Penerbit Akademia Baru

Journal of Advanced Research in Computing and Applications
ISSN (online): 2462-1927 | Vol. 2, No. 1. Pages 25-38, 2016

A Review and Survey of Vehicular Network's Cybercrime and Security Approaches

F. N. Bhatti[*,1,a], *R. B. Ahmad*[1,b], *H. M. Bhatti*[2,c,] *M. N. M. Warip*[1,d] *and S. J. Elias*[1,e]

[1] ENAC, Research Cluster, School of Computer and Communication Engineering, University of Malaysia Perlis, Malaysia
[2] Institute of Information & Communication Technology, University of Sindh, 76080 Jamshoro, Hyderabad, Pakistan
[a,*]*fahadnazirbhatti@gmail.com*, [b]*badli@unimap.edu.my*, [c] *hamid2k8_hb@gmail.com*,
[d]*nazriwarip@unimap.edu.my*, [e]*sjamel@gmail.com*

Abstract – *Cybercrime is a challenging task in vehicular adhoc network (VANET), for develop the tools and reliable sources to analyze the information during the emergencies or incidents. The emergency organizers and responders for prevent the criminal activities gradually depends on computational response systems and communication domains to look forward all phases of emergency management (EM) in terms of prevent from crime alertness by feedback and rescue. During the crime, some of attackers attempt to disable few physical systems to achieve the task, either in term of malicious behavior or accidentally, while accidentally physical devices disability have been widely recognized by evidence in past documents, and the major struggle has been used into the growth and overview of more strongest technologies such as an open nature networks, similarly the developers of security tools have been educating the worries regarding the possibility of cybercrime may be a reason of physical tragedies and to maximize the influence of crime by intentionally blocking or distortion the tools of the emergency systems. This paper is twofold, in first, we analyze the present developments techniques to prevent the cybercrime of VANET along with people, communication domains, sensor devices, Internet of Things (IoT) and information, we gives the review on cybercrime and emphasize the cybercrime that is probable to effect on emergency response, recovery, and management, as well highlighted some of the response tool have not developed yet based on the literature. Second, we gives the review on security work in VANET which is developed for prevent the attacks and available for investigation of crime, and finally, we proposed the Cloud-Based Recorder (CBR) which is consist of database storage of the vehicle events during the participate in VANET, the CBR record the events of vehicle such as position, speed and time and emergency situations for investigation the cybercrime globally.*

Keywords: VANET, Security, Cybercrime, Attacks.

1.0 INTRODUCTION

Academics and industries widely worked together to reduce the road accidents by employee the VANET, and improved the traffic applications, for instance, safety and non-safety applications, the work is shown as well the evidence of researchers [1], that up to 60% of vehicles collision could be escaped within one condition if the vehicle may provide the alert

Journal of Advanced Research in Computing and Applications
ISSN (online): 2462-1927 | Vol. 2, No. 1. Pages 25-38, 2016

within one an half second earlier before an incident, the VANET is regulated the communication domain between car to car (C2C), Car to Infrastructure (C2I) and Car to all (C2X), in the survey of VANET [2], the United States Dept. of Transportation declared more than 80 different type of applications in terms of different scenarios and assumptions as their usage, as it is studied that the safety applications of VANET are real time as well serious task, it would necessitate authoritarian assurance the quality of service (QoS), in terms of security.

The response of the incidents at mean time the EM progressively engaged with highly computational response systems and communication domains for administration, response, evidence, training, and process. For instance, the sensor networks participate the premature detection of dangerous happenings [3, 4] and it enhances the initial alertness throughout the examine and rescue actions, by specific plan or procedures [5], as the Independent procedures as well mainly independent vehicle is too generally suggested in the EM framework. The initial alertness and administration can be enhanced by aware airborne assumption transfer by non-crewed airborne vehicles [6]. The access of Internet in these type of network has an important role for access the comfort applications and so on, by some web-based EM systems, along with extensive usage of social networks to distribution or exchange the info whenever a dangerous situation happens or assumptions of an emergency, by users, or by different confront applications of industries and consultants [7, 8].

According to the current era the development of computational response, systems familiarizes cybercrime in EM. It may openly root to physical destruction or incidentally intensify a physical event by delaying the initial alert. The EM has the varieties of plenty industrial and governmental response systems which use the satellite communication, the mobile networks and web-based procedures, for instance the employee of physical system's resources may disturb the process of devices by cybercrime, in the term of flood control unit or any sensor which is employed for safety responsibilities. The cybercrime possibly harms the integrity of the evidence which may be a direct result on the trust and assurance of given evidence although a DoS attack possibly turns off or break down the network broadcasting among superiors and initial alerts and effect on the network performance.

The classification of EM was categorized by [9]. engaged with devices, evidential, geospatial, planning and social grouping [9, 10]. We analyze the development of EM in VANET cybercrime along with their intrusion and prevention systems to generate the evidence for investigation and possibly prevent during the crime, then we review on the security recommendation development in VANET and finally we suggest the Cloud Base Recorder (CBR), which possibly help to investigation the cybercrime when if physical evidence are broken else intentionally disappear after crime, the CBR can be used for globally investigation of cybercrime, to achieve this task we analyze and collect the papers related to this topic from 2005 to 2015, which determines the important involvement and some of theoretical evidence approaches which focus on the improvement of VANET security, brief survey and techniques discussed in [11 - 20] Figure 1; brief the sum of publications prepared by each year, the papers browse on practical publishers such as IEEE, ACM, Springer, Wiley and Elsevier by pass in the keywords like "Cybercrime-in-VANET", "Attacks-in-VANET", "Attack-countermeasure-in-techniques-VANET","Security-Challenges-in-VANET.

Journal of Advanced Research in Computing and Applications
ISSN (online): 2462-1927 | Vol. 2, No. 1. Pages 25-38, 2016

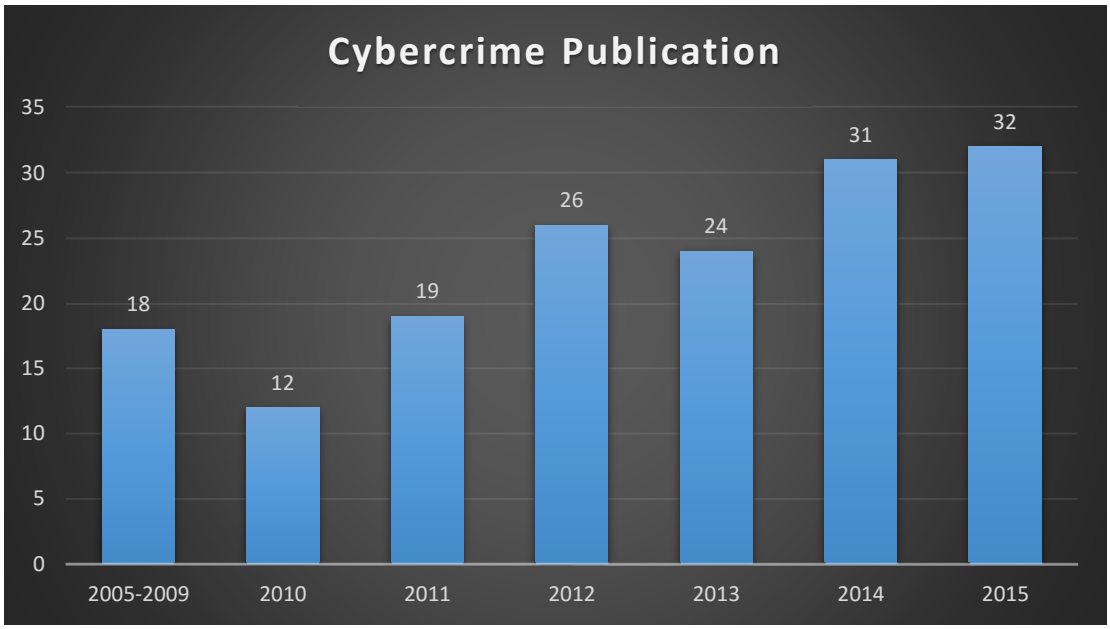

Figure 1: Publication of Cybercrime and VANET's Security from 2005-2015

1.1 Overview of Cybercrime

In general, whenever emergencies arise the main factor conclude as a human negligence or blunders which are historical studied and proved by digital evidence. On the other hand, the limitation of time for any task, for instance, work load, the burden from the administration as well over load of work and nontechnical staff which are not familiar to emergencies strategic policies, plan and procedure of EM consultants by the view of cyber security [21], so commonly human make mistakes. It motivates comparatively informal for cyber criminals to achieve human errors, commonly over social engineering.

The industrial as well insider crime which is recognized as Man-at-the-end attack [22], For instance in the year 1992, a breakdown of Chevron computerized emergency warning system overdue the consultants from alerting the civic of a chemical discharge incident, after investigation the evidence, it was notified that behind the breakdown of alerting system initiated by an insider employee who changed the enable to disable the emergency warning task [23].

Although the human factor is definitely serious in the EM situation, as the neighbor vehicles possibly harm and create the casualties to other vehicle by broadcasting wrong information, alert, and control the physical parts such as the possibly insiders attacks, which may be industries like assembly parts may cause to failure any physical part of vehicle and resultant a serious incident in VANET, our highlighting in this section is based on the weaknesses of the technologies which trigger the cybercrime, we classified the cybercrime in VANET according to the technologies are used in VANET shown in figure 2. And in table 1; present

Journal of Advanced Research in Computing and Applications
ISSN (online): 2462-1927 | Vol. 2, No. 1. Pages 25-38, 2016

the analysis of each technique along with their trail, influence, and planning's for response and countermeasures for cybercrime.

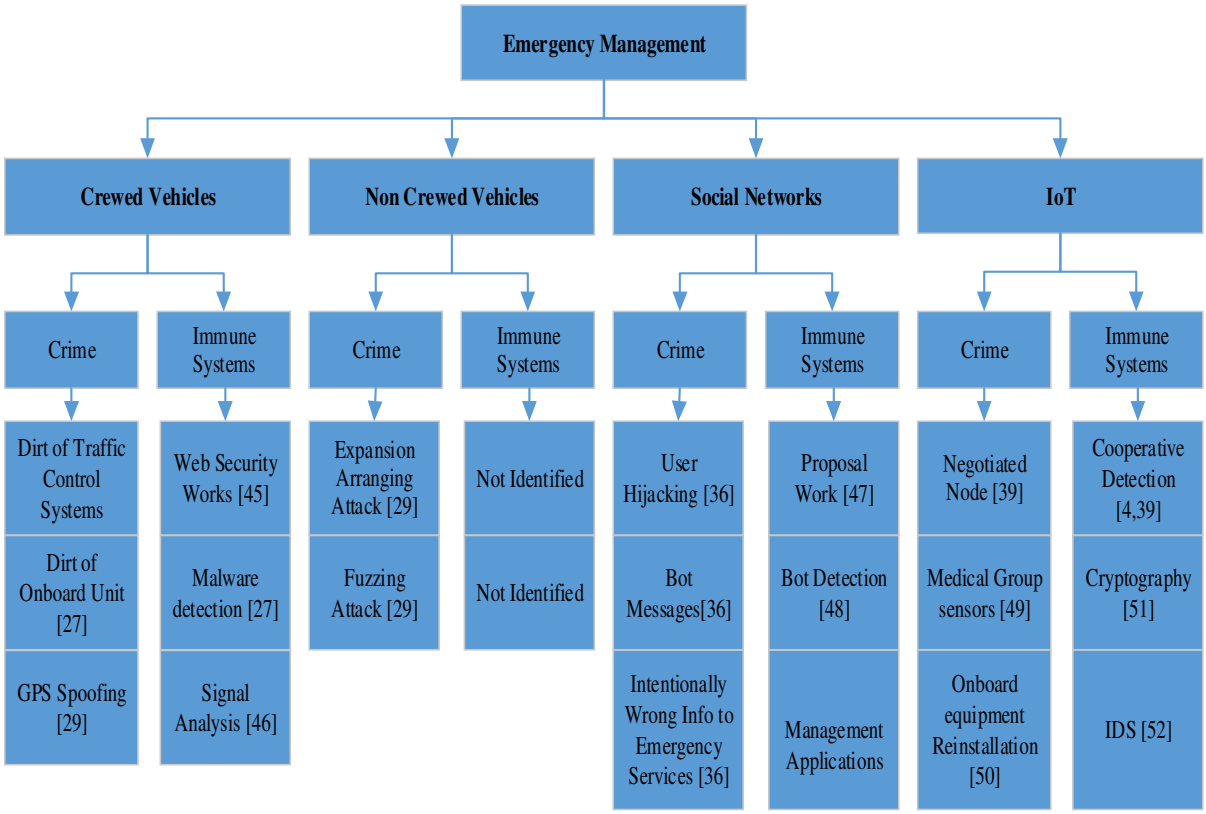

Figure 2: Classification of Cybercrime and Immune Systems in VANET

1.1.1 Crewed Vehicles

The crewed vehicles used for the emergency purpose as well response, at the time of unexpected events or reaction of disaster mean, the crewed vehicles are used for recovery or initial reaction or stage of any attack as a rescue, which are well trained to mitigate the cybercrime or disaster at urban areas and highways. In the urban areas the intelligent transportation region, the cyber-attacks accrued typically due to interruption in positioning as well signaling, for instance at the time of 1990s the major problem accrued due to the absence of node authentication tools, the attackers as well hackers linking through a modem to an airplane station network imagining considered as an authentic system management and varying the serious evidence of data or any information. And at the time of the 2000s the malware and battered cyber-attacks disturb the transference, which is comparatively mutual, particularly in airports [24].

The rapidly employee of off-the-shelf running environments operating systems, the common number of unexpected events accrued in the transport region due to mutual worms as well

Journal of Advanced Research in Computing and Applications
ISSN (online): 2462-1927 | Vol. 2, No. 1. Pages 25-38, 2016

viruses, which are spread through the use of internet and running the operating systems without any intrusion detectors generally, for instance a virus deactivating air traffic regulator organizations of Alaska in 2006 [25]. Hitherto, in general, it is considered that it was free from malicious, it was free from damage according to documents and evidence. By the year 2008 a youngster achieved control tram system in Lodz, Poland, and run its path switches, so the sum up for this issue challenged to four trains to derail along with fourteen people hurt [26].

The motorized manufacturing is also progressively viewing attention in cybercrime, partially the cause of remote events of cyber interruptions in contradiction of targeted vehicle type [27]. By the year 2010, the prediction discussed as well conformed that it is probable to infect a vehicle network through connectivity of other additional sensors and other devices used to achieve the control of vehicle locks, emergency brakes as well vehicle assembly parts such as engine control along with other circuits, probably a vehicle delayed by involuntary to turn nearest other track although the dynamic at speed.

Whereas these kind of weaknesses conclude with accurate evidence and testing, the main question is arise that it sham important worry in the context of EM, by way of it does not measure simply sufficient to basis large measure interruptions. If we view the accident's history in Austin, Texas, the number of vehicles can be at the same time danger by unpredicted way over a web-based vehicle-immobilization system. Hence, the overall sum up it is mostly exciting that hundreds of vehicles to be individually immobilization [28] by a website's security fault which an unintended physical impact.

1.1.2 Non-Crewed Vehicles

Non-crewed vehicles are started to use for citizen determinations, with law enforcement and emergency response, which provides the awareness and coordination based on situations, while non-crewed vehicles face a lot of unexpected events and incidents. The fuzzy attack, which is done by injects unsystematic inputs to the vehicle's actuators [29], similarly untechnical top level analyzing of the probable impact of cybercrime on non-crewed vehicles are discussed in the vehicles which are under control an autonomous or semi-autonomous remotely-controlled way gradually suggested and trialed for EM. For instance these vehicles first responders and functionality of an infrastructure [30]. While non-crewed vehicles are characteristically not used in the mean of information security, in general, the vulnerable to various nature of attacks disturbing the broadcasting of dangerous situation updates or warning information. The detail of these type of cyber-attacks are presented in [31].

1.1.3 Social Networks

Emergency facilities and services are used in web-based alert systems and warning systems by the community support [32], the majority of social networks newly designed the policies for emergency response in mean to mitigate the cybercrime as well attacks. In general, the local and global establishments is participating the alerting and warning messages to their users and followers, for instance, Facebook groups, Twitter groups and other social accounts [33].

The example is present in the history, by the year 2010, which is about, when the flood happen in the central Europe, at that time the central authority of Poland create a group which used to alert and inform about localized flood, this method was considered as efficient as compare

Penerbit Akademia Baru

Journal of Advanced Research in Computing and Applications
ISSN (online): 2462-1927 | Vol. 2, No. 1. Pages 25-38, 2016

to traditional communication methods [34]. As the Twitter communication is possibly delivered geo location info that can be priceless, while it is not extensively using when the emergencies happened until now not getting into the use of it [35].

The majority of crime and incidents reported as hijacking accounts of social networks which are dependable only single username and passwords, the passwords are also dependable on the user, for instance, some user use weak and some user uses strong passwords for their authentication and authorization. In general, the social network's user accounts can be compromised.

The detailed in [36], which is highlighted the procedure of relay attacks the Facebook and twitter user accounts and gives some tips which are involved the crime as well attack on Facebook. The relay attack also can be considered as a Sybil attack where a user holds the multiple identifications as well fabricated accounts into the social network so the Sybil user can share the wrong information and victim the policies and spy the users by their fake profile accounts.

Table 1: Analysis of Cybercrime, Trail, Influence, and Planning

Author	Trial			Influence					planning		
	Theoretical	Protocol	Simulation	Confidentiali	Integrity	Authenticatio	Authorizatio	Availability	Detection	Response	Technical
Gelenbe, et al		×	×	×	×	×	×	×	×	×	×
Walker, J	×			×	×			×			×
Cerchio, & Riley	×			×	×			×			
Storey	×				×						
Kim, A. et al			×	×	×			×			
Hiltz & Gonzalez	×				×						
Mitchell et al				×	×				×		
Chu et al.		×	×		×				×		
Malan et al		×		×	×		×	×			
Zeng et al		×			×				×		

1.1.4 Internet of Things

The use of multiple sensor nodes and circuits in network as well the internet is using for safety monitoring, for instance, the application in 5G, the research is ongoing for implement the 5G which gives the applications about health conditions, for instance in the local ecological, health monitoring, similarly in body area networks for health monitoring [37]. In these approaches meets the possible number of cybercrime as well attacks which are dangerous for emergency response in sensor networks and on the internet. It would aim only detection the

Journal of Advanced Research in Computing and Applications
ISSN (online): 2462-1927 | Vol. 2, No. 1. Pages 25-38, 2016

sensor nodes insert bad data, the disorder connection as well drain the energy of sensor nodes [38], Through the Sybil node the confidentiality of data can be compromised as well by sinkhole [39], as it is also studied that through the Sybil node can be create the multiple identities for appearance into various layers of protocol stack [40].

Sybil nodes possibly generate the fake links which responsible to modification into data as well messages in the network [41]. In [42] the author proposed a procedure to the employee the fuzzy logic which chain with the real-time network data and physical contribution topographies, along with the variation among the ration of informed by neighboring or surrounding sensors.

1.2 Overview of Security Work

Industries and researchers brings the ideas and help to protect and mitigate the security attacks against network, many of authors contribute to VANET security, for instance in [43] author proposed a hardware for recording all possible information, also in [43] author proposed to assign the unique identification and so on, each work solved some security related issues by applying different techniques and comprehended the security challenges which are needed to protect the VANET and make it free from possible attacks, we classify the possible security recommendation in figure 3.

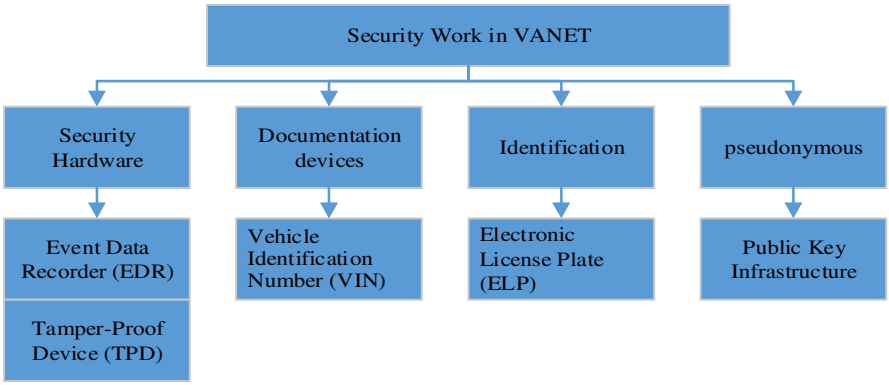

Figure 3: Security Work in VANET

1.2.1 Hardware Tools

Each vehicle is assembled an onboard unit as per security requirements it is considered that in each vehicle must be assemble two additional hardware's which are, 1. Event Data Recorder (EDR) and 2. Tamper-Proof Device (TPD). The functionality of EDR is to offers the unaltered data which can use for analyzing the event or any type of incident.

EDR records all type of events and activities during the drive, this idea is the similar approach of Black Box in airplanes, in vehicles, EDR records the vehicle's position, speed time, and critical emergency situations [43] and TPD is offered to help in cryptographic running

Journal of Advanced Research in Computing and Applications
ISSN (online): 2462-1927 | Vol. 2, No. 1. Pages 25-38, 2016

competences. EDR is help for investigation the crime and attacks but the limitation of EDR is that it may not support the globally detection of cybercrime, it may intentionally can disappear or may be physical damage to the device when if need of serious investigation of any crime.

Since 1948, it is recorded that the 88 aircraft disappeared without a trace, it is historical proven if black box is not recovered then it is hard to investigate or intentionally disappearance the black box at the time of investigation, so it can say that the only physical device is not enough to record the emergency events or unexpected events, the figure 4; shows the disappearance of airplanes reported at [44].

1.2.2 Identification Tools

The Identification is also challenging part of VANET so the industries of vehicles companies decided to assembles each vehicle with a Vehicle Identification Number (VIN) during the manufacturing, the purpose behind this approach is to assign the unique identification to each vehicle, which help the privacy and integrity of vehicle as well identification into the network, the vehicle can be tracked by using their VIN for investigation [43]. VIN can be prevented against non-repudiation attacks which are serious attacks for trustworthy into the network, for instance after circulated any emergency report the vehicle must not deny at the time of the investigation.

1.2.3 Authentication Tools

The identification of electronic devices such as a vehicle which has a circuit of identification named Electronic License Plate (ELP). it is use for electronic identification, the vehicle assigned a unique identification, through ELP a vehicle can be investigate and locate the position of vehicle as well the ELP also help to privacy as and it can be used for authentication and authorization purpose by cryptographic techniques and methods, as TPD is supportive tool to reserve the competency which can use for cryptographic mean, as many of researcher purposed to use the ELP to assign the authentication into the network, the ELP holds the database of public key certificates and cryptographic schemes to secure the privacy of each vehicle in the network. The use of ELP can be prevented against the Sybil attack and maintain the integrity of data, information and broadcast the warnings.

1.2.4 Pseudonymous

The third party which is performing as trusted authority is involved for Pseudonymous certificates, the certificates are based on trusted authority into the vehicle network, for instance, the vehicular public key infrastructure is an assumption for the vehicular network. The trusted third party is managing the structure and administration of Pseudonymous certificates which is considered as a hierarchical based structure, it has a certificate authority for each region, for instance, country to the country or region to region.

2.0 PROPOSED METHOD

As VANET is currently ongoing research on security challenges to mitigate the attacks, some attacks are more dangerous for drivers and vehicles, as it studies many of accidents occur due to wrong information or fake identification, it is notified that some of the crimes are very serious in term of physical disaster and financial losses, until now the EM is planning to

Penerbit Akademia Baru

Journal of Advanced Research in Computing and Applications
ISSN (online): 2462-1927 | Vol. 2, No. 1. Pages 25-38, 2016

protect the VANET from cybercrime and incidents which are challenging for open nature networks.Our assumption for EM is Cloud Based Recorder, which can be employed to look forward to investigation purposes by accurate evidence, as many of social networks are participating into VANET comfort applications and as per literature the social network groups can be used for alert the dangerous situations, as before the social network groups [33] are used to alert as community-based.

In the paper discussed about EDR [43] which is proposed to record the vehicle events, our assumption is similar example of EDR which record the events into the vehicle , but the limitation of EDR is not supportable in global level, for instance if any vehicle's EDR destroyed or intentionally hide for investigation then it is difficult the get data or information for investigation, due to the limitation of global level investigation or unavailability of EDR hardware for instance when if an attacker tries to hide its EDR then it is difficult to investigate and produce the accurate result of event or incident, so we proposed the CBR which is cloud based and reliable to investigate the globally for crime as many of EM systems are web-based which gives the response and rescue, the CBR is responsible for recording all events such as position, speed, time and emergency situations which can be used to investigation of any crime, it can support the globally and base on CBR can be detect the cybercrime in VANET.

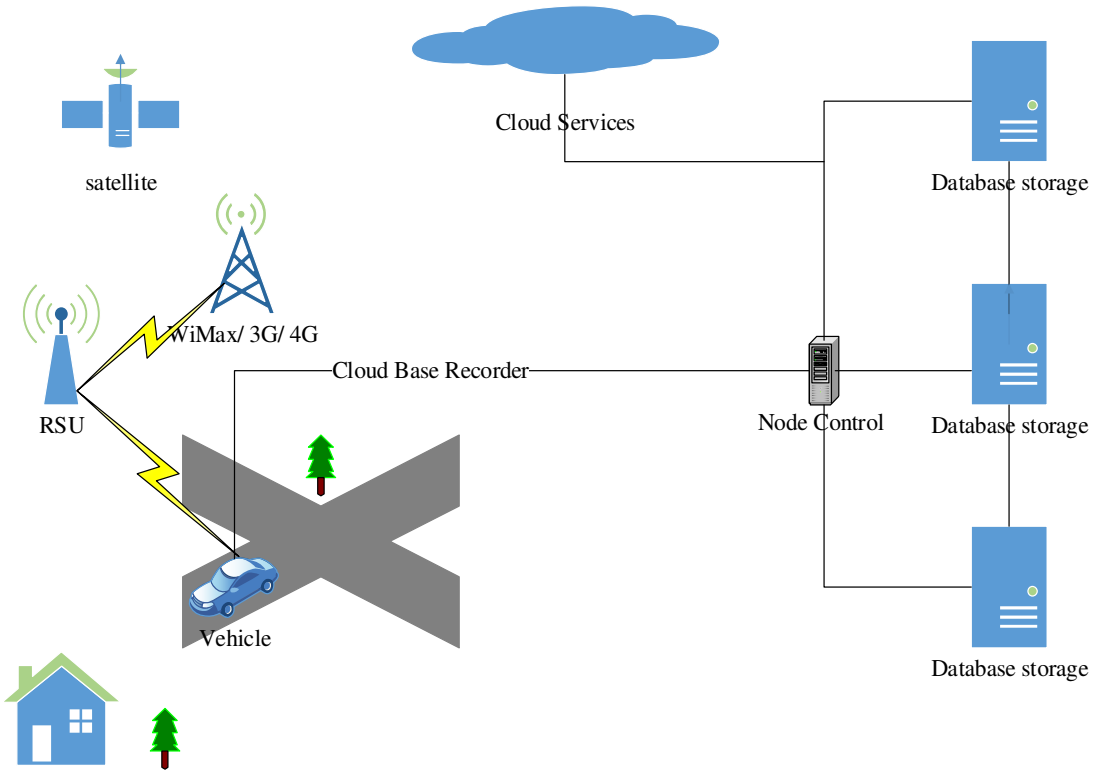

Figure 4: Proposed Cloud Based Recording for VANET

Our proposed CBR is present in figure 4, the CBR is consists of web-based Database which records the events of each vehicle and EM is directly linked to CBR which analyzes the

information by comparing the variation of vehicle if any criminal activity is detected the EM is responsible for taking action against that vehicle, the main challenge is to develop the tool which records all evidence and analyzes the attacks from EM, it can be used as well globally for detection of serious crime.

3.0 CONCLUSIONS

The value of up-to-date emergency response depends on the continuous process of a variety of information and response systems. As it is studied of various papers notified a cybercrime can be secondhand to backing criminal events which are tempering a threat earlier a physical attack, as well, it may produce horror and misperception. However, generally many of researcher's work on the EM systems by focusing on defensive methodologies that are considered a privacy and authentication basis by using the cryptographic tools and techniques for broadcast the information and authorization.

It must be to accept that a committed criminal individual or group they would like to assistance a parallel devices threat which perhaps usage the social engineering can bypass the privacy and authorization, the DoS threat can gain the accessibility instead of the integrity of the EM infrastructure. While accessibility of services of network reliably accessible as a key concern in a mutual cybercriminal attack [28], until now it considered a significant absence of an applicable Emergency response for particular prevent techniques which have advanced over the level of theoretical investigation.

We proposed the CBR for investigation the cybercrime globally which can help to prepare the rescue according to the analysis of CBR, which can alert any serious crime at the initial time. We provide a survey on VANET cybercrime along with their countermeasure techniques and their influence on the EM trends external factors, emphasizing on the challenges for research. We observed through literature review that an imposing issues for VANET EM the development of prevent tools, as the research is ongoing to secure and accurate use of Intelligent transportation, the major issue is to develop the tools in open nature network like VANET that can help to analyze and calculate the real influence of such cybercrime, overall sum up the cybercrime is serious challenge in VANET in term of casualties and financial losses.

REFERENCE

[1] C. D. Wang, J.P. Thompson, Apparatus and method for motion detection and tracking of objects in a region for collision avoidance utilizing a real-time adaptive probabilistic neural network, US, 1997.

[2] US Dept. Transp, Vehicle Safety Communications Project Task 3 Final Report, 2005.

[3] M. Bahrepour, N. Meratnia, M. Poel, Z. Taghikhaki, P.J.M. Havinga, Distributed Event Detection in WSN for Disaster Management, Proceedings of the 2nd International Conference on Intelligent Networking and Collaborative Systems, Greece (2010) 507-512.

[4] E. Gelenbe, F.J. Wu, Sensors in Cyber-Physical Emergency Systems. Proceedings of the IET Conference on Wireless Sensor Systems, UK, 2012.

[5] A. Filippoupolitis, L. Hey, G. Loukas, E. Gelenbe, S. Timotheou, Emergency Response Simulation Using WSN, Proceedings of the 1st International Conference on Ambient Media and Systems, Canada, 2008.

[6] D. Fave, A. Rogers, N. R. Jennings, A Coordination System to Provide First Responders with Live Aerial Imagery of the Scene of a Disaster, Proceedings of the 11th International Conference on Autonomous Agents and Multiagent Systems, Valencia, Spain 3 (2012) 1467–1468.

[7] C. White, L. Plotnick, J. Kushma, S. R. Hiltz, M. Turoff, An online social network for emergency management, Proceedings of the 6th International ISCRAM Conference – Gothenburg, Sweden, May 2009.

[8] D. Yates, S. Paquette, Emergency knowledge management and social media technologies: A case study of the 2010 Haitian earthquake, International Journal of Information Management 31 (2011) 6-31.

[9] D. Dudenhoeffer, M.R. Permann, M. Manic, A Framework for Infrastructure Interdependency Modeling and Analysis, Proceedings of the 2006 IEEE Winter Simulation Confeference, Monterey, USA (2006) 478-485.

[10] D. Dudenhoeffer, M. R. Permann, S. Woolsey, R. Timpany, C. Miller, A. McDermot, Interdependency Modeling and Emergency Response, Proceedings of the 2007 Summer Computer Simulation Conference, San Diego, CA, USA (2007).

[11] J. S. Sengar, SURVEY: Reputation and Trust Management in VANETs, International Journal of Grid and Distributed Computing 9 (2016) 201-206.

[12] M. N. Rajkumar, M. N. P. HemaLatha, Overview of VANET with its features and security attacks, International Research Journal of Engineering and Technology 3 (2016) 137-142.

[13] I. Bhardwaj, S Khara, An Analytic Study of Security Solutions for VANET, International Journal of Computer Applications 132 (2015) 1-7.

[14] L. Kumar, P. K. Dahiya, Performance Evaluation of the Techniques to Mitigate Blackhole Attack in VANETs, International Journal of Applied Information Systems 9 (2015) 69-72.

[15] X. Feng, C. Yan Li, D. Chen, J. Tang, A method for defensing against multi-source Sybil attacks in VANET, Peer-to-Peer Networking and Applications, (2016) Article in Press.

[16] S. Al-Sultan, M.M. Al-Doori, A.H. Al-Bayatti, A comprehensive survey on vehicular Ad Hoc network, Journal of Network and Computer Applications 37 (2014) 380-392.

Journal of Advanced Research in Computing and Applications
ISSN (online): 2462-1927 | Vol. 2, No. 1. Pages 25-38, 2016

[17] I.A. Sumra, H.B. Hasbullah, J.B. AbManan, Attacks on security goals (confidentiality, integrity, availability). In: VANET: a survey. Vehicular ad-hoc networks for smart cities. Singapore (2015) 51-61.

[18] A. Mohaisen, S. Hollenbeck, Improving social networkbased sybil defenses by rewiring and augmenting social graphs. Information security applications. Springer International Publishing (2014) 65-80.

[19] V. Raghuwanshi, S. Jain, Denial of Service Attack in VANET: A Survey, International Journal of Engineering Trends and Technology 28 (2015) 15-20.

[20] G. Kaur, S. Rani, T. C. Aseri, An Analytical Study towards mitigation of Grayhole Attack in VANET, International Journal of Scientific & Engineering Research 6 (2015) 815-820.

[21] J. Walker, Cyber Security Concerns for Emergency Management. In Emergency Management, InTech: Rijeka, Croatia (2012) 39-59.

[22] P. Falcarin, C. Christian, A. Mikhail, J. Mariusz, Introduction: Software protection, IEEE Software (2011) 24-27.

[23] S.S.P. Madhava, K. Jaishankar, Cyber Terrorism: Problems, Perspectives, and Prescription, Crimes of the Internet, ACM Digital Library: USA (2008) 593-611.

[24] R.J. Turk, Cyber Incidents Involving Control Systems, US-CERT Control Systems Security Center, USA (2005).

[25] R. De Cerchio, C. Riley, Aircraft Systems Cyber Security, Proceedings of IEEE DASC, Seattle, WA, USA (2011).

[26] D. Storey, Securing process control networks, Network Security 10 (2009) 10-13.

[27] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, Experimental Security Analysis of a Modern Automobile, Proceedings of the IEEE Symposium on Security and Privacy, USA (2010) 447-462.

[28] E. Schoitsch, Cyber-Physical Systems What Can We Learn from Disasters with Respect to Assessment, Evaluation, and Certification/Qualification of Systems-of-Systems? Proceedings of 20th IDIMT Conference, Czech Republic (2012) 69-81.

[29] A. Kim, B. Wampler, J. Goppert, I. Hwang, H. Aldridge, Cyber Attack Vulnerabilities Analysis for Unmanned Aerial Vehicles, The American Institute of Aeronautics and Astronautics: USA (2012).

[30] G. Loukas, S. Timotheou, E. Gelenbe, Robotic Wireless Network Connection of Civilians for Emergency Response Operations, Proceedings of the 23rd IEEE ISCIS, Turkey (2008).

Journal of Advanced Research in Computing and Applications
ISSN (online): 2462-1927 | Vol. 2, No. 1. Pages 25-38, 2016

[31] T. Kohno, Security for Cyber-Physical Systems: Case Studies with Medical Devices, Robots, and Automobiles. In Proceedings of the 5th ACM (WISEC), USA (2012).

[32] D. Bunker, S. Smith, Disaster Management and Community Warning Systems: Inter-Organizational Collaboration and ICT Innovation, Proceedings of the Pacific Asia Conference on Information Systems, India (2009).

[33] S.L. Magsino, Applications of Social Network Analysis for Building Community Disaster Resilience, The National Academies Press: Washington, DC, USA (2009).

[34] W. Wojciechowicz, J. Zych, W. Hołubowicz, Information and communication technology and crisis management, Technical Sciences 15 (2012) 101-110.

[35] K. Kreiner, G. Neubaur, Social Media for Crisis Management: Problems and Challenges from an IT-Perspective, Proceedings of IDIMT, Czech Republic (2012).

[36] S. Mahmood, New Privacy Threats for Facebook and Twitter Users, Proceedings of the Seventh International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), Canada (2012) 164-169.

[37] K. Lorincz , D. J. Malan, T. R. F. Fulford-Jones, A. Nawoj, A. Clavel, V. Shnayde, G. Mainland, M. Welsh, S. Moulton, Sensor networks for emergency response: Challenges and opportunities. IEEE Pervasive Computer 3 (2004) 16-23.

[38] R. Mitchell, I.R. Chen, A Hierarchical Performance Model for Intrusion Detection in Cyber-Physical Systems, Proceedings of the IEEE WCNC, Mexico (2011) 2095-2100.

[39] G.W. Skelton, Cyber-Physical Security for Wireless Sensor Networks, In Proceedings of the Workshop on Future Directions in Cyber-Physical Systems Security, USA (2009).

[40] X. Liao, D. Hao, K. Sakurai, Classification on Attacks in Wireless Ad Hoc Networks: A Game Theoretic View, Proceedings of 7th International Conference on Networked Computing and Advanced Information Management (NCM), Korea (2011).

[41] J. Lin, W. Yu, X. Yang, G. Xu, W. Zhao, On False Data Injection Attacks against Distributed Energy Routing in Smart Grid, Proceedings of the ACM/IEEE 3rd International Conference on Cyber-Physical Systems, China (2012).

[42] Y. J. Chen, J. S. Shih, S. T. Cheng, A Cyber-Physical Integrated Security Framework with Fuzzy Logic Assessment for Cultural Heritages, Proceeding of the IEEE International Conference on Systems, Man and Cybernetics, USA (2011).

[43] B. Parno, A. Perrig, Challenges in Securing Vehicular Networks, Proceeding of HotNets-IV (2005).

[44] Aviation Safety Network, Available at http://www.thejournal.ie/since-1948-88-aircraft-went-missing-without-a-trace-two-off-the-irish-coast-1372638-Mar2014, 2014.

[45] M. Jensen, N. Gruschka, R. Herkenhöner, A survey of attacks on web services, Computer Science - Research and Development 24 (2009) 185-197.

[46] Q. Zeng, H. Li, L. Qian, GPS Spoofing Attack on Time Synchronization in Wireless Networks and Detection Scheme Design, Proceedings of the Military Communications Conference (MILCOM), USA (2012).

[47] S.R. Hiltz, J.J. Gonzalez, Assessing and Improving the Trustworthiness of Social Media for Emergency Management: A Literature Review, Proceedings of the Norwegian Info Sec. Conf. (NISK), 2012.

[48] Z. Chu, S. Gianvecchio, H. Wang, S. Jajodia, Detecting automation of twitter accounts: Are you a human, bot or cyborg? IEEE Transactions on Dependable and Secure Computing 9 (2012) 811-824.

[49] D. Malan, T. F. Jones, M. Welsh, S. Moulton, An Ad Hoc Sensor Network Infrastructure for Emergency Medical Care, Proceedings of the International Workshop on Wearable and Implantable Body Sensor Networks, UK (2004).

[50] J. Kallberg, Designer satellite collisions from covert cyber war, Strategic Studies Quarterly (2012) 124-136.

[51] M. Li, W. Lou, K. Ren, Data security and privacy in wireless body area networks. Wireless Communications, IEEE 17 (2010) 51-58.

[52] T.V.P. Sundararajan, A. Shanmugam, A novel intrusion detection system for wireless body area network in health care monitoring, Journal of Computer Science 6 (2010) 1355-1361.