ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com

Classification of Anomaly Based Intrusion Detection Systems in VANET

[1]Fahad Nazir Bhatti, [2]R Badlishah Ahmad, [3]MNM Warip, [4]Hamid Mohammad Bhatti

[1, 2, 3] *School of Computer and Communication Engineering, Universit of Malaysia Perlis,* 02600, Arau, Perlis, Malaysia.
[4] *Institute of Information & Communication Technology, University of Sindh, 76080 Jamshoro, Hyderabad, Pakistan.*

ARTICLE INFO

Article history:
Received 13 June 2015
Accepted 28 July 2015
Available online 5 August 2015

Keywords:
VANET, Security, Intrusion Detection System

ABSTRACT

Security is a serious task in the vehicular ad hoc network (VANET), the first level of counter measure the security attacks are cryptography, and the authentication which is designed for known attacks. While for unknown attacks a counter measure system for detect the malicious or attacks is Intrusion Detection Systems (IDS). This paper is designed in twofold, first we review the various techniques of Anomaly Based IDS (ABDIS), and classification of all ABIDS techniques in VANET, second we analyze the common techniques of ABIDS, and the comparison of Knowledge base techniques, Data mining techniques, statistical techniques, and Machine learning techniques are present along with their fundamental characteristics, advantages and limitations of each of the techniques. Finally, we proposed a cloud based intrusion detection technique which uses the cloud server and the database of fingerprints to measure the intrusion activities and unexpected events which helps to secure the communication of VANET, we are analyzing the performance of our proposed Cloud Based IDS.

To Cite This Article: Fahad Nazir Bhatti, R Badlishah Ahmad, MNM Warip, Hamid Mohammad Bhatti., Classification of Anomaly Based Intrusion Detection Systems in VANET. ***Aust. J. Basic & Appl. Sci.,*** *9(25): 24-29, 2015*

INTRODUCTION

Vehicle ad hoc network (VANET) is sensitive than other devices like Mobile ad hoc network, every year death happened on roads, cause of accidents and collisions of vehicle the most important is human life than device, devices can be reproduce but human life once lost then it never ever can be recover, security is main concern in VANET because of data transmission as well confidentiality, integrity and availability, as traditional techniques to measure the malicious only useful for wired networks while this is wireless ad hoc network so the intrusion detection system is favorable for detect the malicious. This era drivers dreaming of avoiding traffic congestion, get up-to-date information about road condition, traffic jams, finding parking lot, over tracking alerts, warning messages, collision control, line change, intelligent traffic lights, speed controlling alerts, driver health condition, weather condition, fuel stations, and many more. The important portions of VANET are vehicle2vehicle (V2V), vehicle2roadside (V2R) or Vehicle2Infrastructure (V2I), vehicle to all (V2X) and intelligent transportation systems (ITS) claimed to give safety and reduce the death caused by accidents and collisions of vehicles, the advancement in VANET federal communication commission United States invest billions for communication medium that is Dedicated short Range Communication (DSRC) the channel 5.885-5.895GHz is capable for transmit and receive alerts. DSRC characteristically regulated 6 up to 27 mbps with data rate in excess of 1000m is the actual range calculated (N.Lyamin, *et al*, 2013). DSRC is standing on 802.11aIEEE regulated and 1609IEEE, operational panel is being regulated as IEEE802.11p for mean to vehicular communication [4], WirelessAccess in Vehicular Envir: (WAVE) policy is designed for faster velocity of cars by little changing into PHY IEEE and activated IEEE 802.11p communicate roadway surroundings [Jiang, 2008]. Via many other authors notified security risks and challenges (I.A.Soomro, 2010) and (Jiang, 2011). The security requirements are presents in table 1

Table 1: Security Requirements

Confidentiality	It is also known as confidential communication (Mittag *et al*, 2008) for instance cryptography, the transmitted message is only encrypt within the group members.
Integrity	It prefers the authentication to make sure if once the data is sent is authenticated by check the integrity that the message contained correct or incorrect data, make sure the data is directed and engaged by another node without any modification by another node.

Corresponding Author: Fahad Nazir Bhatti, School of Computer and Communication Engineering, Universiti of Malaysia Perlis, 02600, Arau Perlis, Malaysia.
E-mail: fahadnazirbhatti@gmail.com

Availability	It prefer the availability of network which is most important to make it accurate and useful of this open nature of network, the serious risk of availability in open nature network is DoS, an attacker can be violate the network security if availability is not functional in a proper way.
Privacy	It prefers personal identification, the identification shouldn't disclose to unauthorized nodes, message transmitting between vehicle and infra-structure or vehicle and vehicle is difficult to resolve whether two various messages communicating from same vehicle.
Tracking & Revocation	It prefers the identification must be hidden to other vehicles and only legal authority hold access to identify vehicle identity (Trace Manager) to revoke then and keep maintain for future use or need.
Non-Repudiation	It prefers to node/driver must dependably identification in case of accident/disaster, node should be follow responsibility to transmitting the data/packet for further investigation for calculate the accurate sequence and content of data/packet swapped before event/accident (Raya, 2007).
Real-Time Control	It prefers the leaving and joining group because vehicles are moving with fast speed so nodes are moving faster for short-time so constraints must be sustained.
Low-Overhead	It prefers the time and validity of transmitted data/packet, all messages are punctual to time, therefore lowoverhead is vital to hold and strength of data/packet.

In the signature IDS maintain the history of known attacks that compare with stored signatures or certificates, the major limitation of this method for instance, it is only follows the stored history of an attacker and do not capable to recognize the new attacks. Because of this reason anomaly IDS takes attention to researchers for mitigating new attacks. The major strength of ABIDS that it can detect the novel attacks that help to mitigate new attacks.

In this paper, we introduce a classification of classification of an ABIDS in VANET according to their fundamental characteristics, and analyze the performance of each techniques by comparisons of their advantages and limitations. Finally we proposed a cloud based Intrusion Detection Technique, which use the cloud server and database of fingerprints to detect the malicious activities which helps to secure the communication of VANET, The article is systematized as follows; section 2 describes the Vehicular security, in section 3 describe Overview of IDS, in section 4 Proposed Cloud Based intrusion detection technique, and in section 5 conclusion of the present work.

II. Vehicular Security:

The Vehicular technology is a novel study area for researchers and developers, the authentications and authorization in vehicular network (Plossl *et al*, 2006), (LiuX.Fang *et al* 2007), and (Papadimitratos *et al* 2007) widely employed the public key infrastructure as well digital certificates which are proposed from many authors to protect the security of vehicular network, the authors (Plossl, LiuX.Fang and Papadimitratos) considered an appropriate approaches for challenging issues on vehicular network for instance authentication and authorization. In order to reduce the load of work the third party is employed for supervision the vehicular certificate's such as issuance, circulation, endorsement and reversal of certificates the author (Papapanagiotou, 2007) designed a certificate validation approach which is depends on circulation version of OCSP for perseverance of authorization and authentication in vehicular network. While In this approach the privacy is challenging because it not taken a look in this approach. The author (Raya *et al*, 2006) proposed a certificate reversal model, and the major parts of model RC2RL, RTPD and DRP, each part is performs the unique job, the full detail is available in (Raya *et al*, 2006). The author (Fischer *et al*, 2006) author designed SRAAC protocol which enables to circulate the certificates unsigned message authentication with minimum based blinded certificate, the reversal and separation of misbehaving cars, the SRAAC use the magic Ink-DSS, which is an algorithm of digital signature while the limitation of this approach is noticed that a car distinguished as malicious cannot be rescinded in mean time since this approach is issue the certificates which are based on their previous stored memory in their onboard unit. The author (Moustafa *et al*, 2006) presented the approach which is an appliance for access control that use the Kerberosl, in this work the author designed an authentication and authorization appliance to access offered service via a previous token, furthermore it is authenticated the car at the entry point of road, the work in this approach is done only for highway scenario. The authors (Aijaz *et al*, 2006) and (Parno & Perrig, 2005) presents a comprehensive investigation of common method threats on InterVehicle Comm (IVC) as well gives the comprehensive challenges in vehicular network and notified the major need of this network is privacy. The author (Choi *et al*, 2005) designed an approach which deal the balance auditability and privacy in vehicular network this approach is based on symmetric cryptographic as well twofold sorts of pseudonyms for instance, short term and long term. The author (Lu *et al*, 2008) designed a protocol for privacy which follow the conditions by suggesting short-time anonymous key generation.

III. Overview Of Intrusion Detection:

It can be divided into two ways, the circuit and also can be an medium the main purpose is to detect malicious, it also can be classified as host-based which performs the security measurement on operating system for evaluate the log files and for audit data to identify the attackers or malicious activates, which are based on user activities, for instance it monitor the running processes in the task manager of operating systems, and in the network based performs the security measurements on data packets for identify the attackers or malicious on the network, for instance, it examine the packets that goes through the medium (P.Innella & O.McMillan, 2001). In general the intrusion detection divided into signature based , anomaly based and specification based, our focus is to classify anomaly based IDS, which are classify all possible techniques, we review various types of ABIDS. And summarized as Knowledge base, Data Mining base, Statistical base, and Machine Learning base. The complete classification of ABIDS is shown in figure 1.

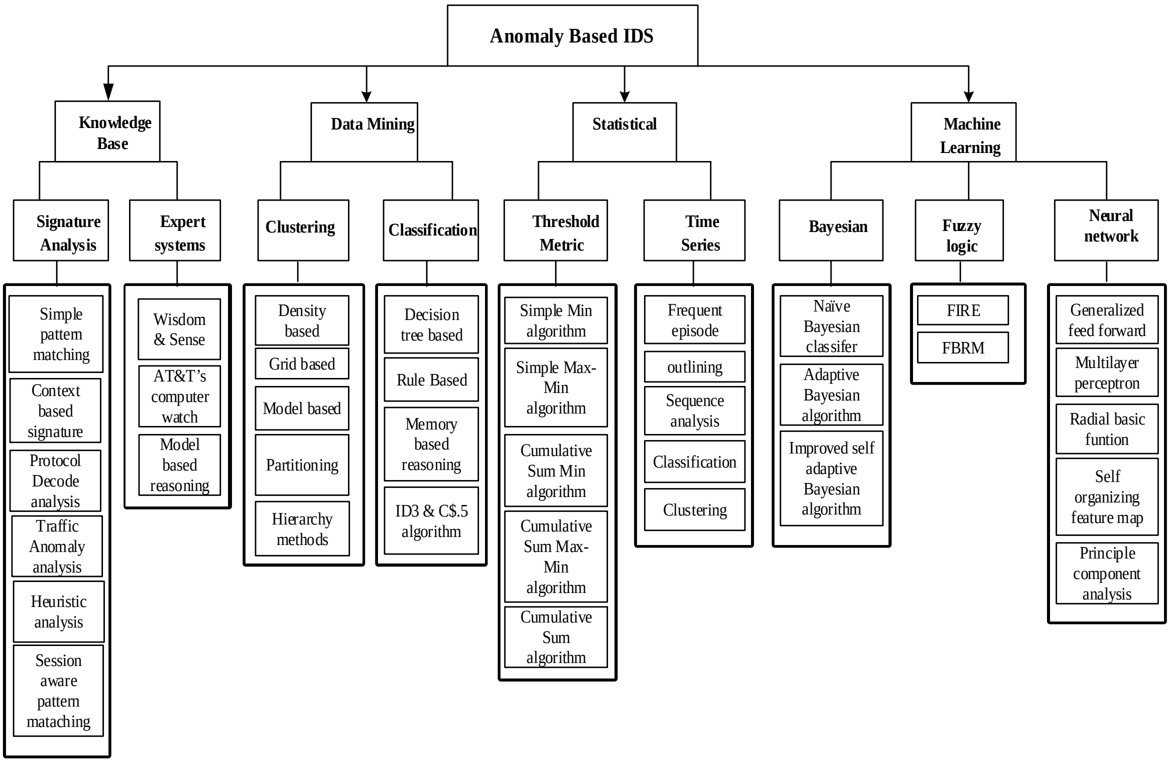

Fig. 1: Classification of Anomaly Based IDS

A. Anomaly based Intrusion Detection Techniques:

The anomaly based IDS is classified in four major parts 1. Knowledge base, 2. Data Mining, 3. Statistical and, 4. Machine learning. In the knowledge based technique the counter measure the attack is done by signature analysis and expert systems, the signature analysis technique is widely used for counter measure the security attacks or malicious, this technique is widely used to identify intrusion by Database to match the captured vehicle. The database is needed for full fill the requirements of this methods because this technique need a data base to store all signatures to match the versions, after match it can be label the vehicle either malicious or normal. And the other one which is the expert system also based on knowledge based technique, in the Expert System run with the help of interface human-,interface machine, predictor, and so on. This technique is a server based where an administrator take care of its server for identify the malicious activities within defined guidelines and procedure along with known behavior which is matching and comparing the traffic for detection purpose and label with normal or abnormal vehicle the techniques are used for expert systems in (H.S.Vaccaro and G.E.Liepins, 1989), (Cheri.D and Paul.R, 1990) and (Thomas.G and Teresa.L, 1991).

The Data Mining Base has two techniques 1. Clustering and 2. Classification, the Clustering technique is known type for open nature network for security measurements and as well other area of computing, the clustering basement has two major parts, 1. Client clustering and admin-clustering. The techniques are used for detect the malicious is in (Jian.P *et al*). And the other technique of data mining is Classification which is a learning approach that learn from predication, training by the data review, which is look on results which are predicted. The techniques of classification are in (Mohd.E *et al*, 2010).

The Statistical Base has two major approaches which are 1. Threshold metric and 2. Time series, the Threshold Metric approach holds values or ratio of a rule to alert the alarm for unexpected events or malicious activities as well comparison based. Threshold depends on assumed value once the vales matches as per defined then an alarm will alert about attach. For instance a login time period which based on attempts, if attempts more than defined time then an alarm trigger The threshold algorithms presents in (Vasilios.A.S, and Fotini.P, 2006), and simple and cumulative algorithms are discussed in (Alexandros.G.F *et al* 2010), and other technique of statistical is Time series model that detect the malicious based on time, which check the time in and time out and an array In the time series if performance prospect of an event is decrease, then it treat as malicious the capability of time series model that it is flexible to generate the time based events of the users (James.C.J.H, 1996).

The machine learning has three major approaches, 1.Bayesian, 2. Fuzzy logic and 3. Neural Network, in the Bayesian approach which is focus on a construction of training fuzzy expert knowledge in expert-systems. The Bayesian is use for counter measure the attacks or malicious with the bounding the statistical approach (David.H, 2006).The Bayesian algorithms are presents in (Mehran.A, 2013), which are generally use for instance Naïve Bayesian classifier, another approach of time series is The Fuzzy logic approach which depend on variables, rules and sets. Along with a smaller part which is called fuzzy-logic that is responsible to manage the large input parameters and calculation of the input-data. The use of Data mining supports to decrease the size of input data-set and allows the topographies, which identify the attacker. The techniques in fuzzy logics are used in (J.E.Dickerson and J.A.Dickerson, 2000) and (S. Sujatha *et al*, 2008). And the third one is the neural network that is a marginal of a statistical techniques to identify the attacker in expert system. The various neural network are used in ABIDS, Machine learning Base.

B. Comparison of Anomaly Based Intrusion Detection:

In this subsection we review various types of ABIDS and compare the common techniques of ABIDS the complete comparison is summarized in table 2 along with their advantages and limitation, the most common techniques comparison are knowledge base technique, data mining technique, statistical base technique, and machine learning technique.

Table 2: Comparison of ABIDS

ABIDS	Type	Advantages	Limitation
Signature analysis	Knowledge Based	Knowledge based Community supports as well evidence to enable signatures for recently alerts.	Knowledge-based malicious detection need more up-to-date for newly malicious.
Expert systems	Knowledge Based	These systems suitable for misuse detection and abnormality detection by comparison of normal and abnormal vehicles with captured vehicle for detection the malicious	Requires frequent updates to detect newly attack
Clustering	Data Mining	Clustering algorithm is suit able for particular data types, Suitable for unsupervised mode, Testing-phase is fast.	If cluster head compromise then an attack can be launch, it increase network overhead.
Classification	Data Mining	It is multi-class approach that can employee influential algorithms to decide between belonging to other classes	Dependable on accurate labels so it is normally not feasible.
Threshold Metric	Statistical	It is stable when if no significant variation in normal behavior.	It fails when if attack rely on more than one event, it fails when if upper and lower boundaries are not significant.
Time Series	Statistical	It has ability to detect the attacks those are launched in shape of series.	This model is costly.
Bayesian	Machine Learning	Auto deal situations if data set is incomplete, learning experience about relation- ship.	High computational effort is required.
Fuzzy logic	Machine Learning	The rules enables if then to reduce malicious, fuzzy-sets easily customized.	Complex to development of model base on fuzzy system, Not flexible to enable for mixed database.
Neural network	Machine Learning	Less formal statistical training, capability for multi training algorithms, capability for detection the complex nonlinear connection among dependent and independent.	Higher computation- al effort is required, long training time, over fitting.

IV.
Proposed Ids:

Our proposed Intrusion Detection is a cloud based, present in figure 2, in cloud computing, we assumed a data base which maintain the fingerprint of every vehicle’s user, for initial process as long as it can be maintain for the future use also, our assumption is, when a vehicle joins the RSU, for initialization the vehicle must verify its finger print of authentication purpose and after fingerprint, the system switch to the intrusion detection system, where it verify the user authentication as well identify the user behavior either a normal vehicle or abnormal vehicle, and finally it switch to the decision to the RSU and RUS update the user as participate and it enable to use services of the vehicular network, as cloud server is capable to maintain a database to maintain the drivers identification and give the authorization, this method is more secure which can detect the malicious nodes with accurate satisfactory result, the fingerprint authentication is more secure than other system, due to the security task is challenging in the vehicular network, we looking forward our Intrusion detection based on cloud, and analyzing the performance of Intrusion

Detection based on cloud, as the performance of this system is accurate, which help to detect the unexpected events generate from attackers or malicious, the challenging attacks such as Sybil attack, Tempering and Eavesdropping which are use the fake identification or modification into identification, our system is more accurate which maintain the fingerprint of each vehicle drivers who ever participate into the vehicular network, this system give prevention to the all participates and avoid the fake information as well fake warning which are caused to accidents and cause to congestion as well fake identification give the confusion to the other participants to take decision or reaction on given information or warning.

Conclusion:

This paper gives brief overview of the Anomaly base Intrusion Detection system in VANET, which can be help to researchers and developers to mitigate possible attacks by developing the possible prevention measures. Our goal is to classify all the possible techniques of anomaly based intrusion detection techniques and distinguish the detection methodology and analyze the performance of common techniques which helps to improve the security features in Anomaly base Intrusion detection techniques, In general VANET is still evolving, not fully deployed yet in practical life. It is observed that in VANET, we have many vulnerable / unsecure communication channels are operating which increased the overall security risk in the VANET system and other network overheads. So researchers and developers should take a serious note on VANET to improve the security features and manage the control systems to enhance the existing security risks. On the other hand, using VANET, we can secure the financial consequence due to collisions, which is the beneficiary to insurance companies. . To sum up all, we categorized all the trees of IDS and define the possible Attacks in the VANET system which are unsecured or contain high risks. The proposed cloud based IDS is an accurate system of detection the intrusion, which contain signature database of each user for initialization of each user and detect the malicious at initial stage, all vehicle assigned their own fingerprint to authentication and identification, we are analyzing the performance of our proposed system, which help to mitigate the security attacks in VANET, and improve the security as well secure the communication of VANET by our proposed Cloud Based IDS. Our proposed system is novel approach in VANET.

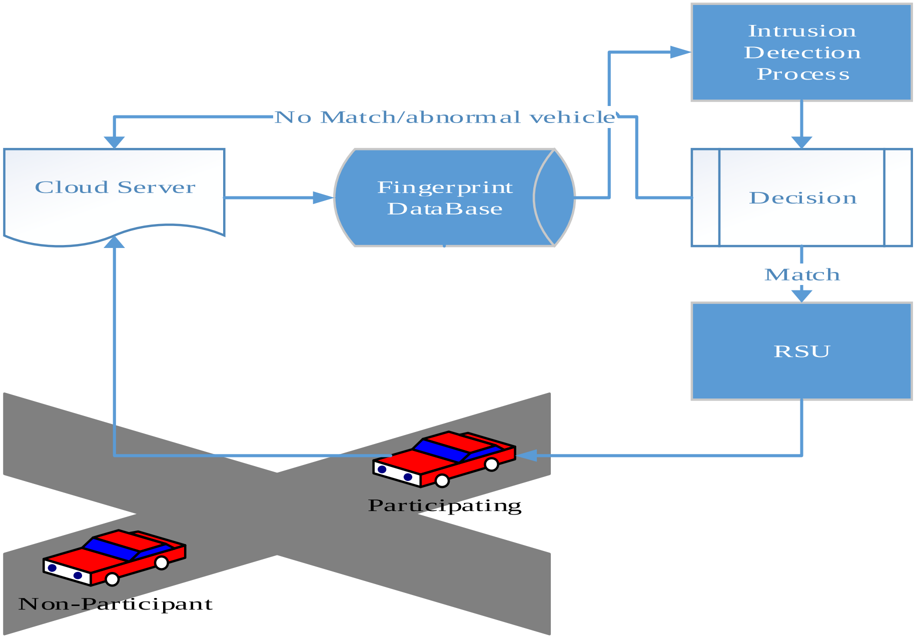

Fig. 2: Proposed IDS

REFERENCES

Alexandros, G.F., A.S. Vasilios and P. Nikolaos, 2010 "Anomaly-Based Intrusion Detection Algorithms for Wireless Networks" Springer-Verlag Berlin Heidelberg.

Aijaz, A., B. Bochow, F. Dtzer, A. Festag, M. Gerlach, R. Kroh, T. Leinmller, 2006. "Attacks on inter-vehicle comm systems, an analysis”, Ensuing of the 3rd Intr Workshop on Intelligent Transportation.

Wing, C.T., 2011. “Secure and Privacy-preserving Protocols for VANETs,” in PhD thesis at The University of Hong Kong.

Choi, J.Y., M. Jakobsson, S. Wetzel, 2005. “Balancing auditability and privacy in vehicular networks”, Ensuing of the Q2SWinet '05:

Proceedings of the 1st ACM intr workshop on Quality of service & security in wireless and mobile networks, New York, NY, USA, ACM.

Cheri, D and R. Paul, 1990. “The Computer Watch data reduction tool,” Ensuing of the 13th NCSC, Washington, DC.

David, H., 2006. “A Tutorial on Learning with Bayesian Networks,” Ensuing of the Microsoft Research, official Report MSRTR 95.

Fischer, L., Aijaz, A. Eckert, C. Vogt, 2006. “Secure revocable anonymous authenticated inter-vehicle comm (SRAAC), Ensuing of the 4th Workshop on Embedded Security in Cars (ESCAR 2006).

Heijenk, and Frank Kargl, 2013. “Graph-Based Metrics for Insider Attack Detection in VANET Multihop Data Dissemination Protocols,” IEEE Transactions on vehicular technology, 6: 4.

Vaccaro, H.S. and G.E. Liepins, 1989. “Detection of anomalous computer session activity,” Ensuing of the IEEE Symposium on Research in Security and Privacy, pp: 280-289.

Soomro, I.A., H.B. Hasbullah, J.lb.Ab Manan, 2010. “User requirements model for VANET applications”, Ensuing of the Intr Symposium on Info Tech-2010 (ITSim 2010).

Jiang, Delgrossi, 2008. “IEEE-802.11p towards an intr standard for wireless access in vehicular environments,” IEEE Vehicular Tech Conf (VTC), pp: 2036-2040.

James, C.J.H, 1996. “A Comparative Analysis of Current Intrusion Detection Technologies,” Ensuing of the 4th Tech for Info Security Conf, TISC’96, Houston, TX.

Lu, R., X. Lin, H. Zhu, P.H. Ho, X. Shen, 2008. “Ecpp: Efficient conditional privacy preservation protocol for secure vehicular communications” Ensuing of the INFOCOM 2008. The 27th Conf on Comp Comm. IEEE.

Liu, X. Fang, Z. Shi, 2007. “Securing VANET,” Ensuing of the Pervasive Computing and Applications, ICPCA. 2nd Intr Conf.

Jian, P., J. Shambhu, Upadhyaya, F. Faisal and G. Venugopal, “Data Mining for Intrusion Detection Techniques, Applications and Systems,” Data Mining Techniques for Intrusion Detection and Computer Security, University at Buffalo, New York.

Mohd, E., M. Sara, S. Fatimah and S.A. Lilly, 2010. “Intrusion Detection Using Data Mining Techniques Information Retrieval & Knowledge Mgt”, CAMP.

Mittag, J., E. Schmidt, M. Killat, J. Harri, Hartenstein, 2008. “Analysis and design of effective and low-overhead transmission power control for VANETs,” Ensuing of the ACM, San Francisco, California, USA.

Raya, M., J.P. Hubaux, 2007. “Securing VANET,” ensuing of the Journal of CompSecurity, 15.

Moustafa, H., G. Bourdon, Y. Gourhant, 2006. “Providing authentication and access control in vehicular network environment. Ensuing of the SEC-Vol201 of IFIP, Springer.

Lyamin, N., A. Jonssonand J. Loo, 2013. “Real-Time Detection of DoSAttacks in IEEE 802.11p Vehicular Networks,” IEEE Comm Letters.

Papapanagiotou, K., Marias, G.F. Georgiadis, 2007. ”A certificate validation protocol for VANETs”, Globecom Workshops, IEEE.

Papadimitratos, P., L. Buttyan, J.P. Hubaux, F. Kargl, Kung, A. Raya, 2007. “Architecture for secure and private vehicular comm. Telecom, 2007. ITST '07. 7th Intr Conf on ITS.

Plossl, K. Nowey, T. Mletzko, 2006.”Towards a security architecture for VANET. Ensuing of the ARES '06.

Innella, P. and O. McMillan, 2001. “An Intro to IDS, Symantec Connect.

Raya, M. Jungels, D. Papadimitratos, P. Aad, I. Hubaux, 2006. Certificate revocation in vehicular networks. Official Report LCA-REPORT-2006-006, EPFL.

Thomas, G and L. Teresa, 1991. “Model-based intrusion detection,” ensuing of the 14th National Comp Security Conf, pp: 372-385.

Vasilios, A.S., and P. Fotini, 2006.“Application of anomaly detection algorithms for detecting SYN flooding attacks”, Elsevier, Computer Comm, 29: 1433-1442.