Journal of Theoretical and Applied Information Technology
31st October 2019. Vol.97. No 20

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

REVIEW ON AVOIDING SYBIL ATTACK IN VANET WHILE OPERATING IN AN URBAN ENVIRONMENT

NITHA C VELAYUDHAN[1], A.ANITHA[2], MUKESH MADANAN[3], VINCE PAUL[4]

[1]Research Scholar, Noorul Islam Center for Higher Education, Department of Computer Science and Engineering, Tamil Nadu, India

[2]Associate Professor, Noorul Islam Center for Higher Education, Department of Computer Science and Engineering , Tamil Nadu, India

[3]Lecturer, Dhofar University, Department of Computer Science, Salalah, Oman

[4]Professor, Universal Engineering College, Department of Computer Science and Engineering, Kerala, India

Email ID: [1]nithacvelayudhan@gmail..com, [2]anidathi@yahoo com , [3] mukesh@du.edu.om, [4]vinceakkara@gmail.com

ABSTRACT

VANET security became a significant and active area within the research community. Despite the different attacks on certain nodes of the VANET which have been revealed, numerous attacks for instance Jamming, Sybil, and also passive eavesdropping can debase the VANET performance. Consequently, it is vital to have some precautionary mechanism in opposition to these attacks. In Sybil Attack (SA), the attacker produces multiple identities that might belong to other vehicles or dummy identities and send messages to legal nodes. These sham identities are generated by the assailant to get the trust of the legal node. In VANETs (Vehicular Ad Hoc Networks), the vehicular needs smart road maintenance, smart signaling, along with other services. The new security problem arises because of the actuality that there is chance for the semi-trusted Road Side Units (RSUs) to be compromised. This Review Paper highlighted the latest studies regarding the avoidance of the SA in VANET like detecting SA on urban Vehicular Networks (VN), attacks in VANET, security challenges on VANET and robust technique for SA detection. Also, details of SA and VANETs are examined. The mechanisms are assessed centered on the positive rate, non-trustworthy rate, and false negative rate.

Key words: *Vehicular Ad-Hoc Network, Instance Jamming, Sybil Attack, Passive Eavesdropping, Road Side Units.*

1. INTRODUCTION

Over the last 2 decennia, VN was rising as a foundation of the next-age Intelligent Transportation systems (ITSs), contributing to secure as well as more proficient roads by offering well-timed information to the drivers in addition to the authorities (involved). In VN, vehicles that are moving are authorized to communicate among one another by means of the inter-vehicle communications along with RSUs. The urban VN in which the privacy, particularly the location confidentiality of vehicles ought to be assured [1], [2], vehicles are required to be confirmed in an unspecified way. An extensive spectrum of application in such a network counts on collaboration and also information aggregation amongst partaking vehicles [3]. Devoid of the participant's identities, such applications are susceptible to the SA, in which a malicious vehicle masquerades as manifold identities, overpoweringly influencing the outcome. The effect of SA occurring in VN can well be imperative. For example, in safety-associated applications like hazard warning, collision evasion, in addition to passing aid, biased outcomes caused by a SA can bring about rigorous car accidents. Consequently, it is of huge significance to detect SA as of the very commencement of their occurrences [4].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The detection of SA in urban VN stands as a challenging task, i) the vehicle is not identified ii), location confidentiality of vehicle is of massive distress. Locality in series of the vehicle can incredibly be off the record, iii) conversation flanked via transport is terribly small. Payable to towering mobility of the vehicle, a moving vehicle can encompass merely some seconds to communicate with an extra sporadically encounter vehicle [5].

1.1 VANET in Urban Environment

The VANET is called as a network on wheels that is employed to offer communication betwixt vehicular nodes. It is essentially an off-shoot of mobile ad-hoc networks. In VANETs, nodes (vehicular) are self-organized; in addition, communicate amongst one another in an infra-structure less setting [6]. Even though VANET is not a fresh matter, it persists to give new research demands along with issues. The chief goal of VANET is to assist a compilation of vehicles to set up and uphold a communication network amongst them devoid of utilizing any central base station or controller. The VANET's chief applications are in the serious medical emergency conditions in which there are no infra-structure where it is serious to convey the information intended for protecting lives [7].

Table 1: General Overview of Vehicular Ad-Hoc Network

VANET CHARACTERISTICS	• High Mobility • Does not require power constraints • Rapidly Changing Network Topology • Unbounded Network size • Time-critical • Frequent Changing Information • Wireless Communication • Variable Network Density • High Computability ability
COMPONENTS OF VANET	• Vehicle • Infrastructure • Communication Channel
COMMUNICATION IN VANET	• Vehicle to Vehicle communication • Vehicle to Infrastructure Communication • Cluster to Cluster Communication
SECURITY REQUIREMENTS OF VANET	• Authentication • Access control • Message confidentiality • Message integrity • Message Non repudiation • Privacy • Real time guarantees
CHALLENGES IN VANET	• Technical issues • Security issues • Security need Issues • Attacks On VANET • Attackers on VANET

In VANET, vehicles interacts using wireless links which are fixed on every vehicular node. Every node inside the VANET functions as the member and also as the network's router since the nodes interact via the intermediary nodes which lie inside their own transmission gamut. There is basically no fixed design of VANETs on account of their self-organizing tendency. The structural design of VANETs can well be categorized into 3 sorts: (i) Pure cellular wire-less local area network; (ii) Pure ad-hoc networks; (iii) Hybrid networks [6]. The structural design of the VANET is exhibited in figure.1

Journal of Theoretical and Applied Information Technology
31st October 2019. Vol.97. No 20

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

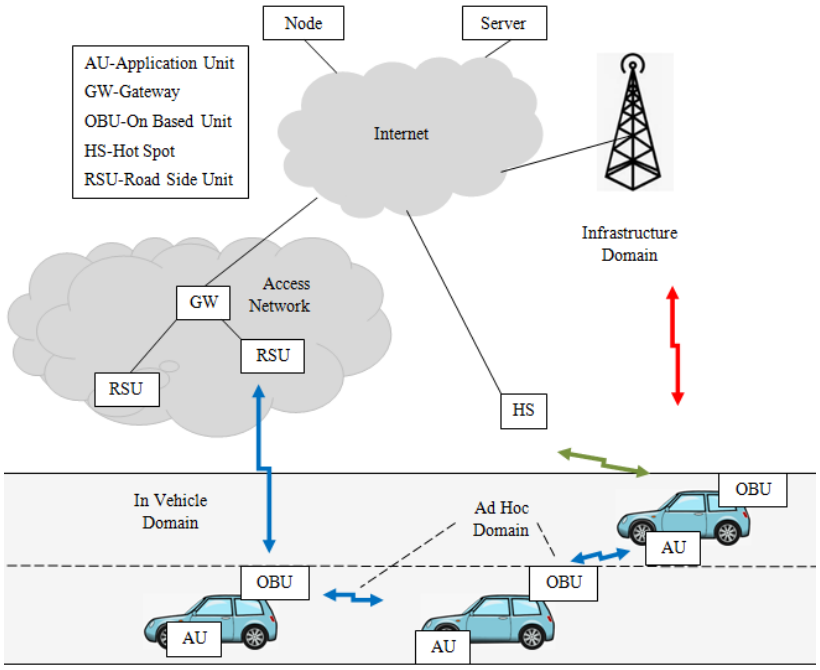

Figure 1: VANET Architecture

1.2 Detail About Sybil Attacks in VANET

SA is a substance of critical significance and also concern in network safety paving the way for numerous false identities which can cause tumult on the network [8]. SA occurs mostly in the course of broadcasting, and also it functions without individual confirmation or identity comparison of communication entities. The attacker node is capable of obtaining numerous identities. That entity can endeavor to manipulate the Sybil attacker because of the awareness about the others in every entity by means of messages in the communication channel [9]. This attack is an extremely serious one wherein a vehicle can be claimed at different places with several fake identities simultaneously and generating huge security risks. A SA is harmful to network topologies, connections together with network band-width expenditure. In Figure.2, an attacker 'A' transfers manifold messages with disparate identities to all other vehicles. Therefore, other vehicles identify the presence of huge traffic. Detecting such sort of attacker along with the actual vehicle is an aggravating task on VANET [10].

Figure 2: SA

A SA is the one wherein a malicious node (MN) on a network illegally alleged to be numerous disparate nodes simultaneously. It lets malevolent sender to generate numerous false identities (termed Sybil nodes) to function as normal nodes. It stands as an attack in which a reputable system is debased by faking identities on peer-to-peer networks.

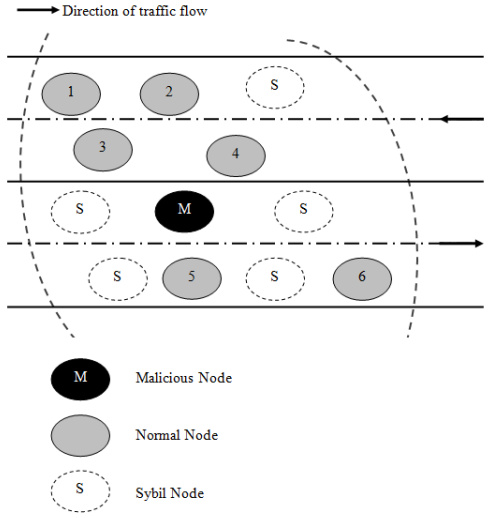

Figure 3: An example VANET under SA

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

It is a dangerously advanced world out there. Security along with antivirus programming is necessary for any system. Limited security can be separated in a SA. False information accounted via a solo malicious vehicle mightn't be adequately cogent. Applications might need numerous vehicles to consolidate specific information, prior to acknowledging it as truth. Nevertheless, a grave issue emerges when a malicious vehicle is capable of pretending as manifold vehicles termed a SA, and duly consolidates false data. On the off-chance that the benign entities are not capable of recognizing a SA, then it will consider the false information and built their decisions based on it [11].

Table 2: Various Type of SA and Detection Methods

TYPES OF SA	• Direct and indirect Communication • Simultaneous as well as Non-simultaneous Attack • Fabricated and stolen identities
SA ON PROTOCOLS	• Distributed storage • Routing • Data Aggregation • Voting • Misbehavior detection • Fair Resource Allocation
EXISTING DETECTION METHODS	• Radio Resource Testing • Registration • Post Verification • Based on RSSI

2. RELATED WORK

2.1 Attacks in VANET

Kamlesh et.al [12] examined the Black Hole (BH) node's effect in the AODV routing protocol on VANET. To learn the BH attack's effect on AODV, the performance metrical: NRL, Throughput, PDR, and also average path length were used. The experimental outcomes showed that the working of the AODV was ruined greatly owing to the effect of BH attack on VANET surroundings. The suggested SVODR protocol showed enhanced outcome in contrast to IDS on VANET. The suggested protocol provided secure vehicular communication. The method is not suited with other domains like cluster centered routing and geographic based routing because it needs highly secure environment.

Table 3: Types of Attacks in VANET

ATTACKS IN VANET	DESCRIPTION
DENIAL OF SERVICE	DoS Attack Check the Authorized user to utilize the service as of the suffered node. It allows dummy message for jamming the Channel in addition to lessening the network's effectiveness.
ROUTING ATTACK	Here, the attacker either disorders or releases the packet.
IMPERSONATE	Approved nodes identities are used to access the network. This was done by active attackers.
WORM HOLE ATTACK	Here, competitor attains packets at one point and then tunnels it to a different point on the network and repeats the steps.
BLACK HOLE ATTACK	In this sort of attack, firstly the attacker engages the nodes to transport the packet via itself.
GRAY HOLE ATTACK	This is the addition of BH attack. The MN behaves as a black node; however, it releases the packet selectively.

Jyoti et.al [13] presented a different position faking attacks on VANETs including attacker(s) that sent fake traffic caution messages to generate a delusion of incidence of a non-existent occurrence. The attacker performed this by utilizing virtual identities along with counterfeited positions. To shun the unanticipated traffic events, the nodes getting these scam messages changed their driving behavior. Unlike the existent detection approaches, this method was not centered on the conception of evaluating the site of senders. The detection techniques' efficacy for disparate attack situations was compared. Simulation outcomes demonstrated the efficacy along with the adaptability of this approach for VANETs. But the method cannot detect the position and ID foraging attack dynamically.

DeepaThilak and Amuthan [14] propounded an improved version of ant colony optimization (ACO) termed Cellular Automata

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

centered Improved Ant Colony-centered Optimization Algorithm (CA-IACOA) for isolating the conception of stagnation that was the chief disadvantage aimed at CA-ACOA mitigation algorithm to facilitate a worldwide searching setting or Pheromone adaptive adjustment approach. CA-IACOA achieved this active adaptation via negative feed-back conception to identify an optimum solution. It confirmed a trusted and also accurate worldwide search dimension intended for ameliorating the degree along with the possible extent of attacker's mitigation. The shortcoming of the method was that it could not give a better detection rate as well as mitigation rate.

Mohammad et.al [15] presented the detection as well as prevention RREQ flooding attack. This algorithm detected the MN as per the entire nodes' behavior on the network. B-AODV was devised with these aspects: (1) The utilization of adaptive threshold as per network conditions along with nodes actions (2) Not utilizing extra routing packets to recognize MN (3) Performed detection together with prevention operations autonomously on every node (4) Performed detection together with prevention operations in actual time (5) No requirement aimed at promiscuous mode. This technique for detection as well as avoidance flooding attack used average along with standard deviation. But the method was only applicable to DOS attacks on VANET.

Raghad et.al [16] suggested a cross-layer cooperative system to detect BH attack which generally targeted the quality of services secured optimized links state routing protocol (QoS-OLSR) on VANETs. Allotting signature key intended for every genuine user at the physical layers together with employing the watchdog monitoring method at the routing layer improved the general system detection. In addition, as cooperative watchdog detection considered any genuine collision to be malicious, the false positive rate was further lessened by differentiating betwixt attacks and collisions on the MAC layer. The method was not suitable for application oriented attacks and MAC layers related attacks.

Karan et.al [17] recommended an efficient method which detected all malicious IP addresses. Centered upon the Bloom filter, a storage-proficient data structure that merely required a fixed-length table intended for recording pertinent vehicle traffic information was suggested. An IP CHOCK technique was then implemented to detect sudden changes on the vehicle traffic traits that corresponded to the incidence of flooding attacks. The adopted technique, that utilized the Bloom filter aimed at the filtering process, was best suitable for smaller scale and also larger scale DOS attacks. Simulation outcomes demonstrated that the detection rate increased when the optimum quantity of nodes was faked by means of the attackers.

Xia et.al [18] suggested an event based reputation system (EBRS), wherein a dynamic reputation together with trusted value aimed at every event was utilized to repress the extent of spam messages. This method detected SA with made-up identities as well as purloined identities in the communication process; it as well defended in opposition to the conniving SA since every incident had an elite reputation value along with trusted value. Simulation outcomes showed that EBRS was capable of defending and detecting multi-source SA with higher performances. But the drawback of the method was that it could not establish the trust relationship among the participant vehicles automatically.

RoselinMary et.al [19] projected an Attacked Packet Detection Algorithm (APDA) which was utilized to recognize the DOS attacks prior to the confirmation time. This minimized the over-head delay intended for processing as well as enhancing the safety on VANET. The mechanism was attached to every RSU. Vehicles sent messages to RSU via APDA. It was to identify a particular location of the vehicles (messaged). Subsequent to detecting the site of vehicle detail, it was stocked up on an RSU. Every vehicle had OBU along with TAMPER PROOF gadget. These store comprehensive information regarding the vehicles. The algorithm was not applicable for multiple invalid requests from multiple vehicles simultaneously.

2.2 Detecting Sybil Attacks in Urban Vehicular Networks

Rasheed and Heekuck [20] intended at 2 conflicting objectives, i.e. SA and privacy in VANET. To circumvent SA during scheduled beacons, this approach used tamper resistant model (TRM) aimed at the pre-assembly data examination on data. It was used to gather beacons aimed at event reporting message (ERM), after that it used RSUs for Sybil nodes localization in VANET along with a report to the revocation authority (s). In both cases of beacons, this approach preserved user privacy in addition to ERM by dropping the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

aforementioned message identification information and still-revocable if needed. Additionally, this scheme was lightweight and also computationally less costly contrasted with the previous scheme.

Muhammad et.al [21] presented a protocol which was used in VN aimed at Sybil detection. The innovation comes as of the physical phenomenon fusion and from cyber domain to identify SA. The physical and cyber environments were combined to make the protocol effective, efficient, practical, and also simple. Furthermore, this approach presented the attack techniques in advanced, in which the detection system was known by the attacker and had a priori road information. The protocol showed alike performance in support of Normal Dispersion Efficiency Attack model, though the Minimum Efficiency Attack model remained undetected at higher Sybil percentages. But the method was coded using the TCL script and not by an object oriented language.

Thiago et.al [22] projected anonymous authentication as well as SA detection protocol intended for VANETs termed as ASAP-V. To give users' privacy, multi-level anonymity set structural design was provided by the protocol, with pseudonyms and group signature. The exploratory outcomes showed it to be secured and efficient. Furthermore, ASAP-V was resilient to the detection of false positive as well as false-negative without the help of central infrastructures amid detection time (DT) of SA. The drawback was that the dependability of the whole system may not be compromised due to the high impact on people's lives.

Bo et.al [23] reviewed a cooperative technique to appraise the suspicious node's physical position. Further two solutions were suggested against existing challenges that was the statistical detection method and Evidence System. The attacks commenced via greedy drivers were suppressed effectively by these methods. Actual US maps based simulations along with traffic models proved this scheme's performance. This scheme proved that an economical approach was used to suppress SA without any extra support from specific positioning hardware. The shortcoming of the method was that the method only commenced the fundamental ideas of the sub-system such as presence evidence system as well as the channel noise estimation. And another drawback was that the signal strength readings were not precise naturally, on the off-chance that the Sybil nodes were claimed to be extremely close to the physical vehicle, then it is tough to distinguish the Sybil nodes.

Amuthan and Kaviarasan [24] projected a weighted inertia-centered dynamic virtual bat algorithm (WIDVBA) used for improving the conventional Virtual bat scheme's characteristics that integrated the particle swarm optimization (PSO) along with simulated annealing merits for effective localization of NLOS node. This suggested WIDVBA prohibited the issue of early convergence via including the weighted inertial factor profit contrasted with the conventional active virtual binary bat-centered NLOS localization methods.

Iwendi et.al [25] aimed at large-scale VANETs, suggested a biologically-stimulated Spider Monkey Time Synchronization (SMTS) methods. The suggested system was centered upon the meta-heuristic stimulated method via spider monkey activities. An artificial spider monkey procedure was applied to review the SA techniques in VANETs to expect a variety of vehicular collisions during compactly deployed challenge region. Additionally, this suggested a pseudo code algorithm and it was inconstantly distributed for energy effectual time synchronization within scenarios of 2-way packet delivery to assess the propagation delay and clock off-set in the transmission of packet beacon [message] to destination vehicles properly. It was performed well over longer transmission distance aimed at Sybil detection in VANETs in respect of intrusion detection rate, measurement accuracy as well as energy efficiency.

Tong et.al [26] suggested a method to detect SA in VANET. The computational workload was distributed from DMV to RSBs, while the hash collisions were used to release only a limited amount of information. A scalable and lightweight protocol was used in this method to detect SA. Here, a malicious user was pretended to be manifold (other) vehicles and that was identified in a dispersed manner during passive overhearing with a set of fixed nodes referred to as road-side boxes (RSBs). The SA detection doesn't need any vehicle to disclose its uniqueness; therefore at every time, the privacy was preserved.

Grover et.al [27] exploited the Sybil nodes' characteristics as fake identities neighbors

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

(originated as of an MN) also share common important neighboring nodes. The motivation behind the plan of this approach was to spot Sybil nodes fast without utilizing secret information exchange as well as special hardware support. Then, this approach was evaluated on the real traffic scenario. The method was not applicable for the detection of ON/OFF transmission range attacks.

Table 4: Analysis of Detection of SA in VANET

Researcher Name and year	Model Used	Purpose	Limitations
Xia et.al [18]	EBRS	repress the spread of false messages	Less security.
Thiago et.al [22]	Authentication and SA detection protocol for VANET (ASAP-V)	Detect SA	The RSU as of forwarding every single prosecution message to the CA
Bo et.al [23]	Random Sample Consensus (RANSAC)-based algorithm	Make more robust against outlier data formulated by Sybil nodes.	Signal strength readings are not precise in nature.

2.3 Security Challenges in VANET

Shiang-Feng et.al [28] suggested an effective Identity-centered Batch Verification (IBV) system for vehicle-to-infrastructure as well as inter-vehicle communications in VANET. In the arbitrary oracle model, the IBV system was utilized to provide provable security. The suggested scheme contains 3 phases: anonymous identity generation, system initialization including message signing along with message verification. Then, this IBV scheme was assessed with other schemes of batch verifications in respect of transmission overhead and computation delay. Furthermore, the scheme practicality and efficiency were substantiated by the scrutiny of simulation. Simulation outcomes showed that the message loss rate along with average message delay of the suggested IBV scheme was below those of the previous methodologies.

Wenjia et.al [29] recommended an attack-defiance trust management technique labeled as ART was used to assess the dependableness of traffic data in addition to vehicle nodes for VANETs. Especially, data trust was evaluated centered upon the data that was sensed as well as collected as of multi-vehicles. In addition, the node trust was evaluated in 2D, i.e., functional as well as recommendation trust, pointed out how probably a node could complete its functionality as well as how dependable the recommendations as of a node for other nodes will be, correspondingly. The effectiveness along with the efficacy of the ART scheme was validated via wide experiments. The advanced trust management idea was applicable to various levels of VANET applications to progress mobility, traffic safety and also environmental protection with ameliorated trustworthiness.

Osama and Azzedine [30] propounded an integrated protocol to confirm a prefixed position when direct communication betwixt the verifier and the queried node was impossible. Along with verification of node location on a multiple-hop cooperative strategy, numerous security measures were encompassed to augment the message integrity. The simulation outcomes evinced that the propounded protocol elevated the vehicles' rate of neighbor awareness under the influence of simulated barriers.

Manuel et.al [31] proffered a proactive and cooperative strategy for neigbor position corroboration grounded upon the information exchanged amongst 1-hop neighbors. CNPV protocol was simply pliable to disparate Warning Messages Dissemination (WMD) schemes which exploited the neighbor detail to choose the relevant forwarding strategy in VANETs. CNPV permitted the verification of the neighbors' position before choosing the subsequent forwarding vehicle by supporting the dissemination as well as by restricting the count of vehicles which does not attain the necessary warning messages. Then, assessed the CNPV protocol's performance by pairing it with 2 dissemination algorithms, UV-CAST and eMDR, showing how (i) the existence of adversary nodes influenced the WMD performance in urban cases, and (ii) CNPV could aid to diminish the influences of adversarial users on the VN.

Chin-Ling et.al [32] recommended a secured ambulance communication protocol aimed at VANET to assure that messages would not be exposed or purloined. The recommended system

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

incorporated the symmetric encryption, digital signature and also MAC approaches and thereby had attained non-repudiation, availability, known-key security, integrity, confidentiality, session key security, mutual authentication, and the competency to evade recognized attacks. Lastly, with NS2 outcomes that were grounded on the Taipei city road map and actual automobile density statistics.

Mingzhong et.al [33] propounded a lightweight as well as effectual verification strategy termed LESPP along with robust privacy preservation for secured VANET communication. The propounded system deployed self-created pseudo identity to assure the conditional traceability along with privacy preservation. Here, it only needed the generation of lightweight Message Authentication Code (MAC) and symmetric encryption for signing a message in addition to attaining a faster re-generation of MAC for verification. Contrasted with the prevailing public key centered schemes, the propounded scheme notably diminished the computation expenditure by 102–103 times and also diminished the communication overhead by means of 41.33–77.60 %, hence attaining resilience to DoS attack.

Changji et.al [34] recommended a provable secured pseudo centered cryptosystem with a trustful authority, encompassing i) a pseudonym-centered encryption strategy, ii) a pseudonym-centered multiple-receiver encryption approach, iii) a pseudonym-centered signature strategy, and iv) a pseudonym-centered 1-pass key establishment protocol. The efficacy of data access was highly augmented by permitting the coordination and sharing of cached data amongst numerous vehicles, in addition to the anonymity of vehicles, non-repudiation, data confidentiality and integrity were assured by deploying the recommended pseudonym-centered cryptosystem. Simulation outcomes had exhibited that the recommended data access strategy was relevant to the VANET.

Seyed et.al [35] suggested a conditional privacy-preserving authentication protocol that could be utilized for V2I and V2V interactions or a blend of both, like a vehicle-to-vehicle- to infrastructure interactions (V2V2I). This encompassed the gain of including batch corroboration as a verification strategy. This methodology was an integration of RS centered and TPD base strategies in which the chief network keys and the imperative network information were saved in the TPD of RSUs. Here, contrasted disparate authentication strategies of VANET namely, RSUB, GSB, TDPB, and HAB. Then, the security of this methodology was confirmed via informal examination, formal proof, and automated analysis tool. The outcomes were contrasted with other strategies and it proffered better security, efficacy along with performance in VANETs.

2.4 Robust Method for Sybil Attack Detection

Panagiotis et.al [36] recommended a rule-centric anomaly detection strategy, termed RADS, which observed and timely spotted the SA in massive WSNs. At its base, the recommended expert scheme depended on a UWB (Ultra-Wide Band) ranging-centered detection algorithm that worked in a disseminated manner requiring no information sharing or cooperation betwixt the sensor nodes to execute the anomalies detection. The possibility of the recommended strategy was verified analytically, whilst the RADS's performance in disclosing SA was widely assessed numerically and also mathematically. The attained outcomes delineated that the RADS attained higher detection accurateness and lower false alarm rate confirming it as a propitious ADS candidate for this category of WSNs. The limits of the system were 1) the application of the ADS might induce lack of compliance with traditional WSNs, 2) the offered expert system concentrated on stationary networks. However, mobility should be examined since many critical application sectors of sensor networks like military, health care, and industry required the use of mobile sensor nodes, and 3) the detection of indirect SA is not supported by the suggested system. Nevertheless, a Sybil node could steal the identity of a legal node via impersonation.

Neil et.al [37] propounded a SybilBelief which was a semi-supervised learning strategy to spot Sybil nodes in dissemination systems. SybilBelief considered i) social networks amongst the nodes existent in the system, ii) a smaller set of recognized benign nodes, optionally, iii) a smaller set of recognized Sybil nodes as input. Subsequently, SybilBelief broadcasted the label information as of the recognized benign and/or Sybil nodes to the resting ones in the system. SybilBelief was flexible to noise regarding the Sybil and benign nodes. Additionally, SybilBelief executed orders of magnitudes better on considering the prevailing Sybil classification approaches and notably better on considering the prevailing Sybil ranking methodologies. But the security problems were aroused in graph based

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Botnet detection, reputation systems, and private information inference.

Wei and Xiaojin [38] suggested RTSP, a strong and secured timesync protocol deploying a graph theoretical methodology. Different from former secure timesync protocols, RTSP was competent to execute anomalies detection at per-message degree, rather than at node level. This augmented the detection competency facilitates RTSP to become stronger against manipulation attacks and SA. Extensive experiential outcomes evinced the elevated efficacy of this suggested protocol. But this security mechanism cannot prevent the system from jamming attcks and DoS attacks.

Morteza et.al [39] propounded a centrality relation which was utilized in the incentive strategy to handle the problem. Incidentally, the more differed the nodes getting service as of a peer were, the superior would be the peer reputation. The outcomes evinced that the longer the network existence, the more Free-riders were spotted, and the count of services made for the collusive nodes would as well be diminished. But the Convergence speed of the system was low.

Binghui et.al [40] recommended SybilSCAR, a structure-centric methodology to execute Sybil identification in OSNs. SybilSCAR sustained the benefits of prevailing approaches whilst overcoming their restrictions. Particularly, SybilSCAR was Scalable, Convergent, Robust and Accurate for labeling noises. Here, primarily to recommend a prototype to merge RW-centered and LBP-centered methods. Under this prototype, those methods could be perceived as iteratively employing a (disparate) local rule to each user that broadcasted the label information amongst a social graph. Secondly, to model a local rule, that SybilSCAR iteratively employed to each user to spot Sybils. Lastly, the SybilSCAR with a modern RW-centered methodology and a modern LBP-centered methodology was contrasted, utilizing the synthetic Sybils as well as massive social network data-sets in addition to actual Sybils. Other types of sybils such as web spams, fake reviews, and fake likes were not detected in this method.

Noor et.al [41] suggested a light-weight trust approach for spotting SAs in clustered WSNs. For spotting the SA, this work suggested an ETS (Energy Trust System) for WSNs. It deployed multi-leveled detection grounded on position and identity verification. Subsequently, a trust algorithm was employed grounded upon the energy of every sensor node. Data aggregation was implemented to conserve energy and to diminish communication overhead. The simulation outcomes evinced that the suggested ETS was effectual and stronger in spotting SA in respect of the false and true positive rates. The approach was not valid for Mobile WSNs, MANETs, and the detection ability of ETS for other sorts of attacks were not giving efficient results.

Muhammad et.al [42] propounded an effectual centralized key management procedure to proffer a secured communication service amongst the users of OSNs. The fundamental principle of this strategy was the presence of the roadblocks that any user endeavored to enter a group should go through a task which merely a human user could achieve. Henceforth, automatic controlled accounts were evaded from entering, whilst the group would comprise just of users who were established as genuine. The strategy was extremely effectual in detecting bot accounts that facilitate it to shield the network from malicious behavior of forged accounts.

Mojtaba Jamshidi et.al [43] proffered a model of SA in cluster-centered sensor networks say LEACH. Then an algorithm grounded upon RSSI and incorporation of cluster head nodes were suggested to shield against this attack prototype. The proffered algorithm was simulated; in addition, its performance was assessed in respect of TDR, communication overhead as well as FDR. Experiential outcomes evinced that the proffered algorithm imposed lesser communication overhead on the network and could spot 99.8% of Sybil nodes with 0.08% FDR (average). Additionally, the proffered algorithm's performance in respect of average FDR and also average TDR was contrasted with other prevailing algorithms that symbolized that the recommended algorithm performed better on considering other existent algorithms.

Figure 4 delineates the fundamental features of [21] protocol when the number of vehicles in an upstream platoon is $n_u = 50$. The Y-axis symbolizes the DT, or the number of RSUs traversed prior to SA detection. When, μ^* increases, SAs are detected quicker. This higher value of μ^* brings augmented dispersion that also elevates the odds of spotting anomalous platoons. Moreover, as the percentage of Sybil attackers differs, the DT also differs. As the percentage

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

elevates, anomalous platoons, become easier to spot and speeds the DT.

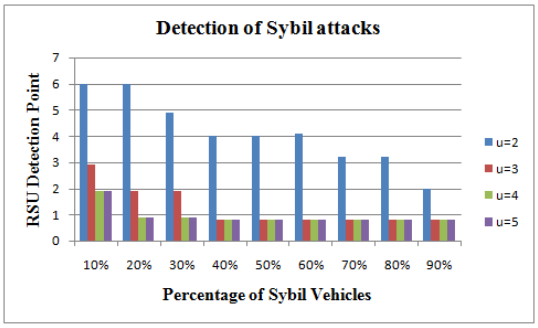

Figure 4: Sybil Detection Under A Varying Percentage Of Sybil Vehicles

Figure 5 [27] delineates the comparison of the percentage of Sybil vehicles with RSU detection points. Sybil attacker is encompassed with more count of fake identities, in addition, all such identities are concurrently utilized and it has multiple neighbor nodes as contrasted to a legitimate node. Every Sybil identities related to an attacker node is encompassed with the same location. Legitimate nodes comprise several neighbor nodes as contrasted to any attacker node. This identity provided by an attacker might also spoof the transmission power to expand its target region, thus augmenting the count of neighbor legitimate nodes. It can well be evidently comprehended as of Figure 4.

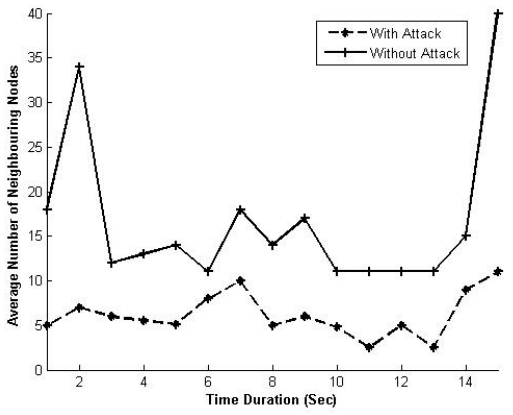

Figure 5: Comparison Of Neighboring Nodes For Both The Presence And Absence Of The Attack

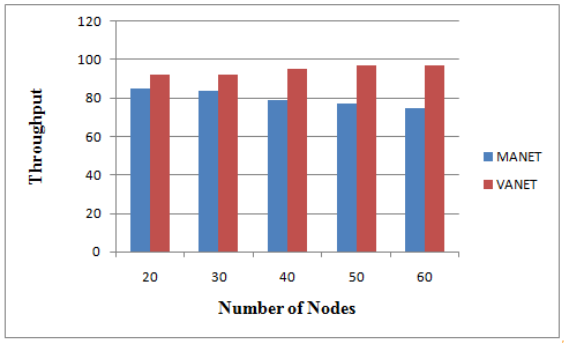

Figure 6: Nodes Vs Throughput In MANET And VANET

From Figure 6 [44], it is established that the VANET performance centered on the throughput parameter is better when compared with the MANET performance. It is concluded that the QoS of VANET contributes an advantage over MANET since the throughput parameter itself has a major impact in QoS. In the above graph, the result of VANET and MANET which is centered on the number of nodes and throughput respectively is given.

3. CONCLUSION

The advancement of wireless communication directs researchers to envisage and expand the idea of VN, also termed as VANETs. In VANET, multiple attacks are being executed by the malevolent nodes. SA is the problem of mobile networks, reputation systems, and peer-to-peer networks. Disparate solutions can spot, limit, or evade attacks in diverse scenarios. The central motive of SA detection methodology is that every physical node is permitted to comprise just '1' valid identity. The present efforts of research society are to bolster VANETs with practical security solutions that can handle the challenging VANETs setting. This literature work emphasizes a) the various prevailing methodologies of SA in VANETs, b) detection of SA in VANETs, and c) security in VANET network. According to the survey, these techniques have some advantages as well as disadvantages to implement. Most of the techniques have an ability to detect SA but they are applied to limited vehicular nodes. The presented methods are concerned with the VANETs security as well as performance efficiency for helping the researchers and developers to identify and also distinguish the main features for VANETs security and performance efficiency. Some open research challenges were presented that still requires attention of the researchers to set up the VANETs technologies, infrastructures, as well as services effectively and securely. Finally a robust secured

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

infrastructure is to be considered in all aspects of a SA and it ought to be simple to incorporate with the prevailing system in a gainful mode. As of this survey, it has been comprehended that the standard methods must exist to enable efficient communication for different applications all together in a multi-dimensional way as well as trounces issues linked with those applications. VANET would offer a better platform as well as effective communication betwixt vehicles with additional advancement and also the evolution of new approaches. This survey mainly concentrates on SA. In future work, a detail survey on some critical and other kinds of attacks on VANET, the challenges present in the attack detection mechanisms, and the solutions for those detection methods will be given.

REFERENCES

[1] Yipin Sun, Rongxing Lu, Xiaodong Lin, Xuemin Shen, and Jinshu Su, "An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications", *IEEE Transactions on Vehicular Technology*, Vol. 59, No. 7, 2010, pp. 3589-3603.

[2] Rongxing Lu, Xiaodong Lin, Haojin Zhu, and Xuemin Shen, "An intelligent secure and privacy-preserving parking scheme through vehicular communications", *IEEE Transactions on Vehicular Technology*, Vol. 59, No. 6, 2010, pp. 2772-2785.

[3] Perumal R., K.P.Sridhar, "Sybil attack detection in urban vehicular networks", *International Journal of Innovative Research in Computer and Communication Engineering*, Vol. 2, No. 1, 2014.

[4] Shan Chang, Yong Qi, Hongzi Zhu, Jizhong Zhao, and Xuemin Shen, "Footprint: Detecting sybil attacks in urban vehicular networks", *IEEE Transactions on Parallel and Distributed Systems*, Vol. 23, No. 6, 2012, pp. 1103-1114.

[5] Tong Zhou, Romit Roy Choudhury, Peng Ning, and Krishnendu Chakrabarty, "Privacy-preserving detection of Sybil attacks in vehicular ad hoc networks" , 2007, pp. 1-8.

[6] Irshad Abbasi, and Adnan Shahid Khan, "A review of vehicle to vehicle communication protocols for VANETs in the urban environment", *Future Internet,* Vol. 10, No. 2, 2018, pp. 14.

[7] Sabih ur Rehman, M. Arif Khan, Tanveer A. Zia, and Lihong Zheng, "Vehicular ad-hoc networks (VANETs)-an overview and challenges", *Journal of Wireless Networking and Communications*, Vol. 3, No. 3, 2013, pp. 29-38.

[8] Sharmila, S., and G. Umamaheswari, "Detection of sybil attack in mobile wireless sensor networks", *International Journal of Engineering Science & Advanced Technology*, Vol. 2, No. 2, 2012, pp. 256-262.

[9] Amol Vasudeva, and Manu Sood, "Sybil attack on lowest id clustering algorithm in the mobile ad hoc network", *International Journal of Network Security & Its Applications*, Vol. 4, No. 5, 2012, pp. 135.

[10] Shikha Sharma, "A review: analysis of various attacks in VANET", *International Journal of Advanced Research in Computer Science*, Vol. 7, No. 3, 2016.

[11] Sakshi Gupta, and Taranjit Singh Aulakh, "Prevention of Sybil attacks in VANETS using bacterial foraging optimizations algorithm", *International Journal of Computer Science Trends and Technology (IJCS T)*, Vol. 4, No. 3, 2016.

[12] Kamlesh Chandra Purohit, Sushil Chandra Dimri, and Sanjay Jasola, "Mitigation and performance analysis of routing protocols under Black-Hole attack in vehicular ad-hoc network (VANET)", *Wireless Personal Communications*, Vol. 97, No. 4, 2017, pp. 5099-5114.

[13] Jyoti Grover, Vijay Laxmi, and Manoj Singh Gaur, "Attack models and infrastructure supported detection mechanisms for position forging attacks in vehicular ad hoc networks", *CSI Transactions on ICT*, Vol. 1, No. 3, 2013, pp. 261-279.

[14] Deepa Thilak, K. and A. Amuthan, "Cellular automata-based improved ant colony-based optimization algorithm for mitigating DDoS attacks in VANETs", *Future Generation Computer Systems*, Vol. 82, 2018, pp. 304-314

[15] Mohammad Javad Faghihniya, Seyed Mojtaba Hosseini, and Maryam Tahmasebi, "Security upgrade against RREQ flooding attack by using balance index on vehicular ad hoc network", *Wireless Networks*, Vol. 23, No. 6, 2017, pp. 1863-1874.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[16] Raghad Baiad, Omar Alhussein, Hadi Otrok, and Sami Muhaidat, "Novel cross layer detection schemes to detect blackhole attack against QoS-OLSR protocol in VANET", *Vehicular Communications*, Vol. 5, 2016, pp. 9-17.

[17] Karan Verma, Halabi Hasbullah, and Ashok Kumar, "Prevention of DoS attacks in VANET", *Wireless Personal Communications*, Vol. 73, No. 1, 2013, pp. 95-126.

[18] Xia Feng, Chun-yan Li, De-xin Chen, and Jin Tang, "A method for defensing against multi-source Sybil attacks in VANET", *Peer-to-Peer Networking and Applications*, Vol. 10, No. 2, 2017, pp. 305-314.

[19] RoselinMary, S., M. Maheshwari, and M. Thamaraiselvan, "Early detection of DOS attacks in VANET using Attacked Packet Detection Algorithm (APDA) ", *In Information Communication and Embedded Systems (ICICES), 2013 International Conference on, IEEE*, 2013, pp. 237-240.

[20] Rasheed Hussain, and Heekuck Oh, "On secure and privacy-aware sybil attack detection in vehicular communications", Wireless Personal Communications, Vol. 77, No. 4, 2014, pp. 2649-2673.

[21] Muhammad Al-Mutaz, Levi Malott, and Sriram Chellappan, "Detecting Sybil attacks in vehicular networks", Journal of Trust Management, Vol. 1, No. 1, 2014, pp. 4.

[22] Thiago Bruno M. de Sales, Angelo Perkusich, Leandro Melo de Sales, Hyggo Oliveira de Almeida, Gustavo Soares, Marcello de Sales, "ASAP-V: A Privacy-preserving Authentication and Sybil detection Protocol for VANETs", Information Sciences, 2016.

[23] Bo Yu, Cheng-Zhong Xu, and Bin Xiao, "Detecting sybil attacks in VANETs", Journal of Parallel and Distributed Computing, Vol. 73, No. 6, 2013, pp. 746-756.

[24] Amuthan, A., and R. Kaviarasan, "Weighted inertia-based dynamic virtual bat algorithm to detect NLOS nodes for reliable data dissemination in VANETs", Journal of Ambient Intelligence and Humanized Computing, 2018, pp. 1-11.

[25] Celestine Iwendi, Mueen Uddin, James A. Ansere, P. Nkurunziza, J. H. Anajemba, and Ali Kashif Bashir, "On detection of sybil attack in large-scale VANETs using spider-monkey technique", IEEE Access, Vol. 6, 2018, pp. 47258-47267.

[26] 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, 2011, pp. 582-594.

[27] Jyoti Grover, Vijay Laxmi, and Manoj Singh Gaur, "Sybil attack detection in VANET using neighbouring vehicles", International Journal of Security and Networks, Vol. 9, No. 4, 2014, pp. 222-233.

[28] Shiang-Feng Tzeng, Shi-Jinn Horng, Tianrui Li, Xian Wang, Po-Hsian Huang, and Muhammad Khurram Khan, "Enhancing security and privacy for identity-based batch verification scheme in VANETs", IEEE Transactions on Vehicular Technology, Vol. 66, No. 4, 2017, pp. 3235-3248.

[29] Wenjia Li, and Houbing Song, "ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks", IEEE Transactions on Intelligent Transportation Systems, Vol. 17, No. 4, 2016, pp. 960-969.

[30] Osama Abumansoor, and Azzedine Boukerche, "A secure cooperative approach for nonline-of-sight location verification in VANET", IEEE Transactions on Vehicular Technology, Vol. 61, No. 1, 2012, pp. 275-285.

[31] Manuel Fogue, Francisco J. Martinez, Piedad Garrido, Marco Fiore, Carla-Fabiana Chiasserini, Claudio Casetti, Juan-Carlos Cano, Carlos T. Calafate, and Pietro Manzoni, "Securing warning message dissemination in VANETs using cooperative neighbor position verification", IEEE Transactions on Vehicular Technology, Vol. 64, No. 6, 2015, pp. 2538-2550.

[32] Chin-Ling Chen, Chau Chang, Chun-Hsin Chang, and Yuan-Fen Wang, "A secure ambulance communication protocol for VANET", Wireless Personal Communications, Vol. 73, No. 3, 2013, pp. 1187-1213.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[33] Mingzhong Wang, Dan Liu, Liehuang Zhu, Yongjun Xu, and Fei Wang, "LESPP: lightweight and efficient strong privacy preserving authentication scheme for secure VANET communication", Computing, Vol. 98, No. 7, 2016, pp. 685-708.

[34] Changji Wang, Dongyuan Shi, Xilei Xu, and Jian Fang, "An anonymous data access scheme for VANET using pseudonym-based cryptography", Journal of Ambient Intelligence and Humanized Computing, Vol. 7, No. 1, 2016, pp. 63-71,.

[35] Seyed Morteza Pournaghi, Behnam Zahednejad, Majid Bayat, and Yaghoub Farjami, "NECPPA: A novel and efficient conditional privacy-preserving authentication scheme for VANET", Computer Networks, Vol. 134, 2018, pp. 78-92.

[36] Panagiotis Sarigiannidis, Eirini Karapistoli, and Anastasios A. Economides, "Detecting Sybil attacks in wireless sensor networks using UWB ranging-based information", Expert Systems with Applications, Vol. 42, No. 21, 2015, pp. 7560-7572.

[37] Neil Zhenqiang Gong, Mario Frank, and Prateek Mittal, "Sybilbelief: A semi-supervised learning approach for structure-based sybil detection", IEEE Transactions on Information Forensics and Security, Vol. 9, No. 6, 2014, pp. 976-987.

[38] Wei Dong, and Xiaojin Liu, "Robust and secure time-synchronization against sybil attacks for sensor networks", IEEE Transactions on Industrial Informatics, Vol. 11, no. 6, 2015, pp. 1482-1491.

[39] Morteza Babazadeh Shareh, Hamidreza Navidi, Hamid Haj Seyyed Javadi, and Mehdi HosseinZadeh, "Preventing Sybil attacks in P2P file sharing networks based on the evolutionary game model", Information Sciences, vol. 470, 2019, pp. 94-108.

[40] Binghui Wang, Le Zhang, and Neil Zhenqiang Gong, "SybilSCAR: Sybil detection in online social networks via local rule based propagation", In INFOCOM 2017-IEEE Conference on Computer Communications, IEEE, 2017, pp. 1-9.

[41] Noor Alsaedi, Fazirulhisyam Hashim, A. Sali, Fakhrul Z. Rokhani, "Detecting sybil attacks in clustered wireless sensor networks based on energy trust system (ETS)", Computer Communications, 2017.

[42] Muhammad Al-Qurishi, Sk Md Mizanur Rahman, M. Shamim Hossain, Ahmad Almogren, Majed Alrubaian, Atif Alamri, Mabrook Al-Rakhami, and B. B. Gupta, "An efficient key agreement protocol for Sybil-precaution in online social networks", Future Generation Computer Systems, Vol. 84, 2018, pp. 139-148.

[43] Mojtaba Jamshidi, Ehsan Zangeneh, Mehdi Esnaashari, Aso Mohammad Darwesh, and Mohammad Reza Meybodi, "A novel model of sybil attack in cluster-based wireless sensor networks and propose a distributed algorithm to defend it", Wireless Personal Communications, 2018, pp. 1-29.

[44] Omkar Pattnaik and Binod Kumar Pattanayak," Performance Analysis of MANET and VANET based on Throughput Parameter", International Journal of Applied Engineering Research ISSN 0973-4562, Vol. 12, No. 18, 2017 , pp. 7435-7441.