Novel Design Based Internet of Things to Counter Lone Wolf Part B: Berlin Attack

HASSAN F. MORSI[1,*], M. I. YOUSSEF[2], G. F. SULTAN[1]
[1] Egyptian Nuclear and Radiological Regulatory Authority, CAIRO, EGYPT
[2] Faculty of Engineering, Al Azhar University, CAIRO, EGYPT
* Corresponding author; E-mail: hassanmfahmy@yahoo.com

Abstract: - This paper proposes a new design methodology for Intelligent Transportation Systems, which uses existing smart techniques in transportation systems and human behavior detections to counter lone wolf threats and driver violations. The design can be attached to vehicles as an intelligent embedded system. In this design, the electroencephalogram analysis techniques are used to detect the irregularity in driver behavior which can be categorized into threatened or violated behavior. In threaten behavior like deliberate run-over accidents, the system will stop the vehicle as soon as possible and inform the security agency to ensure a speed response. In violated behavior like driver drowsiness, the system will alert the driver or inform the responding authorities and stop the vehicle, depending on the level of danger. To minimize the consequences of the vehicle fast stopping, it proposed to green the next traffic light signs. By applying this system in vehicles a lot of accidents can be avoided, in particular those caused by lonely wolves like deliberate run-over accidents or stolen of vehicles.

Key-Words: - Intelligent Transportation Systems, Internet of Things, Deliberate Run-Over Accidents, Berlin Attack, Lone Wolves Threats.

1 Introduction

Nowadays the world is suffering from the lonely Wolves (LW) threats. LW uses a new tactics called low-cost attacks. These tactics are including the vehicle ramming, which was represented in the 2016 Nice and Berlin attacks. The simpler the attack, the harder to detect, where the vehicle ramming offers terrorists with limited access to explosives or weapons which are detectable by policing systems. Vehicle ramming terrorism is a hardly noticeable way for law enforcement agencies, since trucks and vehicles are in daily use, hijacking them or renting a new one is not cost more. Also, it can conduct an attack with minimal prior training or experiences of the attacker, which are the features of the LW [1].

Since LWs are individuals that act independently, their identification and detection at any given stage of the attack is extremely difficult. Kaati et al. [2] used a machine learning approach to identify potential LW based on their written communication. This work aims to capture the psychological warning behaviors in written text and identify texts written by LW. They used Linguistic Inquiry and Word Count text analysis tool to extract the psychological meaningful based features that can classified when comparing “regular” texts and texts written by LW.

Therefore, to counter the Vehicle ramming terrorism effectively, it should be countered in the act of ramming, where it appears that programs such as PRISM have failed in stopping terrorist attacks more than 80% of the time [3]. Depending in this idea, the study in [4] was proposed a novel design approach to prevent the LW’s attacks like 2016 Nice attack, where the offender is the truck legal driver. Now, this paper propose a new design approach (called PS_2) that using the existing techniques in Intelligent Transportation Systems (ITS) based Internet of Things (IoT) to prevent the other LW’s attacks like 2016 Berlin attack, where the attacker is the truck illegal driver.

The PS_2 design methodology, requirements and the vulnerabilities of the existing ITS in LW countering will be shown in the following Sections. Section 2 states the motivations for PS_2 design. Section 3 states a survey of the existing techniques which can be used in the PS_2 design. The PS_2 design methodology is presented in Section 4.

Section 5 presents and discusses the expected behavior of the PS_2 in LW attacks and in the hazardous materials transportations. Finally, the conclusion is stated in Section 6.

2 Motivations For Proposed System Design

To show the importance and the motivations for the PS_2 design, Berlin attack scenario will be analyzed. Also, the corrective actions of Berlin attack will be investigated. These Investigations will present the required design criteria of the PS_2.

2.1 Investigation in Berlin attack

On December 19, 2016, the offender intentionally drove the stolen truck through a Christmas market at Breitscheidplatz in Berlin city, killing 12 people and injuring 56. The truck had been hijacked based on its GPS coordinates. The original driver of the truck had been killed by the perpetrator of the attack. However, police investigation reports have indicated that the truck was brought to a stop by its Advanced Emergency Braking System (AEBS) [5]. The death toll in the Christmas market attack in Berlin could have been much higher. But the truck's AEBS, adopted by the EU in 2012, stopped the vehicle after just 70 meters, according to reports.

AEBS specifies the dangerous situations ahead in a timely manner, alarm the driver in case of probable collision risk and independently brake the vehicle in case of emergency if the driver doesn't respond appropriately. Its goal is to prevent a collision with a vehicle travelling ahead or to reduce the collision impact speed.

The attack scenario shows that the truck was brought to a stop by its AEBS. But what would have happened if the offender had experience in dealing with this system, of course he would have been deactivated that system. This is because the traffic regulation in EU countries like Vienna Convention on Road Traffic says that "the driver has to be in control of the vehicle at all times" "Every driver shall at all times be able to control his vehicle" [6]. So, to let the AEBS to counter the Vehicle ramming terrorism, it shall be designed with anti-driver deactivation and it should be called remotely by the police workers.

2.2 Investigation in corrective action of Berlin attack

In responding to Berlin attack, a remote 'kill switch' to immobilize Heavy Goods Vehicle (HGV) is being secretly developed by UK government scientists who fear a Nice style attack. They are investigating methods of interfering with the electronics of Lorries to stop them in their tracks if hijacked or used in an attack. Experts in the UK home Office's scientific wing want to develop and install a technology which would enable them to stop high risk vehicles remotely. These include HGVs and other large vehicles, particularly those carrying hazardous loads such as chemicals and nuclear materials. Earlier this year, Scotland Yard boss said he would like to be able to switch off all vehicles, including mopeds, remotely. It could be activated from a police worker monitoring the movement of the vehicle via GPS from a control centre [7].

The aforementioned paragraph clarified the suggested solutions to prevent accidents styles like Nice and Berlin. But the main drawback is in word "remote/ remotely", which means the police worker could stop the vehicle using wireless communication techniques. As it is known the wireless suffers from problems like hacking and failing of the communication link. Therefore, in addition to the remotely initiation of the innovative system, it shall switch off and stop the vehicles by itself without waiting to external initiation (i.e. self defense).

3 Existing Techniques

Following subsections states the existing techniques which can be used in the PS_2 design.

3.1 Intelligent transportation systems based internet of things

IoT allows the people and things to be connected anytime, anywhere with anything/anyone. The IoT used in smart cities implementation to monitor the traffic congestion. However camera-based traffic monitoring systems are already available in many cities, they require more powerful communication infrastructure to provide more information. Traffic monitoring is conducted by sensing capabilities, GPS installed on modern vehicles and a mixture of air quality sensor and acoustic sensors along the given road. This information is essential for authorities and citizens to discipline traffic and to send officers, as well as to plan the best way to reach the office or a shopping center. In the security of the smart cities, IoT with smart surveillance can monitor people's actions to find any violent act,

where smart surveillance systems can alarm in case of any event of interest occurs. also, camera surveillance systems can detect abnormal situations like vehicles going in a wrong direction and truck driving in abnormal style (as in Berlin attack) by running motion detection algorithms to extract video information, aggregating several frames for performing route detection. Finally, a module classifies reasonable data and translates it to find any abnormalities [8].

There are many ways that IoT can help governments in optimizing services related to transportation, such as traffic management, parking, and transit systems. For example, Gill et al. [9] proposed an intelligent transportation architecture and algorithm for enhancing the security and integrity in the vehicles integrated IoT. In this architecture the real time tracking, collision detection and avoidance protocol is proposed and executed so that the entire IoT based ecosystem can be secured.

Popescu et al. [10] discus probabilistic collection of traffic data through vehicle to infrastructure (V2I) communications and present two novel techniques for automatic detection of traffic incidents in a highway scenario that are based on the use of distance and time for changing lanes, respectively vehicle speed changes over time.

In the advanced ITS [11] the traffic system managers can take action such as traffic light synchronization and emergency vehicles priority based on Integrated Corridor Management (ICM) strategies. The ICM is a decision support system used strategies such as network traffic prediction and real-time response strategy assessments to inform system managers about the current and predicted corridor performance. Connected vehicles system (CV) used to connecting vehicle information and location to other vehicles (V2V); to V2I; or to other modes, such as, pedestrians, and bicyclists (V2X) for functioning many safety features (e.g. avoiding collisions) without driver input or interference. CV applications can significantly reduce most of deadly type's crashes such as vehicles suddenly stopped ahead. ITS technologies (e.g. GPS) and operational advancements (e.g. coordinated traffic management centers) allow quick and efficient mobilization of responders (e.g. fire fighter or police) to an incident by providing real-time traffic, hazardous material information across agencies.

The US-ITS 2015-2019 strategic plan includes research, development, and adoption of ITS technologies in the fields of:

- V2V safety messaging and V2V communications based on wireless technology.
- Automated road vehicle systems and technologies that transfer some tasks of vehicle control from the driver to the vehicle.

Till now there is no ITS nor IoT systems to counter the LW's attacks by vehicles although the integration between them would be sufficient to counter the LW (as a driver), e.g. by prevent the driver from the vehicle's control. So the ITS vulnerability was how to detect that the driver is a LW? The PS_2 proposes to use the human psychological warning techniques to overcome that vulnerability as shown next.

3.2 Electroencephalogram techniques

The PS_2 aims to capture the psychological warning in driver behaviors which can be detected by Electroencephalogram (EEG) brain waves. So the existing EEG techniques for drowsiness and fatigue, person identification, epileptic seizure detection system and drunken driving detection are mentioned. For real time monitoring and driver comfort, the EEG techniques with minimum numbers of electrodes was selected.

- Driver Drowsiness Detection (DDD): Damousis et al. [12] proposed a technique for sleeping onset prediction to avoid the driving accidents. In this technique the EEG's alpha and theta band power are extracted online every 15 seconds and a fuzzy logic application decides the level of drowsiness of the driver and triggers an alarm if the subject is too sleepy. The technique is base on ENOBIO [13] set which is wearable and comfortable. The driver fatigue can be detected using single channel as Ridwan et al. [14] work.
- Person Identification Detection (PID): EEG signals were used for biometric verification because it unique and possess attributes of liveliness detection due to the presence of a legitimate individual for signals acquisition and thus it is non-vulnerable to spoof attacks. Also, ENOBIO used to build an unobtrusive authentication method that only uses two EEG electrodes [15]. Zhendong et al. [16] experimental results show the ability of two frontal electrodes in EEG-Based Person Authentication technique. Also, Mishra [17] developed a Biometric Verification Algorithm using a three-channel EEG data acquisition system. He was combined the EEG data with the Fingerprint using the Fuzzy logic technique. The fusion of the two biometric makes the

system more robust, flexible, secure and accurate.

- Driver Health Detection (DHD): There are more techniques for epileptic detection but for single EEG electrode, Gopika et al. [18] proposed a technique that can be used in classification between epileptic and control persons.
- Driver Alcoholism Detection (DAD): Single EEG electrode used by Lin et al. [19] to predict whether a person is alcoholic or not. Wang et al. [20] had reasonable results in the classification of alcoholic and normal persons by only two EEG electrodes.

4 Proposed System

Now cause of LW threats, the transportations systems should be modified to counter the LW terrorist. The following design is a trial that can be used to enhance the LW countering.

4.1 Design criteria

The PS_2 should be designed to perform the following function to effectively counter the LW. The functions are:-

- Remotely response, i.e. the PS_2 should be called to do its functions remotely by using the wireless technique.
- Changing the Traffic light states (greening and holding of the next forwards signs and reddening the others in intersections) when the vehicle is in an emergency state and will stop suddenly. The system takes that decision depending on:

1) The surrounded traffic density which can be evaluated like Ghazal et al. [21] by using a microcontroller and IR sensors.
2) The existing state of the next Traffic light which can be known by the V2I message.

The effective management of emergency vehicles is satisfied by greening the next forwards traffic signs. This function can performed using a system like the Nellore et al. [22] system. That contains the measurement of the distance between the emergency vehicle and an intersection using visual sensing, vehicle counting and time sensitive alert transmission within the sensor network. The emergency vehicle information is delivering to the traffic authority with less delay so the emergency vehicle is quickly served. The system uses the best wireless protocol to select the emergency vehicle data and reduce the transmission delay for emergency messages.

- Preventing the driver to control the vehicle based on:

1) The EEG's PID signal.
2) Changing of previously approved routes depending on GPS data.
3) The distances between the vehicle and objects depending on AEBS sensors.

- Message broadcasting to other vehicles and the traffic or security authorities.
- In the case of none communication links or if the driver doesn't respond appropriately to the PS_2 orders, the PS_2 shall control the vehicle.

4.2 System architecture

The PS_2 is an embedded system as shown in Fig.1. The signals are divided to:

- Incoming signals which are the GPS Road location and EEG driver monitoring unit that detect DDD, DHD, DAD and the PID.
- Dual communications signals like surround traffic signals (V2V, V2I and V2X); security and traffic authorities; AEBS' initiation/deactivation; and driver's alarm/deactivation.
- Output signals which are the next traffic sign greening (NTSG); Holding the driver (HD); Interlock the ignition (II); and the ambulance informing signal.

The PS_2 central processing unit (CPU) program's performs the desired function according to the flowchart that shown in Fig.2. In Fig.2 (a) the driver is alarmed depending on DDD or DHD modules signal. If the driver deactivated the alarm that means the driver is in good state but if the alarm doesn't deactivated the CPU will process the functions in I branch. Also, the processes in I will perform if the driver is alcoholism, Fig.2 (b).

If the driver is changed, the EEG PID will detect that so the CPU will perform the II branch processes, Fig.2 (c). Also, Fig.2 (c) used to enforces the driver to attach the EEG sensors (e.g. EEG cap or hat) where if the driver take off the EEG sensors cap then the EEG PID signal will be equal to zero and the PS_2 will be processed the functions in II. Depending on the GPS signal if the approved road is changed, the CPU will ask the security authority for permission, if there is no permission the II functions will be processed, Fig.2 (d).

The objective of the PS_2 is to prevent the driver from attacking the lives and property by using the vehicle. Modern systems to detect and prevent

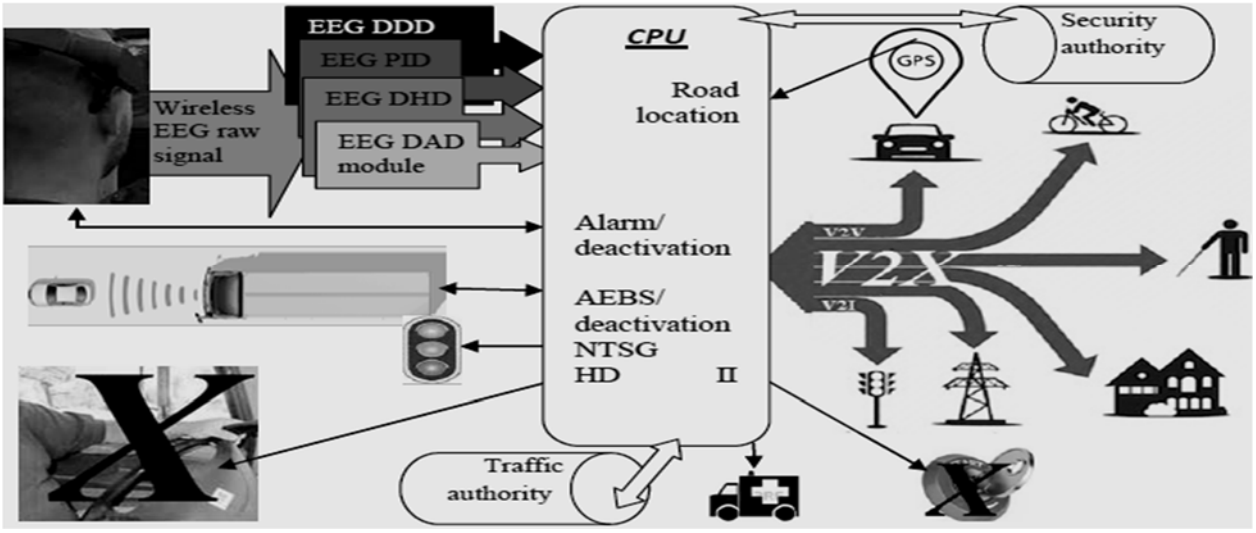

Fig.1. Proposed system architecture

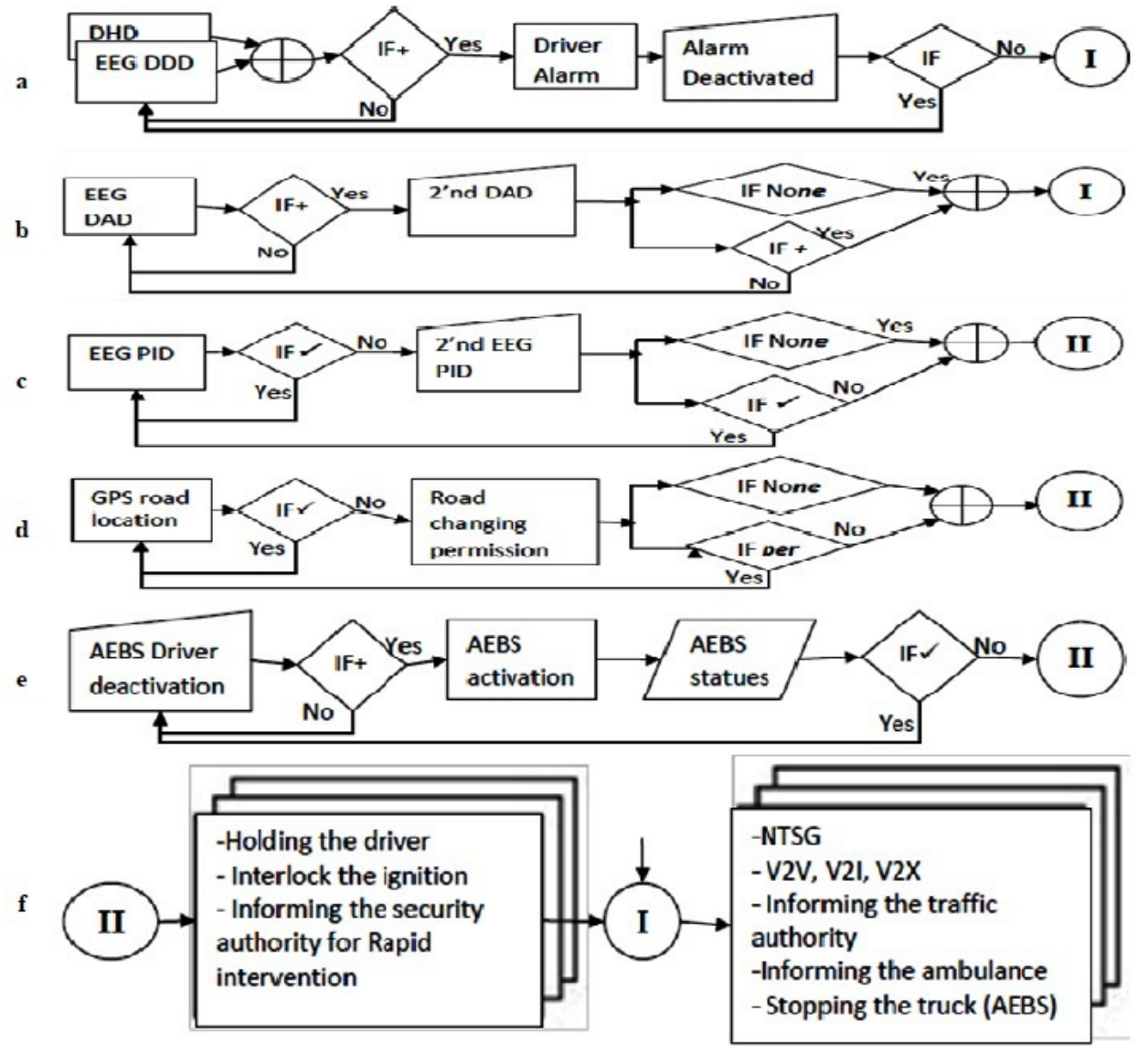

Fig.2. Proposed system flowchart

accidents (like ABES) can perform this objective, provided that the driver doesn't deactivate these systems. Therefore, the PS_2 prevents the driver to deactivate those systems and if the driver tried to deactivate its, PS_2 performs the functions in II, Fig.2 (e)

Finally, Fig.2 (f) states the processes which performed by the branches I and II. The most important processes are holding the driver, interlocking the ignition and Stopping the vehicle. These processes don't need any activation from the out world or the existing of communication links.

The "IF None" statements used in the flowchart to deal with the states when the driver doesn't input the required action or there is no communication links between the PS_2 and the other input systems, so the PS_2 will depend on itself. The 2'nd DAD and 2'nd EEG PID are other techniques to detect DAD and EEG PID respectively, used to increase the PS_2 reliability.

5 Case Study For Lone Wolf Attacks

This section will show the response of the PS_2 if it is applied in two LW attacks scenarios and nuclear materials transportations. Also, the discussion will briefly give the recommendations for the regulations adaptation to facilitate the LW countering.

5.1 Results of PS_2 response in LW attacks

The two most LW's attacks scenarios that are truck legal driver and truck illegal driver. In The first scenario, the driver is an operator or an employee. While the second scenario, the offender is illegal have a truck. The PS_2 will have a good response in the two scenarios.

5.1.1 Truck legal driver

- **The scenario:** In this scenario, the driver under study is the legal driver of the truck and has a good reputation throughout his career history and also has no criminal history or violation of the law. Without previous criminal indications and because of his accessing to terrorist websites, this driver becomes a terrorist (i.e. lone wolf terrorist). Due to his past good reputation and because he acts alone, it is very difficult to detect his terrorist behavior in a short period, so he roams by the truck freely. To kill a lot of public, he deliberately drives into crowded street to run-over the pedestrians.
- **PS_2 detection:** in this LW attack, the driver is the legal driver of the truck. So the flowchart Fig.2 (a, b, c and d) branches can't detect the attack. Because the LW drives deliberately into crowded street with a high speed, the AEBS system will sense that and it will decelerate and brake the truck, hence the driver will try to deactivate that system, then the PS_2 will prevent the driver to control the truck and it will stop the truck, Fig.2 (e).

5.1.2 Truck illegal driver

- **The scenario:** The offender has a truck either by stolen, armed robbery or by Peaceful ways as driver numbing. He deliberately drives the stolen truck into crowded street to run-over the pedestrians.
- **PS_2 detection:** in this LW attack, the perpetrator is illegal driver of the truck. So the PS_2 can detect the LW attack by Fig.2 (c and e) branches.

5.2 Hazardous materials transportations

The most LW harmful attacks were by trucks, admittedly the destruction will be severely increased if the truck was loaded with nuclear or hazardous materials where one of the terrorism aims is to spread the hazardous materials and create panic and disruption. The following lines will show the response of the PS_2 if it is applied to the transportation of the hazardous materials. The nuclear materials are selected as a case study, where the nuclear materials transportation may be suffer from LW threats.

The existing smart transportation cask systems are stated to find the vulnerabilities of the nuclear materials transportations in LW countering. The existing smart cask systems using the advanced surveillance technologies like Argonne's ARG-US[23] for continuous remote tracking and monitoring to enhance the safety, security, and safeguards of nuclear and other radioactive materials during storage, in-transit stoppage and transportation. Also, it applied for critical nuclear fuel cycle facilities and radiological facilities including hot cells and geological repositories. The ARG-US Remote Area Modular Monitoring (RAMM) units can be mounted in a freight truck carrying hazardous/sensitive material. In the case of a spill or transit incident, RAMM would allow first responders to not only know the position of the incident but also the nature and severity of the spill or accident before approaching the scene of the

event [24]. It is clear that RAMM accident responding is happened after the accident and this is the LW's aim, i.e. the recently transportation cask systems can't deal with that kind of terrorists. This vulnerability can be avoided if the RAMM updated to include the PS_2 functions. So, if a scenario like previous ones happens the PS_2 in the RAMM will prevent the accidents. Another scenario can be prevented by the PS_2, where the legal driver wants to stole the nuclear materials (e.g. to make dirty bombs). That is mean he will drive in a good behaviors until reaching to his region. In this case no one of the branches in Fig.2 can detect this problem except the branch d in Fig.2, where the driver will change the previously approved roads (without any causes like construction in the road or traffic jam). Then the PS_2 stop the truck and the processes in Fig.2 f will be achieved.

5.3 Discussion

Although LW identification and detection at early stages before attack is extremely difficult, the PS_2 benefit is it can prevent the LW attack at the acting of attack. Therefore the PS_2 is the last level of the LW defense in depth.

This study points some recommendations and requires a changing of some traffic regulations to let the PS_2 do best.

- Changing of some regulation like the Vienna convention on road traffic which stated that "the driver has to be in control of the vehicle at all times" because this regulation allowing the driver to deactivate the AEBS.
- The nuclear materials transportations regulations should be adapted to effectively counter the LW threats during the transportations. For example, the PS_2 functions should be mandatory in the trucks.
- Attaching of PS_2 to the vehicles/trucks shall be mandatory. PS_2 connection in the vehicles system shall be insured that the vehicles can't start without it, i.e. the driver can't deactivate it.
- Permission from traffic authority for the vehicle in an emergency to change the traffic signs light.

6 Conclusion

In this paper, a system to counter the LW attacks by vehicles is proposed. The system can detect the abnormal behavior and identity of the driver based on the EEG techniques and collision prevention systems like AEBS. In case of a driver violation the proposed system will alert the driver but in a LW threats it (by itself) will prevent the driver to control the vehicle, stop the vehicle and inform the security authority. For collision mitigations the proposed system wills greening the next traffic signs and alerts the surrounds by V2V; V2I; V2X via wireless communications. The proposed system should be attached to hazard materials transportation casks or trucks. The case study results show that the proposed system can effectively counter the LW attacks by vehicles. The proposed system acts as the last level of LW defense in depth.

Acknowledgment

The authors wish to acknowledge the Professor Ezzat A. Eisawy for his strong support. They want also to thank Dr. M. Elzorkany for his precious suggestions. We are thankful to Mr. Khairy Mahmoud Abd-Elmajeed for his worth cooperation.

References

[1] J. Besenyo, "Low-cost attacks, unnoticeable plots? – overview on the economical character of current terrorism," Strategic Impact, vol. 1/62, pp. 83-100, 2017.

[2] L. Kaati, A. Shrestha, and T. Sardella, "Identifying warning behaviors of violent lone offenders in written communication," Proceedings of the 2nd International Workshop on Data Science for Social Media and Risk, Barcelona, Spain, December 2016.

[3] T. Houston, "Mass surveillance and terrorism: does PRISM keep americans safer?," Thesis Projects, University of Tennessee Honors, 2017.

[4] Hassan F. Morsi, M. I. Youssef, and G. F. Sultan, "Novel design based internet of things to counter lone wolf, part a: Nice attack," Proceedings of the 3rd International Conference on Advanced Intelligent Systems and Informatics, September 2017, Cairo: Advances in Intelligent Systems and Computing, Springer, in press.

[5] Wikipedia: https://en.wikipedia.org/wiki/2016 Berlin attack, Accessed 5 June 2017.

[6] W. Eichendorf, "Advanced emergency braking systems for commercial vehicles," German Road Safety Council, 2016.

[7] IHLS news, "Police seeks mass vehicle attack solution," 7 Jan 2017. Available at, http://i-hls.com/he/archives/73974

[8] S. Talari, M. Shafie-khah, P. Siano, V. Loia, A. Tommasetti, and J.P. Catalão, "A review of smart cities based on the internet of things

concept," Energies, vol. 10, No. 421, 2017. doi:10.3390/en10040421

[9] S. Gill, P. Sahni, P. Chawla, and S. Kaur, "Intelligent transportation architecture for enhanced security and integrity in vehicles integrated internet of things," Indian Journal of Science and Technology, vol. 10, no. 10, March 2017, doi: 10.17485/ijst/2017/v10i10/108251

[10] O. Popescu, S. Sha-Mohammad, H. Abdel-Wahab, D.C. Popescu, and S. El-Tawab, "Automatic incident detection in intelligent transportation systems using aggregation of traffic parameters collected through V2I communications," IEEE Intelligent Transportation Systems Magazine, vol. 9, no. 2, pp. 64-75, 2017. doi: 10.1109/MITS.2017.2666578

[11] U.S. Department of Transportation, "History of intelligent transportation systems," 2016.

[12] I. Damousis, I. Cester, S. Nikolaou, and D. Tzovaras, "Physiological indicators based sleep onset prediction for the avoidance of driving accidents," Conf Proc IEEE Eng Med Biol Soc, 2007.

[13] I. Cester, S. Dunne, A. Riera, and G. Ruffini, "ENOBIO: wearable, wireless, 4-channel electrophysiology recording system optimized for dry electrodes," Phealth, International Workshop on Wearable Micro and Nanosystems for Personalized Health, Barcelona, Spain, 2008.

[14] S.D. Ridwan, R. Thompson, B.T. Jap, S. Lal, and P. Fischer, "Single channel wireless EEG: proposed application in train drivers," African Journal of Information and Communication Technology, vol. 5, no. 2, pp. 54-63, June 2009.

[15] A. Riera, A. Soria-Frisch, M. Caparrini, C. Grau, and G. Ruffini, "Unobtrusive biometric system based on electroencephalogram analysis," EURASIP Journal on Advances in Signal Processing, vol. 2008, Article 143728, Hindawi. doi:10.1155/2008/143728

[16] M. Zhendong, H. Jianfeng, and M. Jianliang, "EEG -based person authentication using a fuzzy entropy-related approach with two electrodes," Entropy, vol.18, no. 432, 2016. doi:10.3390/e18120432.

[17] P. Mishra, "Development of biometric verification algorithm using EEG," PH.D thesis, Thapar University, Patiala, India, 2016.

[18] G.K. Gopika, S. Neelam, and B.J. Dinesh, "EEG signal classification in non-linear framework with filtered," 23rd European Signal Processing Conference (EUSIPCO), IEEE, 2015.

[19] C.F. Lin, S.W. Yeh, Y.Y. Chien, T. I. Peng, J.H. Wang, and S.H. Chang, "A HHT-based time frequency analysis scheme in clinical alcoholic EEG signals," WSEAS Transactions on Biology and Biomedicine, vol. 5, no. 10, October 2008.

[20] S. Wang, Y. Li, P. Wen, and G. Zhu, "Analyzing EEG signals using graph entropy based principle component analysis and J48 decision tree," Int. J. Sig. Process. Syst., vol. 4, no. 1, 2016. doi: 10.12720/ijsPS .4.1.67-72.

[21] B. Ghazal, K. ElKhatib, K. Chahine, and M. Kherfan, "Smart traffic light control system," 3rd International Conference on Electrical, Electronics, Computer Engineering and their Applications (EECEA), IEEE, 2016. doi: 10.1109/EECEA.2016.7470780

[22] K. Nellore, and G.P Hancke, "Traffic management for emergency vehicle priority based on visual sensing," Sensors, vol.16, no.1892, 2016. doi:10.3390/s16111892

[23] Y.Y. Liu, K.E. Sanders, and J.M. Shuler, "Advances in tracking and monitoring transport and storage of nuclear material," IAEA-CN-244-186, 2016.

[24] H. Tsai, B. Craig, H. Lee, K. Mittal, Y. Liu, and J. Shuler, "ARG-US remote area modular monitoring for dry casks and critical facilities," INMM 55th Annual Meeting, Atlanta, Georgia, USA, July 2014.