Study on the Inter-Network Cross-Verification representation by Reducing the Impact of DOS Attacks in VANET

Abhishek Sharma
Computer Science & Engineering
Sirda Institute of Engineering and Technology, India

Priyanka
Computer Science & Engineering
Lovely Professional University, India

Abstract – *VANET is a Vehicular adhoc network in which vehicles are communicating to each other through the wireless connection. In VANET each and every participating vehicles are treated as the wireless node mode. We used VANET to improve the (ITS) Intelligent Traffic System. Vehicles can communicate to each other and also communicate through the road side unit that provides the network management. VANET applications can be classified on the bases of security or non security. The adhoc networks have promising future as they provide with an insight to the safe road environment process. When the mobile network is created Vehicles can communicate with each other. A variety of security attacks promising in VANET. In this paper edition we are here going to propose an algorithm for reducing the flooding of DoS attacks in network which is called as VANET. The response time increases by the RRDA algorithm which is used in maximizing the security attacks by reducing DoS attacks.*

Keywords: (Attacked packet detection algorithm)-APDA, (request response detection algorithm)-RRDA, (vehicular ad-hoc network)-VANET, (intelligent transportation system-ITS.

I. INTRODUCTION

VANET stands for Vehicular ad hoc network which uses cars as nodes so as to create a vehicular network. A VANET turns every participating car into a wireless router or a node and in turn create a network with a wide range. As the cars falls out of signal range and drop out of network others cars can join in connecting vehicles to one another. It is basically a wireless sensor network which is used to create the mobile network. Mobile network is based on mobile vehicles that are represented by wireless nodes on the network. VANET is typically provides the wireless communication between the vehicles or wireless nodes on the network [2]. Function of VANET is to provide the privacy, security and safety on the network. Now a day's VANET becomes more popular in many of the Countries [5]. It comes under the sub category of the MANET (Mobile ad hoc network) property].

Vehicular Ad-Hoc Networks (VANETs) is just self-organized and self-managing the information in a distributed manner. They can hold the vehicles, roadside units that aid within the network organization.

In the Intelligent transportation system ITS, VANET is used as an important element of that. To provide the wireless access of the vehicles, ITS used as a WAVE as well as it is designed for the standard termed as an IEEE 802.11p. In a vehicular ad hoc network every wireless nodes and vehicles are well furnished on the board radio transductor which is also known as (ORT). We can use ORT as communicating with the wireless vehicles and the other node on the network [1].

In VANET system we have varieties of application which is used in providing the availability of facility of parking, intensity of traffic and beware of the accidents. We have divided the number of real investigates that endeavors such a have different issues related to researched helps us to identified with VRC, V2V, V2I territories. The three types of communications used in vehicular ad hoc network are VR1 [11], V2V and V2I.

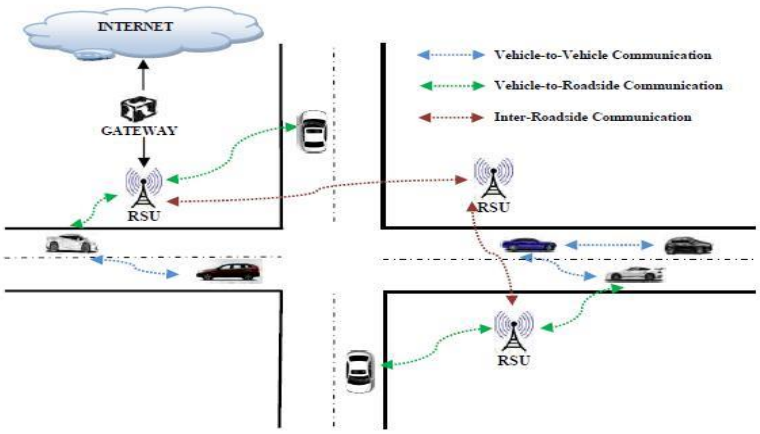

Fig 1.1: Vehicular Ad-hoc Networks (VANETs)

1.1 VANET Attacks and Threats

The size of the network and the various attacks are prone in the VANET and it's become very much hard to overcome them. The various attacks introduced in VANET are:

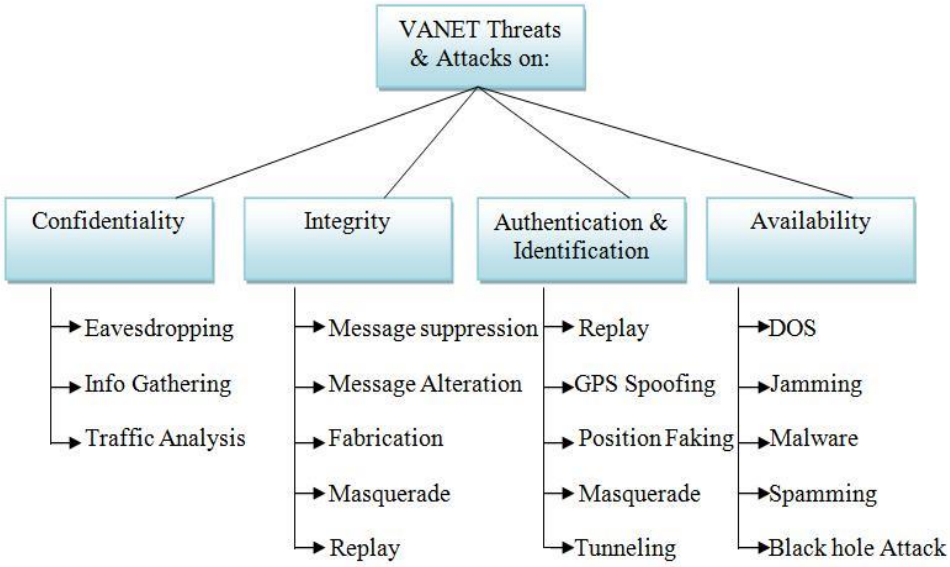

Fig 1.2: VANET attacks and threats

1. DENIAL of Service Attacks: DOS attacks can be done by the system insiders and outcasts and give the system not accessible to genuine clients by flooding the control channel with high stable of actually produced messages and stops the system association. Therefore OBU and RSU are not able to process the limit adequately. An outcast assailant can dispatch a DoS assault by over and again scattering manufactured messages with invalid marks to expend the transfer speed or different assets of a focused on vehicle. The effect of this attack is that, VANET losses its ability to provide services to the legitimate vehicles.
2. SPOOFING Attack: The attack in VANET is related to attack device and also the outside network that uses an internal network address to masquerade network and a device. [5].
3. DISTRIBUTED DENIAL OF SERVICES attack: This type of attack is a DDOS type attack which is used as a mismatched and the multiple and the networks which is uncoordinated to launching the attacks from such as sources which is simultaneous. The thing which is required here is a drone which is used for launching attacks and the software such as zombie.

1.2 Distributed Denial of Service (DDoS)

A Distributed Denial of Service (DDoS) attack is an attempt to make an online administration unavailable by overwhelming it with traffic from multiple sources. They focus on a wide mixed bag of essential assets, from banks to news websites, and present a noteworthy test to verifying individuals can publish and access critical data. DDos more often than not by incidentally interfering with or suspending the administrations of a host joined with the Internet.

DDoS attack, utilizes numerous gadgets and various Internet connection, regularly conveyed universally into what is referred to as a bonnet. A DDoS attack is, accordingly, much harder to avoid, basically in light of the fact that there is no single aggressor to shield from, as the focused on asset will be overwhelmed with solicitations from numerous hundreds and a great many various sources.

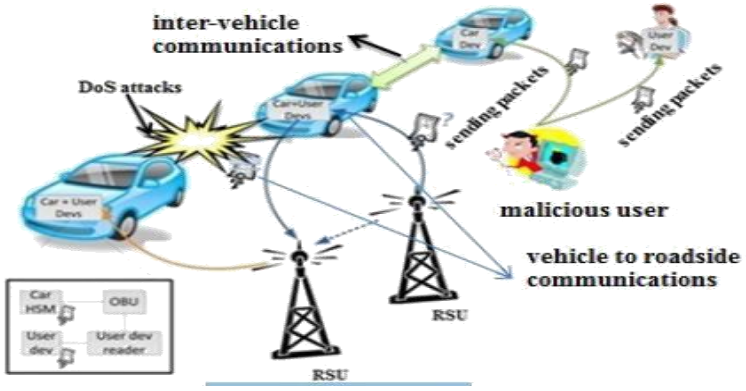

Fig. 1.3: DDoS Attack

The most well-known kind of Denial of Service attack includes flooding the objective asset with outer communication requests. This over-burden prevents the resource from reacting to honest to goodness activity, or slows its response so significantly that it is rendered effectively unavailable.

1.2.1 Types of DDOS Attacks

DDoS attacks can be divided in three types:

Volume Based Attacks: The attack's objective is to soak the transfer speed of the assaulted site, and size is measured in bits every second (Bps).like Includes UDP floods, ICMP floods, and other spoofed-packet floods.

Protocol Attacks: This type of attack based on resource. Like attacks on server or network, this type of attack normally occurs in Organization and consumes actual server resources, or those of intermediate communication equipment, such as firewalls and load balancers, and is measured in Packets per second. Expends real server assets, or those of middle of the road correspondence hardware, for example, firewalls and burden balancers, and is measured in Packets every second. It Includes SYN floods, fragmented packet attacks, Ping of Death, Smurf DDoS and more.

Application Layer Attacks: Includes Slow Loris, Zero-day DDoS attacks, DDoS attacks that target Apache, Windows or Open BSD vulnerabilities and more. Comprised of seemingly legitimate and innocent requests, the goal of these attacks is to crash the web server, and the magnitude is measured in Requests per second.

II. RELATED WORK

Lobna Nassar, M.et.al. VANET IR-CAS for safety ACN: Information Retrieval Context Aware System for VANET Automatic Crash Notification Safety Application: This paper proposes IR-CAS for VANET fully automatic crash notification safety application. It helps to increase the accuracy and efficiency with its exact or accurate notifications and also helps to increase the decentralization. Different IR models are compared using binary and partial effectiveness measures and the estimation of difficulty is done by calculating the Manhattan distance between crash and severest crash context vectors [1].

Chan-Ki Park et. Al (2013) Measuring the Performance of Packet size and Data rate for Vehicular Ad-Hoc Networks: In VANET the wireless access in vehicular environments provides the safety service and information to driver as well as to passenger. Currently most of the researchers have been proposed resolution for high speed and rapid topology change or it assumes to packet size. This assumption could not provide the various services for VANETs because of limited size of the packets. In this paper they resolve this problem by analyzing the transmission rate of different packets in VANET using NS2 simulator. The future work from this paper is to develop the channel assign algorithm using multi-channels and MAC protocol for improving the transmission efficiency [2].

Karan verma et.al. (2012) find an efficient defense method against UDP spoofed flooding traffic of denial of service (DoS) attacks in VANET. In user datagram protocol (UDP) based flooding that is a form of the Denial of Service attacks, in which the malicious node forms the large number of fake identities. Here is the method that is

used to detect and defend against the UDP flooding attack. This method makes use of the storage efficient data structure and Bloom filter method based IPCHOCKREFERENCE detection method [3].

Yeongkwum kim et. Al. (2013) explains about the security issues in VANET: in VANET security and privacy are the most important factor motivating robust vehicular network designs. Here they discuss about the various threats and attacks in the VANET and in response, provides some security solutions. In this paper they introduce some applications and possible attacks. They provide the brief survey of the security related issues and provide their solutions in vehicular network environment [4].

Usha Devi Gandhi et. Al.(2014) RRDA (Request Response Detection Algorithm) for Detecting DoS attacks in VANET. In this paper they have worked on detecting the DoS attacks in VANET. Here the attribute of the requesting vehicle is verified and this verification goes through checking no. of packets sent/sec, speed of the vehicle and the maximum capacity of the packet. In this paper they proposed a Request Response Detection Algorithm (RRDA) that helps to detect the DOS after APDA. This algorithm helps in increasing the response time and maximizing the various security attacks in VANET [5].

Gongjun Yan et al. (2008), in this paper, their main commitment are a novel way to deal with upgrading position security in VANET. To place security in VANETs and attain local security with the aid of on-board radar to discover neighboring vehicles and to confirmed their announced coordinates. Local security is extended to attain global security with the help of preset position-based groups to create a communication network by using a dynamic challenging mechanism to verify remote position information. They accomplish neighborhood and worldwide position security by utilizing the on-board radar to distinguish nearest vehicles and to affirm their declared directions. They process cosine comparability among information gathered by radar and neighbors' reports to channel the manufactured information from the honest information. In view of sifted information, we make a background marked by vehicle development. By checking the history and figuring likeness, we can keep countless assaults and a few mixes of Sybil and position-based assaults. Traded off vehicles are arbitrarily conveyed in the framework. At the point when there are less than 16 traded off vehicles, the time needed to identify them doesn't change with their rate of the activity. On the off chance that there are more than 16 traded off vehicles, the bring down the rate is, the more it takes to discover them on the grounds that they are more sparsely distributed and need more hops to be detected[6].

P. Papadimitratos et al. (2008) analyze threats and recognize security and privacy requirements, and provide a scale of mechanisms to safe vehicular communications systems and present a solution that can be rapidly adopted and deployed[7].

Ali Hamieh et al. (2009) Vehicular Ad hoc Network (VANET) is vulnerable to Denial of Service (DoS) attacks, like jamming attack. The purpose of a jammer is to hinder with legitimate wireless communications, and to mortify the overall QoS of the network. In this paper, they propose a model to detect a particular class of Jamming attack, in which the jammer transmits only when valid radio activity is signaled from its radio hardware. Vehicular ad hoc networks (VANETs) are networks in which wireless mobile nodes establish temporarily network connectivity and perform routing functions under self-organization. Due to their nature, VANET is vulnerable to DoS attacks, such as jamming attack. The goal of a jammer is to obstruct with genuine wireless communications, and to mortify the overall QoS of the network [8].

III. PROBLEM FORMULATION

Vanet is used for creating the network of mobile vehicles in a good manner. We can create an instant kind of network and while working on VANET is a new demand in the society. In previous papers, people had worked on DOS attack in a VANET adhoc network. It is very much efficient, and also we can divide into two categories of algorithms. In the first one, the attributes of the requesting mobile vehicle is verified [5].We can go for these verifications with the help of various number of packets formation sent per second, vehicle speed, and a maximum capacity of a packet storage. Network management as creation of the network is quite a time consumable. To make this process a speedier process of verification, we are proposing a cross verification of an internetwork, where the road vehicles which are present inside the network will be judging the requesting vehicle rather than requesting the Road Side Radio Transductor (RSRT) for a cross verification.

IV. PROPOSED ALGORITHM

Our proposed algorithm is based on the APDA (Attacked Packet Algorithm) followed by the previous approach. The APDA algorithm detects the DOS attack prior to the verification. It considers the position, time stamp, speed, and so forth of the vehicle to discover whether it falls under the scope of radar furthermore in recognition of false cautions. In the event that the quantity of bundles and the most extreme rate is high than the hub speed it is

thought to be an assaulted as the position of the vehicle changes rapidly correspondingly on the off chance that they are low they don't change the position much is additionally thought to be assaulted. After the complete process the vehicles are validated and stored in the RSRT database.

4.1 Request Response Detection Algorithm:

Our work is based on the Request Response Detection Algorithm. After APDA all the vehicles are confirmed and buffered in the RSRT (Road Side Radio transduction). The flooding due to DOS attack can be further compact by the RRDA algorithm. RRDA algorithm is used for the further verification of new requests that be after to join the network. This algorithm compares the previous validated information base with new requests and further reduces the fake alarms by allowing only the validated nodes. This algorithm reduces the flooding by limiting it oppose and also by not allowing the forged vehicles by attacker.

V. PRESENT WORK

Attacked packet detection algorithm (APDA) attempts to verify vehicles which are in the range of the RSU to join the network. The APDA compares the timestamps to accept or discard the packet. The APDA algorithm detects the DOS attack prior to the verification. It considers the position, time stamp, velocity, etc. of the vehicle to find whether it falls under the range of radar and also in detection of false alarms. The APDA verifies the vehicles on the basis of timestamp of the messages, however the malicious vehicle can attempt to send the message in the valid threshold timestamp limit set by RSU, in this case the malicious vehicle will be verified .In APDA, and the vehicles are verified on the basis of threshold value. However, the malicious vehicle may pass the test if it is within range of RSU so that difference in the timestamp is less than threshold value

After initial verification when a vehicle joins the network, the study considers request and response detection algorithm to verify the new requests. And the RRDA is also based on hop count comparison; the malicious vehicle may flood the network without changing its hop count value. RRDA algorithm is used for the further verification of new requests that wants to join the network. This algorithm compares the previous validated data base with new requests and further reduces the false alarms by allowing only the validated nodes. This algorithm reduces the flooding by limiting its counter and also by not allowing the forged vehicles by attacker. In RRDA, the verified vehicles are further detected if they are communicating with RSU but with different hop count. However, the hop count of the vehicles tends to change as they move. This may result in false detection of the malicious vehicle.

a. Objectives

The main objective of our work to addresses the problems.

To verify the vehicular node using attacked packet detection algorithm.

To detect the malicious vehicles using request response detection algorithm and the scheduling approach.

To compare the proposed work with RRDA.

b. Methodology

Step 1: Deploy the nodes in the network and create a vehicular Ad hoc network in the simulation area.

Step 2: The source vehicle broadcasts request message to vehicle that are already in the range of RSU.

Step 3: The normal communication interval for request messages will be recorded.

Step 4: The maximum communication interval will serve as the threshold value.
Step 5: If attacker node floods the network, the communication with it will be stopped as soon as its communication time exceeds the threshold value.

c. Algorithm

Start ()

{

for i =1:N
Each vehicle broadcast RREQ to neighbor
Ti : Time taken by ith vehicle to send the RREQ
{

if(Ti > Threshold value)
Mark Vehicle as malicious
}
End()

}
Here N: Total Number of Vehicles

Time: Set of time values recorded by the nodes during normal communication scenario

Threshold value= max {Time}

The proposed methodology was implemented in MATLAB 2013a.

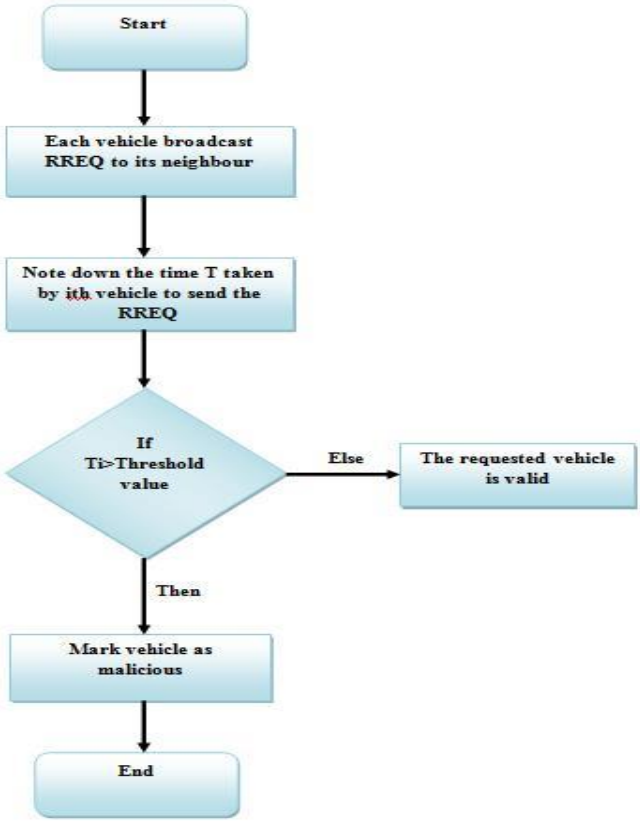

Fig. 5.1: Flowchart for research methodology

VI. PERFORMANCE ANALYSIS

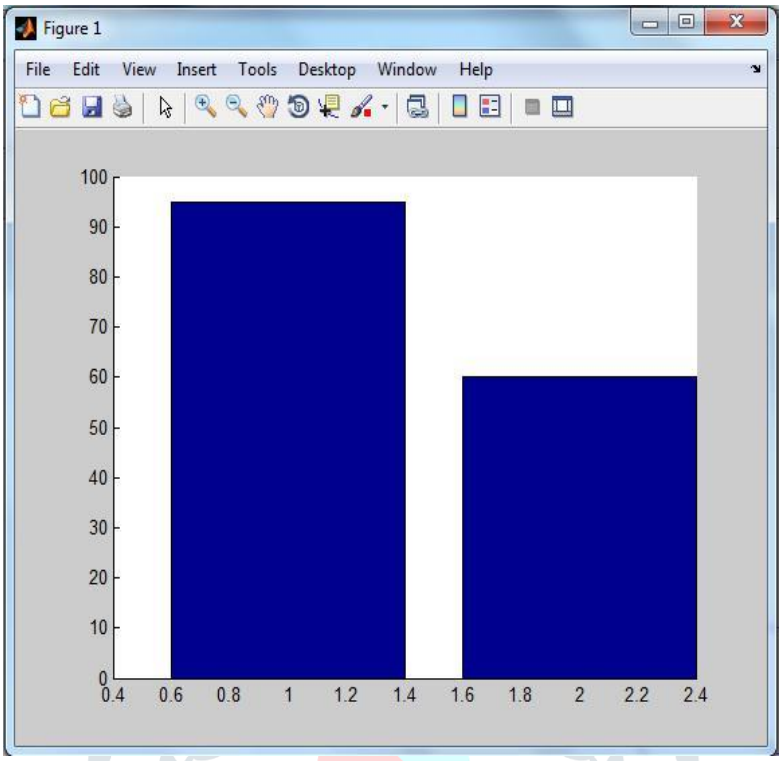

Fig 6.1: Performance analysis of the RRDA and our research work

This comparison graph shows the comparison between the base model and our research work. In this performance graph the x-axis shows the time taken for the request and response of the vehicle and the y-axis shows the no. of iteration performed. By this performance graph it is clear that the performance of our research is better than the base paper.

VII. CONCLUSION

The vehicular ad hoc network has a good vision as they are able to give an insight to the safe road environment process. If all the vehicles in the VANET are having correct information to all the demanding vehicles then many different applications such as traffic monitoring road safety can be verified into real live manner. We have studied the DDOS attacks in the curriculum and can be reduced the impact of flooding for the same manner. However, we would also like to take into account of various other attacks such as spoofing attack and make network secure from the same network.

ACKNOWLEDGEMENT

Firstly, I would like to thank my supervisor Mrs. Poonam Chaudhary for being great mentor and best advisor that I could ever have. His advice, encouragement and critics are sources of innovative ideas, inspiration and cause behind the successful completion of my thesis work. His consistent support and the intellectual guidance made me energize and give up the new idea. I am highly obliged to all faculty members of computer science and engineering department for their support and encouragement. Finally, I am also thankful to my parents who have helped me a lot in completion of my thesis work.

REFERENCES

[1] Lobna Nassar, Mohamed S. Kamel, Fakhri Karray *"VANET IR-CAS for Safety CAN: Information Retrieval Context Aware System For VANET Automatic Crash Notification Safety Application",* Springer Science, 2014.
[2] T.W.Chim, S.M.Yiu, Lucas C.K. Hui "*VANET-Based secure and Privacy-Preserving Navigation (VSPN)",* IEEE, Volume-63, No. 2, February 2014.
[3] Karan Verma, Halabi Hasbullah *"An Efficient Defense Method against UDP Spoofed Flooding Traffic of Denial of Service (DoS) Attacks in VENET"* IEEE 2012.
[4] Yeonkwun Kim, Injoo Kim, *"Security Issues in VANET",* IEEE, 2013.
[5] Karan Verma, Halabi Hasbullah, Ashok Kumar *"An Efficient Defense Method against UDP Spoofed Flooding Traffic of Denial of Service (DoS) stacks in VANET"*, IEEE, 2013.
[6] G. Yan, S. Olariu, , M. C. Weigle, *"Providing VANET security through active position detection,"*. Computer Communications, vol. 31, No. 12, 2883-2897, 2008.
[7] Gandhi.U,.(2014).*"Request Response detection algorithm for detecting DOS attack in VANET"*,Journal of Engineering Science and Technology, 2014.
[8] Park, S., Aslam, B., Turgut, D., Zou, C.C., (2009) *"Defense against sybil attack in vehicular ad hoc network based on roadside unit support"*. In: MILCOM, pp. 1–7.
[9] R. Lu, X. Lin, H. Zhu, and X. Shen, *"An Intelligent Secure and Privacy-Preserving Parking Scheme through Vehicular Communications,"* IEEE Trans. Vehicular Technology, vol. 59, no. 6, pp. 2772-2785, July 2010.
[10] Arindam Ghosh, Vishnu Vardhan Paranthaman, Glengord Mapp and Orhan Gemikonakli *"Exploring Efficient Seamless Handover in VANET Systems Using Network Dwell Time",* Springer, 2014.