iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 2 **Issue:** IX **Month of publication:** September 2014

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

Detection and Localization of Sybil Attack in VANET: A Review

K.Malathi[*1], Dr.R.Manavalan[*2]

Department of Computer Science, K.S.Rangasamy College of Arts and Science, Tiruchengode-637215, India[*1]

Department of Computer Applications, K.S.Rangasamy College of Arts and Science, Tiruchengode-637215, India[*2]

Abstract*—In Vehicular Communication, the security system against the attacker is an essential one. The significant below against the security of VANET is a Sybil attack. It is an attack in which a original identity of the vehicle is corrupted or theft by an attacker and creates multiple dummy identities for stealing the vehicle. Finding such type of attacker and the original vehicle is a challenging task in VANET. This survey paper briefly presents various Sybil attack detection mechanism in VANET.

***Keywords*—VANET, Security, Sybil attack detection, Privacy, Malicious node.**

I. INTRODUCTION

A Sybil attack consists of adversary assuming multiple identities to defeat the trust of an existing reputation system. In vehicular networks, the mobility of vehicles increases the difficulty of identifying the malicious vehicle location during a Sybil attack. Vehicular network is a specific type of Mobile Ad hoc Network (MANET) where the mobile nodes are replaced with vehicles equipped with On Board Unit (OBU) communication devices. The characteristics of VANET comparison with MANETs including rapid change in topology, no power constraint, large scale, variable network density and high predictable mobility (vehicles are driving with limited speed in a road with a certain geometric topology). In the past decade, specializing the well-known Mobile Ad hoc Networks (MANETs) to Vehicle-to-Vehicle and Vehicle-to-Roadside wireless communications have the witness of the emergence of Vehicular Ad-hoc Networks (VANETs).

VANET architecture is designed for Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communications with two communication devices called the Road Side Unit (RSU) that is placed on the road side and OBU which is installed in vehicles. In sensors communications, VANET are vulnerable to many of the security attacks. One of the harmful attacks is Sybil attack. Vehicular Ad hoc Networks (VANETs) are being increasingly advocated for traffic control, accident avoidance, and management of parking lots and public areas. Security and privacy are two major concerns in VANETs. Unfortunately, in VANETs, most

privacy-preserving schemes are vulnerable to Sybil attacks, whereby a malicious user can pretend to be multiple (other) vehicles. In Sybil attack, an attacker creates multiple identities either by forging new identities or stealing identities from neighboring vehicles. A study on Sybil attack in Vehicular Ad Hoc Networks (VANETs) is presented in section II. The rest of the paper is organized as follows: Section II provides a brief survey about the Sybil attack in VANETs. Issues in the Sybil attack are discussed in section III. The conclusion is provided in section IV with further direction.

II. SYBIL ATTACK IN VANET: A REVIEW

In 2000, M.E Zarki et al., [1] proposed Driver Ad Hoc Networking Infrastructure (DAHNI) mechanism for vehicular communication in highways. In this mechanism, cars will be location aware in short range wireless Ad hoc Networking for

inter vehicle communication. The vehicles are interacting with fixed infrastructures for uploading the data among them. The results showed that the mechanism is more suitable to avoid energy problems and increase the speed **("Security Issues In a Future Vehicular Network").**

In 2000, Markus G. Kuhn [2] introduced a non-uniform secure hash function to select a small subset of signatures that the collectors store. The size of this subset becomes a variable estimate for the logarithm of the number of signers. Only the order-of-magnitude number of valid signatures is practically variable through sampling and not the precise number. The algorithm used in this method is Trust Placed in Collectors for the purpose of the a small sample of the signers will become identical such that the correctness of the signature collection can be varied by contacting them. However, it is not necessary to provide a complete database of all signers in order to make the Claimed number of supporting signatures variable **("Probabilistic Counting of Large Digital Signature Collections").**

In 2001, Markus G. Kuhn [3] proposed a signature collections technique for improving the security in digital signature process. The method uses a small amount of memory for storing the large amount of signature. In this scheme non-uniform secure hash function is used to select a small subset of signatures from the collections of signature. Then the size of the subset is verified using probabilistic counting process. The result showed that the method achieved the verification effectively **("Secure and Deducting the Sybil Attack In VANETs").**

In 2002, Samuel Madden et al., [4] proposed a Sybil attack detection technique for urban vehicular networks. In these schemes, a number of location information reports about a vehicle are required for identification. Road Side Units (RSUs) periodically broadcasts an authorized time stamp to vehicles in its vicinity. Vehicles collect the authorized time stamps and the same used for future identity verification. Trajectories made up of consecutive time stamps and the corresponding public keys of RSUs are used for identification process. However, the location privacy was not taken into consideration since RSUs use long term identities to generate signatures. The location information of a vehicle can be inferred from the RSU signatures. In Footprint, authorized messages issued by RSUs are signer-ambiguous which means the information about the location where the authorized message was issued is concealed **("Sybil Nodes Detection Based on Received Signal Strength Variations within VANET")**

In 2002, John R. Douceur, [5] denotes that the Sybil attack, without a logically centralized authority, resource parity and coordination among entities. This method jointly establishes a large-scale distributed system. There are three main sources of information about other entities: a trusted agency, itself, or other (entrusted) entities. The absence of a reliable authority (entity), or directly to be checked only accepts signs or other signs that it has already accepted by the sign accepts to discriminate. That all entities operate under nearly identical resource constraints. All presented identities are validated simultaneously by all entities, coordinated across the system. When accepting identities that are not directly validated, the required number of vouchers exceeds the number of system wide failures **("The Sybil Attack").**

In 2002, S Park et al., [6] proposed a timestamp series approach to secure the Vehicular Ad hoc Network (VANET) against Sybil attack based on the roadside unit support. By using this approach, the Sybil attack can easily be detected the traffic messages have similar timestamps. The aggregated timestamp shows the most recent trajectory and time of each vehicle. The result showed that the proposed method prevented various traffic problems such as traffic congestion, complex roadways and so on. **("Defense against Sybil Attack in Vehicular Ad Hoc Network Based on Roadside Unit Support")**

In 2003, J.Luo and J.P.Habaux [7] proposed the Vehicular Collision Warning Communication (VCWC) protocol to support the drivers for driving process in order to avoid traffic accidents and reduced the traffic. The protocol uses communication mechanism to warn vehicles when an abnormal situation occurs, in order to stop before crashing .VCWC protocol uses two approaches: active and passive approaches. The passive approach makes vehicles to frequently broadcast their information; whereas the active approach sends the message to the vehicle if any problem

occurs. The result showed that the proposed method will reduced the traffic accident and provides maximum the road safety **("A Survey on Inter Vehicular Communication").**

In 2004, Phippe Golle et al., [8] proposed Sensor Driven Technique for detecting and correcting malicious data in VANET. It allows node to detect incorrect information and identify the incorrect source node with high probability. Sensor data that provides the redutant information which allows each individual node to process the data and detect and malicious information. The result showed that the mechanism effectively detect and remove the malicious information in VANETs **("Detecting and correcting malicious data in VANETs").**

In 2004, J. P. Hubaux et al., [9] presented a method to minimize the drivers' hassle and inconvenience. They developed a new intelligent secure privacy-preserving parking scheme through vehicular communications. This paper employed parking lot RSUs to surveil and contact between vehicles and the RSUs, will be processed through. Once vehicles, equipped with wireless communication devices, (onboard units) into the parking lot, the RSUs communicate with them and provide the drivers with real-time parking navigation service, secure intelligent antitheft protection, and friendly parking information dissemination. In addition, the drivers' privacy is not violated. Parking Lot Information Dissemination algorithm was used for conditional privacy preservation for OBUs (drivers). Simulations are conducted to demonstrate that the STD has been reduced to an available parking space and subsequently saved fuel and then save fuel and driver's time**. ("The security and privacy of smart vehicles")**

In 2004, Tamer Nadeem et al., [10] defines a framework to disseminate and gather information about the vehicles on the road. View model design and implementation of the proposed traffic and the various methods used in the system described. Privacy various privacy levels based algorithm is used for the purpose of setting rates. It allows others to obtain information about the vehicle without having to sign another level. As a result, the gap between vehicles increases, the number of vehicles that are scattered on the road showed decreases. So far in the broadcast message, this contains records of vehicles increases the visibility. **("Traffic View: Traffic Data Dissemination using Car-to-Car Communication")**

In 2005, Jinyuan Sun et al., [11] proposed ID-based cryptosystem framework to address the security problem in VANET. The method helps to achieve desired privacy by vehicles and required non repudiation by authorities. In addition to that fundamental security requirements including authentication, message integrity and confidentiality are satisfied. In this framework, certificates are not needed for authentication. It increases the communication efficiency of various VANET applications since the real-time constraint on message delivery has to guarantee. The result showed that the framework achieved good communication and provides authentication security in some extent. **("An ID-Based Framework Achieving Privacy and Non-Repudiation in Vehicular Ad Hoc Networks")**

In 2006, B. Xiao [12] introduced a method for the detection of Sybil attack using cryptography method. Using Mat lab simulator the results of this approach are reviewed. By using this method has low delay for detection Sybil attack, because most operations are done by the Certification Authority. A good security mechanism has short delay for encryption, decryption and key exchange short delay is removed. **("Detection and localization of Sybil nodes in VANETs")**.

In 2006, Fabio Picconi et al., [13] proposed a method called validating aggregated data for dating data traffic information without imposing significant communication overheads. The main idea is to use the test to capture the main idea of the possibility of network attacks possible attack by encouraging its use to catch the random checks, and it has authentication and implementation of the contract, each car has a the tamper-proof service assumes time stamping and random number generation **("Probabilistic Validation of Aggregated Data in Vehicular Ad-hoc Networks").**

In 2006, Tim leinmuller et al., [14] described about the status of the verification in vehicles. The verification methods, as well as results from the combination of different sensors and introduced a framework. Cached Greedy Geo Cast (CGGC) algorithm is used for the purpose of VANETs

addresses special needs in respect of two cases. When you send information from the wrong position at the ends of their beacon messages, they will severely affect the performance of the network. Evaluation based on simulations shows that the position verification system successfully discloses nodes disseminating false positions and thereby widely prevents attacks using position cheating. It also influences the false position data generated by malfunctioning or malicious nodes on geographic routing. **("Position verification approaches for vehicular ad hoc networks").**

In 2007, Maxim Raya et al., [15] proposed Misbehavior Detection System (MDS) protocol and Voting Evaluators (VE) protocol for the identification and local control of misbehaving or faulty nodes. The vulnerability is eliminated by identifying faulty or misbehaving nodes and distributes revocation information in VANET. The Misbehavior Detection System (MDS) protocol detects the fault nodes and activate a Local Eviction of Attackers by Voting Evaluators (LEAVE) to revoke the attacker from the network. The result showed that the proposed scheme is practical, efficient, and effective in isolating misbehaving and faulty nodes. **("Eviction of Misbehaving and Faulty Nodes in Vehicular Networks")**

In 2007, Xiaodong Lin et al., [16] proposed a secure and privacy-preserving Protocol group signature and identity (ID) of the proposed protocol not only security and privacy requirements cannot confirm it, but in the case of each vehicle in the desired detection that can deliver based signature techniques are based on protocol and the ID of the message sender is no dispute of power by the need to know. (Revocation verification algorithm needs only to guarantee security and privacy, but the message sender ID must be revealed by the vehicles in the event of any dispute, in the case where each vehicle is able to provide the desired detection.**("GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications").**

In 2007, Giorgio Calandriello et al., [17] proposed Baseline Pseudonym (BP) scheme for authentication in VANET. This mechanism reduces the security problem and provides safety for transportation strongly, even in bad network. The method enables the vehicle on-board units to generate their own pseudonyms, without affecting the system security. The result showed that the proposed method provides efficient and robust security for VANET. **("Efficient and Robust Pseudonymous Authentication in VANET").**

In 2007, Gongjun Yan et al., [18] described a method for enhancing position security in VANET. They are local and the global level of security through on-board radar to detect neighboring vehicles and to confirm their announced coordinates achieved. Filter in terms of quality, they developed a vehicle movement. Through trial and unity in the history of the system, they have a large number of Sybil attacks and some combinations of Sybil and position-based attacks can be prevented. GPS is used to detect changes in an attack exclusive short algorithm (Global System) position. **("VANET'07 Poster: Providing VANET Security through Active Position Detection"**).

In 2007, M. Raya and J. P. Hubaux [19] developed a method to detect the Sybil attack SCID secondary ID. It maintains a unique ID for each node. This resource parity and coordination among entities except under extreme and unrealistic assumption, (ie are undetected) without a logically centralized authority, Sybil attacks are always shown to be possible. SCID is an extension of AODV protocol each node maintains a unique identity. **("Securing Vehicular Ad Hoc Networks").**

In 2008, Jakob Eriksson et al., [20] introduced two new components for improving Wi-Fi data delivery to moving vehicles: Once the vehicle is moving, Wi-Fi data delivery to improve the two new elements introduced in the first, quick, Wi-Fi, less than 400 ms average connection time, reducing the end-end connectivity to establish a streamlined client process, 10 seconds from the standard wireless networking software is used. The second part, CTP, resulting in the improvement of TCP throughput over the wireless connection, wired portion of the path from losses as a transport protocol that distinguishes congestion. Cabernet deployed a fleet of 10 taxis in the Boston area. Cabernet cars, traffic updates, parking information, event and store information, e-mail and files, as well as data from the internet hosts. Connection between a sender and receiver of these applications do not require end to end interactive. Cabernet primary purpose, these adverse

conditions to obtain the highest data transfer rate of the techniques that will allow cars to move. **("Cabernet: Vehicular Content Delivery Using Wi-Fi").**

In 2008, Jesus Tellez Isaac et al., [21] proposed Kiosk Centric Model payment protocol to secure vehicle-to-road side communication in vehicular Ad hoc Network. This method is used for authentication while communication is not directed between the nodes. The payment process is enabled for both credit-card and debit-card transactions. The result showed that the scheme achieved more security for online payment. **("A Secure Vehicle-to-Roadside Communication Payment Protocol in Vehicular Ad Hoc Networks")**

In 2008, Chenxi Zhang et al. [22] introduced a RSU-aided messages authentication scheme. Road Side Units (RSUs) are responsible for verifying the authenticity of the message from vehicles to vehicles and notifying the return results by vehicles. In addition, this scheme adopts the k-anonymity approach to protect user identity privacy, where an adversary not associated to a message with a particular vehicle. The results demonstrated that the scheme yield much better performance than any of the previously reported counterparts in terms of message loss ratio and delay. **("RAISE: An Efficient RSU-aided Message Authentication Scheme in Vehicular Communication Networks").**

In 2008, RongxingLu et al., [23] proposed an Efficient Conditional Privacy Preservation (ECPP) protocol for vehicular Ad hoc Networks to address the issues of anonymous authentication for safety messages with authority traceability. The proposed protocol is characterized the generation of On-the-fly short-time anonymous keys between On Board Units (OBUs) and Road Side Units(RSUs),which can provide anonymous authentication and privacy tracking while minimizing the required storage for Short –time anonymous keys. The result showed that the trusted authority can find a way to track a targeted OBU and collect the safety messages. **("ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications")**

In 2008, Christine Laurendeau and Michel Barbeau [24] proposed a hyperbolic location estimation mechanism for VANET. The scheme employs based on a large scale path loss statistic to estimate the distance from the transmitter to a set of trusted receivers, for a selected confidence level. The distances are computed using the RSS values and the some is utilized to find a distance differences between the transmitters and each pair of receivers. Hyperbolas are then constructed between each receiver pair at the minimum and maximum bounds of the distance difference range. The intersecting hyperbolic area between multiple pairs of receivers constitutes. **("Insider Attack Attribution Using Signal Strength Based Hyperbolic Location Estimation")**

In 2009, Albert Wasef and Xuemin [25] proposed a Message Authentication Acceleration (MAAC) protocol for VANETs to replaces the time-consuming Certificate Revocation Lists (CRL) checking process by an efficient revocation check process. The revocation check process uses a keyed Hash Message Authentication Code (HMAC), to compute shared key only between non-revoked On- Board Units (OBUs). In addition, the MAAC protocol uses a probabilistic key distribution, which enables non-revoked OBUs to securely share and update a secret key. Analysis clearly proved that the MAAC protocol is to be more secure and efficient than others **("MAAC: Message Authentication Acceleration Protocol for Vehicular Ad Hoc Networks"**)

In 2009, Mohamed Salah Bouassida et al., [26] proposed a Sybil detection approach based on the received signal strength variations, according to their localizations, which allows a node to verify the authenticity of the other communication nodes. In addition, VANET that allows two nodes to determine the Sybil and malicious ones, an estimate of the degree of ability to distinguish between metric. This contribution fits the geometric analysis, simulations and validated by actual measurements. Assessment of their ability to differentiate their geographic localizations verification VANET: This approach is the interaction between the ends of two complementary technologies to verify the authenticity of a node in an allowable. **("Sybil Nodes Detection Based on Received Signal Strength Variations within VANET").**

In 2009, J.T. Isaac et al., [27] described some of the main security threats and attacks that can be exploited in VANETs and presented the corresponding security solutions that can be

implemented to those attacks. Here the HMAC algorithm is used for the security purpose. The main security areas on this Project are anonymity, key management, privacy, reputation and location. **("Security attacks and solutions for vehicular ad hoc networks").**

In 2009, Albert Wasef et al. [28] proposed an Efficient Decentralized Revocation (EDR) protocol based on a pairing-based threshold scheme and a probabilistic key distribution technique. The decentralized nature of the EDR protocol enables a group of legitimate vehicles to perform fast revocation of a nearby misbehaving vehicle. Consequently, the EDR protocol improved the safety levels in VANETs when it reduces the revocation vulnerability window in conventional certificate revocation lists (CRLs). The results showed that the EDR protocol is reliable, efficient, and scalable compare to others. **("EDR: Efficient Decentralized Revocation Protocol for Vehicular Ad Hoc Networks")**

In 2009, Soyoung Park, Baber Aslam et al., [29] described about the timestamp series approach to defend against Sybil attack in a vehicular ad hoc network (VANET) based on roadside unit support .The proposed approach targets the initial deployment stage of VANET when basic roadside unit (RSU) support infrastructure is available and a small fraction of vehicles have network communication capability. The timestamp updating protocol can be used to remove the previous RSU information from the certificate. The algorithm used in this method was timestamp series-based data propagation that is used to neither vehicular-based public-key infrastructure nor Internet accessible RSUs, which makes it an economical solution suitable for the initial stage of VANET. The result showed that the dynamic mobility of vehicles, the Sybil attack can be easily detected if traffic messages have similar timestamps, since the aggregated timestamp shows the most recent trajectory and time of each vehicle **("Defense against Sybil attack in vehicular ad hoc network based on roadside unit support"**).

In 2010, Jinyuan Sun et al., [30] proposed a privacy-preserving technique for VANETs security to preserve desired privacy by vehicles. Fundamental security requirements including authentication, non repudiation, and message integrity are analyzed in the method. To avoid the use of certificates the ID-based cryptography(IBC) algorithm uses the public key entity which is derived from its public identity information such as name, email address in PKI **("An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks").**

In 2010, Xiaohui Liang et al., [31] proposed a Privacy-Preserving chatting scheme for secure vehicular communication and preserve privacy in vehicular peer-to-peer networks. In this method, identity-based-encryption technique is used to protect the confidentiality of chatting content and also preserve user privacy. Ring signature technique also adopted for providing message authentication and guarantees unconditional source anonymity. In this method vehicles change the fake identities periodically and never permit the attackers to change the user's transactions id in different periods. The results showed that the proposed scheme can achieve data confidentiality, efficient authentication, and privacy violation elimination. **("PPC: Privacy-preserving Chatting in Vehicular Peer-to-peer Networks")**

In 2010, Yu-Chih Wei et al., [32] proposed a Received Signal Strength Indicator (RSSI) based on user Centric model, to improve the location privacy and traffic safety. The vehicles use their current position, speed, and direction periodically to fulfill the safety functions. The safety messages are broadcasted to improve driving safety by exploiting unauthorized parties or attackers and to compromise the location privacy of the interested vehicles. The result showed that the better location privacy is achieved by the method in VANETs **("RSSI-Based User Centric Anonymization for Location Privacy in Vehicular Networks").**

In 2010, Rongxing Lu et al., [33] proposed a Social-based Privacy-preserving Packet Forwarding Protocol (SPRING) for Vehicular Delay Tolerant Networks (DTN). In this scheme, the Roadside Units (RSUs) support packet forwarding to achieve highly reliable transmissions. By using this method, the RSUs are placed at the common intersection, for dependable transmission the RSUs provides more support in storing the packets temporarily in Vehicle to inter vehicle communication. When the vehicle is not available means the probability of packet drop is reduced. The result showed that

the RSUs can provide great support in temporarily storing packets to achieve high delivery ratio in VANETs. **("SPRING: A Social-based Privacy-preserving Packet Forwarding Protocol for Vehicular Delay Tolerant Networks")**

In 2010, Kewei Sha et al., [34] used the role-differentiated cooperative deceptive data-detection mechanism to detect the false data in VANETs. RD4 assessment algorithm using an extended traffic simulator is used to detect erroneous data. Three scenarios; Freeway, road construction on a highway, local street with a traffic light, as well as security-based approaches used in this manner, RD4 data focuses. Based on a comprehensive evaluation, this time in a more efficient and effective than it really is too soon to confirm the reports and traffic flows within a reasonable range of 95.70% to 99.90%, over the false accident reports are able to filter. VANET proposed technique results in most cases than the 90.00% rate of return and the precision that can be achieved showed..**(" RD4: Role-Differentiated Cooperative Deceptive Data Detection and Filtering in VANETs").**

In 2010, Jyoti Grover et al. [35] presented, a simple security scheme, for detecting Sybil attacks in VANET. In this approach, each Road Side Unit (RSU) calculates and stores different parameter values such as Received Signal Strength, distance and angle after receiving the beacon packets from nearby vehicles. The value of these parameters are combined and used to increase the detection accurate. After a significant observation period, the RSUs exchange their records and calculate the difference in the parameters values. If some nodes have same values during the observation, those nodes are identified as Sybil nodes. The results showed that the method achieved 99% accuracy and reduced approximately 0.5% error rate. **("A Novel Defense Mechanism against Sybil Attacks in VANET")**

In 2011, Jyoti Grover et al., [36] proposed a distributed and robust approach to preserve the VANETs from Sybil attack. In this scheme, the fake identities of malicious vehicles are localized by analyzing the consistent similarity in neighborhood information. Packets are exchanged periodically by all the vehicles to announce their presence and get aware of neighboring nodes. Each node periodically stores a record of its neighboring nodes. In this approach, each node exchange groups of its neighboring nodes periodically and perform the intersection of these groups. Some of the nodes have similar neighbors for certain duration of time, these similar neighbors are identified as Sybil nodes. Proposed approach locates Sybil nodes quickly without the requirement of secret information and special hardware support. The results showed that detection rate of the method are increased when optimal numbers of Sybil nodes are forged by the attacker. **("A Sybil Attack Detection Approach using Neighboring Vehicles in VANET")**

In 2011, Sushmita Ruj et al., [37] introduced the concept of data-centric Misbehavior Detection Schemes (MDS) to detect false alert messages and misbehaving nodes by observing their actions after sending out the alert messages. In the data-centric MDS, each node decide whether received information is correct or false. Based on the consistency of recent by arrived alert messages vehicle positions are estimated. So, voting or majority decisions are not needed for making MDS resilient to identify Sybil attacks. Once misbehavior is detected, it does not revoke all the secret ID of misbehaving nodes. Instead of imposing fines on misbehaving nodes (administered by the certification authority) discourage them to act selfishly. The results showed that the scheme reduced the computation and communication costs involved in revoking all the secret ID of misbehaving nodes**. ("On Data-centric Misbehavior Detection in VANETs")**

In 2011, Mina Rahbari and Mohammad Ali Jabreil Jamali [38] proposed a Sybil attack detection method using cryptographic system. Sybil attack is a cryptographic technique that they used this method of detection. Finally, using a Mat lab simulator the results of this study are reviewed. The most operations are certified, detection Sybil attack is low delay, so that effective detection method named Sybil attack.**("Efficient detection of Sybil attack based on cryptography in VANET").**

In 2011, Tong Zhou et al., [39] proposed a lightweight and scalable protocol called Privacy Preserving Detection of Abuses of Pseudonyms protocol to detect Sybil attacks in VANET. Using this protocol, the multiple vehicles which are affected by malicious user can be detected in a distributed

manner through passive listener using set of fixed nodes called road-side boxes (RSBs). The detection of Sybil attacks in this manner does not require any vehicle in the network to explore its identity; hence privacy is preserved at all times. Simulation result showed that the scheme has the ability to detect Sybil attacks at low overhead and delay, while preserving privacy of vehicles. **("P2DAP – Sybil Attacks Detection in Vehicular Ad Hoc Networks")**.

In 2012, Yipin Sun et al., [40] proposed a Efficient one-way Hash-chain based Certificate Management scheme (NEHCM) for vehicular communications. In NEHCM, a large set of certificates whose serial numbers satisfy some hash-chain based serial relationship that can be revoked by only for releasing two hash seeds. However, it is infeasible to reveal the link ability among these certificates without knowledge on the correct seeds. In this way, vehicles can get enough pseudonyms for privacy preservation while the size of the Certificate Revocation List (CRL) is just linear in the number of revoked vehicles. Furthermore, the Roadside Units (RSUs) are reduced the level of privacy preservation. The greedy vehicles did not get benefit even though the RSU services are requested repeatedly. Extensive experiment results demonstrated that the proposed scheme outperformed well in terms of revocation cost. **("NEHCM: A Novel and Efficient Hash-chain based Certificate Management Scheme for Vehicular Communications")**

In 2012, Ramakrishna M [41] described about the Distance jobs Routing (DBR) protocol described. This protocol is used to create real-time traffic information via a link to the vehicles. Connection diagram depicts the distance between neighboring vehicles. Location-based routing algorithm significantly when compared to flood-based routing protocol, which reduces the probability of packet and reduces network traffic. The proposed protocol error GP Even if the information is being obtained by using the S-velocity digital map data loads neighbors. As a result, the vehicle's speed and direction change, thus reducing network overhead, without a hello message periodically broadcast protocol that avoids the reducing the network overhead**.(" DBR: Distance Based Routing Protocol for VANETs")**.

In 2013, V. Geetha Devi et al.,[42] a Threshold ElGamal system based key management scheme for safeguarding VANET from the compromised RSUs and their collusion by the malicious vehicles. The packet loss tolerance is used to analyze the performance of the model. This method provide security with low overhead in emergency Braking notification and does not increase overhead for Decentralized floating car Data driving security promotion. The result showed that the scheme effectively compromise and reduce the collusion in VANET. **("A Route map for Detecting Sybil Attacks in Urban Vehicular Networks")**

In 2013, Navneet and Rakesh Gill [43] developed a method to detect the Sybil attack a new filed is introduced in the AODV named SCID i.e. Secondary id. It maintains a unique identity of each node. The packet format of AODV consists of all the secondary identity. This system can attack both internally and externally in which external attacks can be restricted by authentication but not internal attacks. As there is one to one mapping between identity and entity in WSN network, this Sybil attack violates it by creating multiple identities. **("Sybil Attack Detection and Prevention Using AODV in VANETs").**

In 2013, Huibin Xu et al., [44] introduced an approach to evaluating the honesty of safety message reported by neighbor vehicles by detecting the consistency between the actions and safety message in a VANET. The results showed that this proposed method can detect effectively the incorrect safety message. The detection ration is about 90% when the number of malicious vehicles is small. The approach relies on using data from safety message and beacon message, collected by vehicles in the VANET, shared with immediate neighbors and propagated to a neighboring region. The data provides speed and location information, allowing each neighbor vehicle to process the data and detect malicious information and discard it. Vehicle checks the validity of the data from message. The location information is verified by the RSSI, the speed information is verified by the relationship between location and speed. Moreover, the consistence between the action and words is evaluated. If inconsistencies arise, the vehicle is considered as malicious vehicle and the message is discarded. Simulation results showed that the proposed scheme is

effective and efficient to detect the incorrect safety message. **("Detecting the Incorrect Safety Message in VANETS").**

In 2013,ByungKawn Lee et al.,[45] Proposed a Detection Technique Against a Sybil Attack (DTSA) protocol using Session Key based Certificate(SKC) to validate inter-vehicle IDs in VANETs. In DTSA, the SKC (Session Key based Certificate) used to verify the IDs among vehicles, and also generates a vehicle's anonymous ID, a session Key, the expiration date and a local server's certificate for the detection of a Sybil Attack and the verification time for ID**. ("A DTSA(Detection Technique Against A Sybil Attack) Protocol Using SKC(Session Key Based Certificate) On VANET")**

In 2014, Vignesh.C et al., [46] proposed a lightweight Sybil attack detection scheme for detecting the Sybil Attack and DoS (Denial of Service) Attack in Mobile Ad hoc Networks. In this scheme an intermediate node receives abnormal routing information from its neighbor node called as a malicious node. The information about the malicious node is appended in the route reply packet and every node receiving the same for upgrading its routing table to mark the node as malicious node. Thus, a node receiving fabricated routing information finds the malicious node either by identifying false routing information or by verifying its routing table; the node then tells other nodes donot consider the routing information received from the malicious node. The result showed that the proposed scheme accurately detect the Sybil Attack and DoS Attack in Mobile Ad hoc Networks. **("Efficient Detection of Sybil Attack and DOS Attack in Mobile Ad-hoc Networks")**

In 2014, D. Balamahalakshmi and Mr. K.N. Vimal Shankar [47] proposed a compromised RSU detection mechanism for Sybil attack detection. A footprint concept is used in proposed method to detect the Sybil attack by using the trajectory information which is generated by multiple RSUs and the location of the vehicle is preserved. The RSU will generate the location and timing information to vehicle while it passes through RSU. Using this message, the verification is carried and the number of adjacent RSUs are eliminated to reduce message size. The result showed that the length of the trajectory information is reduced without loss of information and the bandwidth overhead is also reduced. **("Sybil Attack Detection with Reduced Bandwidth Overhead in Urban Vehicular Networks")**

In 2014, Muhammad Al-Mutaz et al., [48] described a novel protocol for Sybil detection in vehicular networks, which are cyber-physical systems, The protocol showed similar performance for Normal Dispersion Efficiency Attack model, while the Minimum Efficiency Attack model may remain undetected at high Sybil percentages. Cryptographic primitives for Sybil detection algorithm is used for the purpose of effective, practical, efficient, and simple. Additionally, they have presented some advanced attack methods where the attacker knows the detection scheme and has a priori road information **("Detecting Sybil attacks in vehicular networks")**

In 2014, Shalini.A et al., [49] used directional antennas to identify the position from which a message arrives. A lightweight and scalable protocol is presented to detect Sybil attacks. In this protocol, a malicious user pretending to be multiple (other) vehicles can be detected in a distributed manner through passive overhearing by set of fixed nodes called road-side boxes (RSBs). The detection of Sybil attacks in this manner does not require any vehicle in the network to disclose its identity; hence privacy is preserved at all times. Simulation results are presented for a realistic test case to highlight the overhead for a centralized authority such as the DMV, the false alarm rate, and the detection latency. The authors discussed these challenges, and address them systematically through a light-weight, scalable protocol called "Privacy Preserving Detection of Abuses of pseudonyms"(P2DAP). **("Taming enactment using neighbor discover distance against masquerading attack in manet").**

In 2014, Shivani Kanwar et al., [50] proposed a trust evaluation based security mechanism to detect Sybil attack in VANET. For developing a trust model, permits are assigned to nodes, updating private keys, managing the trust value of each node, and making appropriate decisions about the access rights of nodes. It provides effective decision or data protection for secure routing and other network activities in VANET. The result showed that the mechanism effectively

detect the Sybil attack. **("Detection of Sybil Attack in VANETs by Trust Establishment in Clusters")**

III. ISSUSES IN SYBIL ATTACK

From this literature survey, the following issues are identified in Vehicular Ad-hoc Network with respect to Sybil attack.

- It constraints more bandwidth overhead.
- It takes revocation cost.
- It takes time delay and message loss ratio.
- More traffic congestion and complex roadways.
- Latency, Scalability and Integrity problem.

IV. CONCLUSIONS

Sybil attack is one of the major issues in Vehicular Ah Hoc Network (VANET). Sybil attack detection and localization is a challenging task in Vehicular Ah Hoc Network. Various algorithms are proposed to identify the Sybil attack and eliminate the same. There is no unique method for identifying and removing the Sybil attack in the VANET. Each method has its own advantages and disadvantages. The number of issues such as detecting the presence of Sybil attacks, localizing multiple adversaries and eliminating them are not solved effectively. Further, this paper will help the researcher to propose novel method in order to identify the Sybil attack as well as remove the same.

REFERENCES

[1] M.E Zarki "Security Issues In a Future Vehicular Network", In Proceedings of USENIX Security Symposium, 2000.

[2] Markus G. Kuhn, "Probabilistic Counting of Large Digital Signature Collections", IEEE Computer 33 (8), IEEE, 2000, pp. 61-68.

[3] Markus G. Kuhn, "Secure and Deducting the Sybil Attack In VANETs," 1st Int'l. Wksp. Peer-to-Peer Systems,2000.

[4] Samuel Madden, "Sybil Nodes Detection Based on Received Signal Strength Variations within VANET ", In Proceedings of the Fith Annual Symposium on Operating Systems Design and Implementation (OSDI), 2002.

[5] John R. Douceur, "The Sybil Attack", In Workshop on Security and Assurance in Ad hoc Networks, 2002.

[6] S Park , "Defense against Sybil Attack in Vehicular Ad Hoc Network Based on Roadside Unit Support", 2002

[7] J.Luo and J.P.Habaux, "A Survey on Inter Vehicular Communication" in International Workshop on vehicular Inter-networking (VANET)-2003

[8] Philippe Golle, Dan Greene, Jessica Staddon, Golle, D. Greene, and J. Staddon, "Detecting and correcting malicious data in vanets," in ACM International Workshop on Vehicular Inter-Networking (VANET), October 2004.

[9] ean-pierre hubaux, Srdjan capkun, and Jun luoe "The security and privacy of smartvehicles," IEEE Security Privacy, vol. 2, no. 3, pp. 49–55, May 2004

[10] T. Nadeem, S. Dashtinezhad, C. Liao, and L. Iftode, "Trafficview: Traffic data dissemination using car-to-carcommunication. InIEEE International Conference onMobile Data Management (MDM), 2004.

[11] inyuan Sun, "An ID-Based Framework Achieving Privacy and Non-Repudiation in Vehicular Ad Hoc Networks" in workshop on Hot Topics in Networks(HotNets-IV),2005

[12] B Xiao,B Yu and C Gao, "Detection and localization of Sybil nodes in VANETs", DIWANS '06 Proceedings of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks,2006.

[13] Fabio Picconi, Nishkam Ravi, Marco Gruteser, Liviu, "Probabilistic Validation of Aggregated Data in Vehicular Ad-hoc Networks", VANET'06, 2006.

[14] Tim Leinmüller, Daimlerchrysler, "Position verification approaches for vehicular ad hoc networks", IEEE Wireless Communications, pp.16–21, 2006.

[15] Maxim Raya, "Eviction of Misbehaving and Faulty Nodes in Vehicular networks", IEEE 1-4244-1455-5/07/$25.00 c, 20007

[16] Xiaodong Lin, Xiaoting Sun, Pin-Han Ho and Xuemin Shen , "GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications", IEEE Transactions On Vehicular Technology, Vol. 56, No. 6, November 2007.

[17] Giorgio Calandriello, Panos Papadimitratos, Jean-Pierre Hubaux, Antonio Lioy, "Efficient and robust pseudonymous authentication in vanet," in Proc. 4th

ACM international workshop on Vehicular ad hoc networks (VANET '07),Quebec, Canada, 2007, pp. 19–28.

[18] Gongjun Yan, Gyanesh Choudhary, Michele C. Weigle, Stephan Olariu, "VANET'07 Poster: Providing VANET Security Through Active Position Detection", September 10, 2007, Montréal, Québec, Canada.ACM 978-1-59593-739-1/07/0009.

[19] Maxim Raya and Jean-Pierre Hubaux, "Securing Vehicular Ad Hoc Networks. Journal of Computer Security,Special Issue on Security of Ad Hoc and Sensor Networks, 15(1):39–68, 2007.

[20] Jakob Eriksson, Hari Balakrishnan, Samuel Madden, "Cabernet: Vehicular Content Delivery Using WiFi" Mobicom '08, September 14–19, 2008, San Francisco, California, USA.Copyright 2008 ACM 978-1-60558-096-8/08/09 . . . $5.00.

[21] Jesus Tellez Isaac, "A Secure Vehicle-to-Roadside Communication Payment Protocol in Vehicular Ad Hoc Networks", IEEE communication networks,2008

[22] Chenxi Zhang, Rongxing Lu, Haojin Zhu, Pin-Han Ho,and Xuemin (Sherman) Shen, "RAISE: An Efficient RSU-aided Message Authentication Scheme in Vehicular Communication Networks, IEEE Communications Magazine0163-6804/08/$25.00 © 2008

[23] Rongxing Lu, "ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications", 1(4):337-349, 2008.

[24] Christine Laurendeau and Michel Barbeau, "Insider Attack Attribution Using Signal Strength Based Hyperbolic Location Estimation" Security and Communication Networks 2008, 1(4): 337-349.

[25] Albert Wasef and Xuemin , "MAAC: Message Authentication Acceleration Protocol for Vehicular Ad Hoc Networks" IET communication,pp.894-903, 2009.

[26] Mohamed Salah Bouassida, Gilles Guette, Mohamed Shawky, and Bertrand Ducourthial ," Sybil Nodes Detection Based on Received Signal Strength Variations within VANET", International Journal of Network Security, Vol.9, No.1, PP.22 33, July 2009.

[27] J.T. Isaac, S. Zeadally, J.S. Camara,"Security attacks and solution for vehicular ad hoc networks" ,IET communication, pp.894-903,2009

[28] Albert Wasef, "EDR: Efficient Decentralized Revocation Protocol for Vehicular Ad Hoc Networks", Embedded Security In Cars Conference(Escar),2009.

[29] Soyoung Park, Baber Aslam, "Defense against sybil attack in vehicular ad hoc network based on roadside unit support", Embedded Security In Cars Conference(ESCAR), 2009.

[30] Jinyuan Sun, "An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks", IEEE Transcations On Vehicular Technology, Vol.X,No.X,Xx 2010.

[31] Xiaohui Liang, "PPC: Privacy-preserving Chatting in Vehicular Peer-to-peer Networks", IEEE Transcations On Vehicular Technology, Vol.59, No. 6,2010.

[32] Yu-Chih Wei, "RSSI-Based User Centric Anonymization for Location Privacy in Vehicular Networks", in proc.IEEE ICC,2010.

[33] Rongxing Lu and Ajinkya Uday Joshi, " SPRING: A Social-based Privacy-preserving Packet Forwarding Protocol for Vehicular Delay Tolerant Networks", SIGCOMM,2010.

[34] Kewei Sha, "RD4: Role-Differentiated Cooperative Deceptive Data Detection and Filtering in VANETs", International Journal of Network Security & its Applications(IJNSA), Vol 3, no.6, 2010.

[35] JYOTI GROVER , Vijay Laxmi , Manoj Singh Gaur, "A Novel Defense Mechanism against Sybil Attacks in VANET", SIN, page 249-255. ACM, 2010.

[36] jyoti Grover, "A Sybil Attack Detection Approach using Neighboring Vehicles in VANET", Published by ACM Article. Bibliometrics Data Bibliometrics,2011.

[37] Sushmita Ruj, Marcos Antonio Cavenaghi, Zhen Huang, Amiya Nayak, "On Data-centric Misbehavior Detection in VANETs", International journal of Network Security& its applications, 2011.

[38] Mina Rahbari1 and Mohammad Ali Jabreil Jamali, "Efficient Detection Of Sybil Attack Based On Cryptography In Vanet", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011.

[39] Tong Zhou, Romit Roy Choudhury, Peng Ning, and Krishnendu Chakrabarty, "P2DAP – Sybil Attacks Detection in Vehicular Ad Hoc Networks", IEEE Journal

On Selected Areas In Communications, Vol. 29, No. 3, March 2011.

[40] Yipin Sun, Rongxing Lu, Xiaodong Lin, "NEHCM: A Novel and Efficient Hash-chain based Certificate Management Scheme for Vehicular Communications", Journal on COMMUNICATIONS, 2011.

[41] Ramakrishna M, "DBR: Distance Based Routing Protocol for VANETs", International Journal of Information and Electronics Engineering, Vol. 2, No. 2, March 2012

[42] V. Geetha Devi, P.Shakeel Ahmed, P.Babu, " A Route map for Detecting Sybil Attacks in Urban Vehicular Networks", International Journal of Modern Engineering Research (IJMER Vol.3, Issue.2, pp-1157-1160 ISSN: 2249-6645,2013.

[43] Navneet, Rakesh Gill, "Sybil Attack Detection and Prevention Using AODV in VANET", IJCSMS International Journal of Computer Science & Management Studies, Vol. 13, Issue, ISSN (Online): 2231 –5268, 2013

[44] Huibin Xu, Limin Hua, Yumei Ning and Xiaoping Xue, " Detecting the Incorrect Safety Message in VANETS", Research Journal of Applied Sciences, Engineering and Technology 5(17): 4406-4410, ISSN: 2040-7459; e-ISSN: 2040-7467, 2013.

[45] ByungKawn Lee, "A DTSA(Detection Technique Against A Sybil Attack) Protocol Using SKC(Session Key Based Certificate) On VANET", Electrical & Electronics Engg., Volume 3 , Issue 1; Spl. Issue of IC3T @ISSN: 2248-9584,2013.

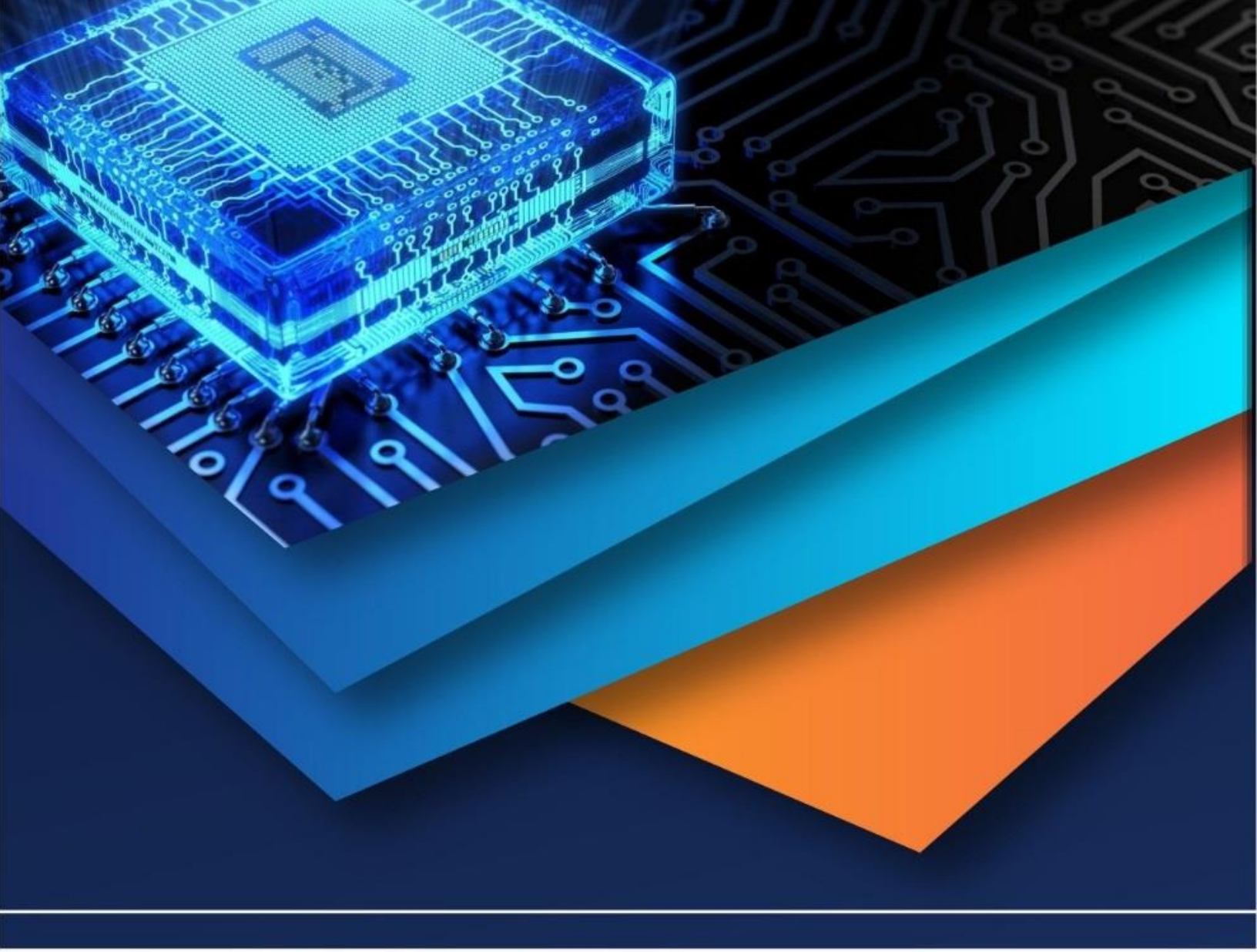
[46] Vignesh.C, "Efficient Detection of Sybil Attack and DOS Attack in Mobile Ad-hoc Networks", International Journal of Computer Engineering & Science. ISSN: 22316590 ,2014.

[47] D. Balamahalakshmi and Mr. K.N. Vimal Shankar, "Sybil Attack Detection with Reduced Bandwidth Overhead in Urban Vehicular Networks", International Journal of Engineering Trends and Technology (IJETT) – Volume 12, 2014

[48] Muhammad Al-Mutaz, Levi Malott and Sriram Chellappan, "Detecting Sybil attacks in vehicular networks", Journal of TrustManagement 2014.

[49] shalini.A, Arulkumaran.G, Srisathya.K.B, "Taming Enactment Using Neighbor Discover Distance Against Masquerading Attack in MANET", International Journal of Computer Engineering & Science, ISSN: 22316590, 2014.

[50] Shivani Kanwar, "Detection of Sybil Attack in VANETs by Trust Establishment in Clusters", IEEE communications letters, VOL. 18, NO. 1, 2014.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY