate, which is highly increased. Several studies have argued that 60% of motorway accidents could be avoided if warning warnings were given to drivers just a few seconds before the time of the collision.

The academic community is the one that will play the vital role in the regulation of another social life issue. This implementation may lead to the expunge of traffic problem. Smart systems and intelligent networks may be the tool to this problem's resolution.

The IoT science has evolved throughout the years and daily life has been simplified significantly. Road traffic and car accidents could not be out of IoT science's scope. The real- time preventer that is examined in this paper may be a revolutionary discovery for another side of the daily life. The features of modern implementation platforms may cover the needs of such issues arising.

ACKNOWLEDGMENT

This work is under the UMI-Sci-Ed project. This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 710583.

REFERENCES

[1] N. Sklavos, I. D. Zaharakis, A. Kameas, A. Kalapodi, "Security & Trusted Devices in the Context of Internet of Things (IoT)", IEEE proceedings of 20th EUROMICRO Conference on Digital System Design, Architectures, Methods, Tools (DSD'17), Austria, August 30 – September 1, 2017.

[2] N. Sklavos, I. D. Zaharakis, "Cryptography and Security in Internet of Things (IoTs): Models, Schemes, and Implementations", IEEE proceedings of the 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS'16), Larnaka, Cyprus, November 21-23, 2016.

[3] I. D. Zaharakis, N. Sklavos, A. Kameas, "Exploiting Ubiquitous Computing, Mobile Computing and the Internet of Things to Promote Science Education", IEEE proceedings of the 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS'16), Larnaka, Cyprus, November 21-23, 2016.

[4] G. Guo, J. Zhang, "Improving PGP web of trust through the expansion of trusted neighborhood", IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology (WI-IAT), 2011, University of Saskatchewan, Canada.

[5] A. Arsenault, S. Turner, Internet X.509 public key infrastructure PKIX roadmap, IETF Roadmap, September 8, 1998.

[6] M. Bourlakis, I. P. Vlachos, V. Zeimpekis (editors), Intelligent Agrifood Chainsand Networks, Wiley-Blackwell, 2011.

[7] N. Sklavos, "Cryptographic Algorithms on A Chip: Architectures, Designs and Implementation Platforms", proceedings of the 6th Design and Technology of Integrated Systems in Nano Era (DTIS'11), Greece, April 6-8, 2011.

[8] N. Sklavos, "On the Hardware Implementation Cost of Crypto-Processors Architectures", Information Systems Security, The official journal of (ISC)2, A Taylor & Francis Group Publication, Vol. 19, Issue: 2, pp. 53-60, 2010.

[9] Arzad Kherani and Ashwin Rao, Performance of node-eviction schemes in vehicular networks, IEEE Transactions on Vehicular Technology, vol. 59, no. 2, pp. 550–558, 2010.

[10] H. Tseng, S. Sheu, and Y. Shih, "Rotational listening strategy (rls) for IEEE 802.15.4 wireless body networks," IEEE Sensors J., vol. 11, no. 9, pp. 1841–1855, 2011.

[11] P. Kasinathan, C. Pastrone, M.A. Spirito, and M. Vinkovits, "Denial-of Service detection in 6LoWPAN based Internet of Things," in Proc. Of IEEE 9th Intl. Conf. on Wireless and Mobile Computing, Networking and Communications (WiMob), 2013, pp. 600–607,7–9 October 2013.

[12] M.R. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L.A. Grieco, G. Boggia, and M. Dohler, "Standardized protocol stack for the Internet of (important) Things," IEEE Communications Surveys & Tutorials, vol. 15, no. 3, pp. 1389–1406, 2013.

[13] J. Tan, and S.G.M. Koo, "A survey of technologies in Internet of Things," in Proc. of IEEE Intl. Conf. on Distributed Computing in Sensor Systems (DCOSS), 2014, vol., no., pp. 269–274,26–28 May 2014.

[14] Sijing Zhang, Enjie Liu. Vehicular ad hoc networks (VANETs): Current state, challenges, potentials and way forward. Elias C. Eze, Centre for Wireless Research, Institute for Research in Applicable Computing (IRAC), Department of Computer Science and Technology, University of Bedfordshire, Luton, LU1 3JU, England.

[15] Viswacheda Duduku. V, Ali Chekima, Farrah Wong, Jamal Ahmad Dargham. A Study on Vehicular Ad Hoc Networks., Univ. Malaysia Sabah, Malaysia.

[16] S. Gao, J. Ma, W. Shi, G. Zhan, and C. Sun. Trpf: A trajectory privacy preserving framework for participatory sensing. IEEE Transactions on Information Forensics and Security, vol. 8, no. 6, pp. 874–887, 2013.

[17] M. Groat, B. Edwards, J. Horey, W. He, and S. Forrest. Enhancing privacy in participatory sensing applications with multidimensional data. In Proc. of 2012 IEEE International Conference on Pervasive Computing and Communications (PerCom '12), pp. 144–152,2012.

[18] Jonathan Andrew Larcom and Hong Liu, Authentication in GPS-directed mobile clouds, in Proceedings of IEEE Global Communications Conference 2013 (IEEE GLOBECOM 2013), pp. 470–475, Atlanta, GA, 9–13 December 2013.

[19] Texas Department of Transpotation, www.txdot.gov, 2018.

[20] Tom Tom Traffic Index , https://www.tomtom.com/en_gb/trafficindex/.

[21] Hasan Omar Al-Sakran "Intelligent Traffic Information System Based on Integration of Internet of Things and Agent Technology", Management Information Systems Department, King Saud University Riyadh, Saudi Arabia, International Journal of Advanced Computer Science and Applications, Vol. 6, No. 2, 2015.

[22] Tesla Cars, www.tesla.com, 2018.

[23] Udoo Kits, www.udoo.org, 2018.

[24] R. Piquepaille, "Turning Cars into Wireless Network Nodes", ZDNet, Vehicular Network Lab @ UCLA – Implementing the First Campus Vehicular Testbed, Vehicular Lab, 2007.

[25] P. McCloskey, "The Mobile Internet: Your Car Could Save a Life", medGadget, 2007.