Merged technique to prevent SYBIL Attacks in VANETs

Salman Ali Syed
Department of Computer Science,
College of Sciences and Arts
Jouf University,
Tabarjal , KSA
sasyed@ju.edu.sa

B.V.V.S Prasad
Department of Computer Science Engineering
DRK Institute of Science and Technology
Hyderabad,India
macromca@gmail.com

***Abstract*— Vehicular ad hoc Network (VANET) are a class of ad hoc systems work to guarantee the safety and security of traffic. An important point in VANET is the manner by which to believe the data transmitted when the neighboring vehicles are quickly changing and moving all through range. The fundamental point of this paper is to distinguish Sybil attack in VANET. A two phase security based mechanism is proposed to give reliable solution in identifying and blocking the Sybil attacked nodes to secure the information and providing safety and trust on the application. In the first phase Public Key Infrastructure (PKI) is taken and in the second phase hash function is considered. In this way to defeat Sybil attack we can easily recognizing Sybil attacks in VANET with much accurate.**

Keywords—VANET, Public Key Infrastructure, SYBIL attack , Authentication.

I.ⁿ INTRODUCTION

Vehicular Ad-Hoc Network (VANET) is to transfer the running vehicles as nodes to build a MANET. So, this technology makes every vehicle into Wi-Fi node and connects with each other in a particular radius. VANET have occupied a major place in the area of both in research and Industry .This technology has a high mobility, one time interactions and topology changes rapidly. VANET and MANET have same characteristics.

Vehicular Ad-hoc Network (VANET) is a rising and most difficult research zone to give Intelligent Transportation System (ITS) administrations to the end clients. With the fast improvement of remote advancements people have begun to use remote access all over, even in running vehicles. Figure 1 shows the architecture of Vehicular ad-hoc network (VANET) is a set of motors in a wireless network that is dynamic in nature and speaks with each different and/or with nearby signaling towers.

The intelligent Transportation structures (ITS) principal aspire is to provide a solution for unintended safety of passengers and the site heavy traffic problems. The types of communications.

Vehicle To Vehicle (V2V): In this type of communication motor vehicles communicate with each other in ad hoc approach. In V2V, a motor vehicle can accept broadcast and change useful traffic information like road accidents, information about traffics in a particular region or with different nearest nodes.

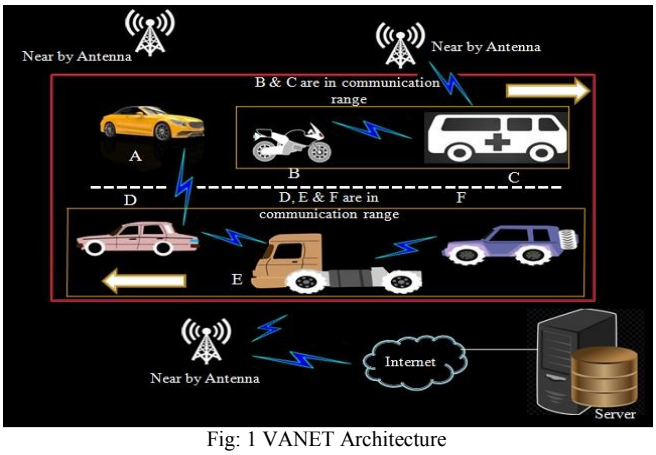

Fig: 1 VANET Architecture

Vehicle to Infrastructure (V2I): In this type of communication interaction is done between the nodes and the infrastructure, to speak about treasured facts inclusive of traffic and road situations and safety events that have been taken into consideration. On this V2I, a vehicle (node) launches a connection between Nearby Antenna and contact with outside networks which is the internet.

Vehicular Ad-hoc Network (VANET) is a gathering of vehicles in a remote system that is dynamic in nature and speaks with one another as well as with close-by Nearby Antenna. A VANET is a system that does not depend on any central system for giving communication among the claimed On Board Units (OBUs) in adjacent vehicles, and among OBUs and nearby fixed framework RSU utilizing a method called, Dedicated Short Range Communication (DSRC). Security of vehicular systems remains the most noteworthy worry in VANETs organization – in light of the fact that it is compulsory to guarantee open and transportation safety. Wireless Access in Vehicular Environment (WAVE) design likewise characterizes the security of message vehicular Ad-hoc Network (VANET) is a rising and most difficult research zone to give Intelligent Transportation System (ITS) administrations to the end clients. With the fast improvement of remote advancements, individuals have begun to appreciate remote access all over, even in vehicles progressing. Today, vehicle producers and broadcast communication companies have collaborated together to furnish vehicles with remote advances which not just convey different data innovation administrations to vehicles yet in addition enhance the security out and about and movement proficiency. Attacking on VANET Technology will cause major problems to the transport and cause great disturbance on road .Nearby Vehicles cannot

978-1-5386-8125-1/19/$31.00 ©2019 IEEE

communicate with each other, major collisions can happen due to fake information transfer, damage to the property, etc.

1.1 Attacks in the VANET

So as to show signs of improvement assurance from attackers, it is fundamental to have the learning about the attacks in VANET against security necessities. These attacks depend on

(i)" Identification and Authentication
(ii)" Privacy
(iii)" Access Control
(iv)" Routing attack and
(v)" Non-repudiation discussed in detail.

1.2 SYBIL ATTACK IN VANET

The Sybil attack is where a solitary defective element, called a malicious node, can exhibit various personalities known as Sybil nodes or fake nodes. This attack can influence the usefulness of the system to serve the attacker. Sybil attacks are additionally equipped for disturbing the directing systems in vehicular specially appointed systems. Sybil attack was first presented by J. R. Douceur in [4]. As indicated by Douceur, the Sybil attack is an attack in which a solitary element can control a generous division of the framework by introducing numerous personalities. These different personalities are known as Sybil characters. Figure: 2. Sybil attacks can acquire major security dangers to VANETs: 1. In Sybil attack, a malicious node makes a hallucination of the traffic congestion by asserting multiple personalities. The driver of the attacked node may misguide the neighboring vehicles that there is traffic blockage ahead, with the goal that they will pick other ways to go and permit the greedy driver a clear way to his/her goal [5]. 2. Sybil nodes may inject fake information in a straight way or indirectly into the systems, highly affecting on the information consistency of the framework. For instance, VANETs may depend on different vehicles casting a vote to create an activity status report. If a portion of the voters are Sybil vehicles, the report might be deviated from the reality. Sybil attack can confuse the network or loot the identity of the remaining nodes in many ways.

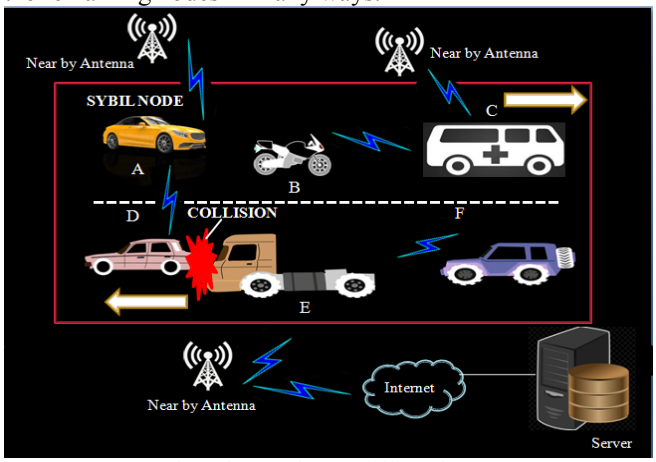

Fig 2: damage due to Sybil attack

Here Node A is a Sybil node and sending fake information to the other nodes. Due to misguidance collision is done between Node E and D, similarly other vehicles also have wrong information. Because of this fake information huge loss will happened. To overcome these issues, we need to detect the malicious node and we have to block it. Here we are proposing two strategies to identify and block the Sybil attack. One is used to detect the malicious node at the time of routing and another approach is used at receiver side installed in vehicle and rechecks the node. This merged method helps to detect and block the attacked node with high accuracy and best results compared with existing proposals.

II." LITERATURE SURVEY

To have secure communication it is essential to remove the Sybil nodes from the network [1].To provide secure VANET, many researchers researched on group solutions to solve different safety and security problems which can be mentioned in this segment. Chauhan and Mahajan in [2] has proposed a way to compute the worldwide belief of the target node depending on its neighbor's advices and their trust levels.Isaac, J.T.; Zeadally, S.; Camara, J.S. In [4] overviews the essential security attacks and shows the relating counter measures and cryptographic solutions. To shield a vehicular system against Sybil attacks, researchers B. Liu, B. Khorashadi, H. Du, D. Ghosal, C-N. Chuah and M. Zhang in [3] proposed a solution includes the use of on-road radar, wherein each vehicle can see nearby vehicles and obtain reports in their GPS arranges. By method for assessing what's seen to what has been heard, a vehicle can prove the genuine position of companions and separate malicious nodes.

Chowdhury, P.; Tornatore, M.; Sarkar, S.; Mukherjee, B., Wagan, A.A.; Mughal, B.M.; Hasbullah, H. in [5] proposed a hybrid approach that takes advantage of both unbalanced and symmetric cryptographic schemes. The methodology utilizes equipment that incorporates each uneven and symmetric cryptography modules for safety messages. A protocol for message checking is suggested by Wang, J., Yan, W in [9] this convention incorporates checking the authentication Validity (CV) of the sender, the beneficiary of the message evaluations the CV of the message sender, the after effect of checking has three cases: inside the principal case, the recipient will keep in mind the message if the sender has a legitimate declaration, second case happens when the sender has an invalid endorsement, in this circumstance the receiver will never again respect the message, inside the third case, the sender has no CV by any stretch of the imagination, the recipient will tell the RSU with the sender and investigate the acquired message, on the off chance that it is right the RSU will issue CV for the sender, in some other case it's going to issue invalid testaments and report vehicle's character into the testament Revocation list (CRL). Yong Hao, Yu Cheng, and Kui Ren in [6] proposed an answer of gathering solution combined with RSU is shown, which brought about smooth denial of a malicious node, put privacy protection is progressed and the framework safeguarding moves toward becoming flexible. Jinyuan sun; Chi Zhang; Yanchao Zhang; Yuguang Fang in [10] proposes a identity based security machine for VANET to illuminate the contentions among protection and tractability effectively. The machine utilizes a pseudonym based plan to preserve user privacy. It utilizes a threshold

signature based plan to permit tractability for law requirement. That is particularly attractive to service providers given that they can accomplish higher productivity of their contributions. In [11] and [12], the suggested solution decides Sybil attacks while vehicles may keep only one moderate nickname at a time. At the point when a nickname needs to be looked into, from a authorized Road-Side Unit (RSU). The advantage of this methodology is a feasible complex alias strategy performed by the roadside unit arrange. Other mechanism to determine directional antennas to select the direction or position of message arrival [14]. A vehicle initiating a Sybil attack will likely be resolved as a several messages will reach from the direction or position. Since, in heavy networks, localization liable can cause to quick false positives. This methodology might be balanced as a smart attacker may use directional antennas to mislead its neighboring vehicles around its way. In [13], Heavy weight cryptographic systems are employed for making sense of Sybil attacks in VANETs. In particular, each vehicle is given a posting of nicknames secure their privacy on the time of the discussion.

Douceur presented the Sybil attack in a distributed network in 2002. In (Douceur 2002)[15], one of the possible answers for preventing this attack is proposed in a way that each one physical substances must be prepared with a constrained computational asset, data transmission, and capacity; accordingly, those obstructions are counter acting Sybil node to lunch any attack as the recreating in excess of one characters calls for more computational asset than normal. A previously mentioned solution may furthermore proper for companion to see a network, be that as it may, specially appointed systems have admission to higher assets than distributed systems. Each and every other downside of utilizing bound resources is the chance of making network congestion in examples while the wide assortment of request or reply to a node is expanded. One efficient system to safeguard a network is to utilize Cryptographic-based techniques which increase the reliability of receiving position and identities requested by vehicles. Digital signatures are talked about in Armknecht, Festag et al. 2007[17]. Beside numerous advantages of utilizing cryptography, a barrier on the road to apply it is that because of the kind of models and maker of engines, it needs a major effort to setup a worldwide cryptographic strategy. G. Samara, and W. Al-Salihy in [16] proposed utilizing of Vehicular Public Key Infrastructure (VPKI), every node sends a security message, it signs that message with its private key and appends it with Certificate Authority (CA). The beneficiary party of the message will get general public key of the sending party by means of utilizing the declaration, and check the mark of that sender, the utilization of its certified public key, however this solution necessitates that the CA public key be known by receiver party. Azogu, I.K.; Ferreira, M.T.; Hong Liu in [18] proposes an Asymmetric Profit Loss Markov (APLM) model to measures the uprightness dimension of the security plans for VANET content material transport. The model makes utilization of Markov chains to document the device's ability to modify itself given benefit and misfortune. Given the estimation through the variant as heuristics, respectability plans for VANET might be upgraded to give better substance material delivery.

Reddy et al., Safer transportation manner saving lives because many car injuries have precipitated splendid casualties. Session key certificates(SKC) for detecting the malicious nodes multiple identities that triggered Sybil attacks in VANETs were proposed(2017)[22].Yao et al. in(2017)[21]proposed a new detection scheme for Sybil assault the use of voiceprint and RSSI. To sidestep of the incorrect location estimation base on the threshold radio propagation reproductions in traditional RSSI detection systems, voiceprint uses the time series RSSI as vehicular speech and matches the likeness with received time collection. Researchers in [7], [8] worked on routing protocols and gave powerful answers all together that the communication between the nodes is computationally viable and principle to significantly less congestion of network traffic. G Jaideep et al. (2018)[19] proposed a techniques for detecting DDoS attacks which is similar to Sybil attack. R V Kishore Kumar et al. (2018)[20] made a study on wireless sensor networks.

The proposed scheme of Rawat et al. [24] proven a resilient overall performance in transmission overhead and delay computations without relying on the variety of messages in sincere cars to save you impersonated automobiles from their privateness and stealing of private data. This preserved VANET records from the incidence of identity falsification to improve overall network performance. Schweitzer et al. in [23] proposed a median to detect the Sybil assault. Each node attack is being detected independently without an assist from VANET infrastructures; however , this scheme tremendously relied on the collaboration among neighboring node to carry out effectively Sybil detection within the network.

III." PROPOSED STRATEGY

When there is more number of nodes attack is much possible and easy to the intruder to perform attack. Public key is assigned to every registered node and based on this we can identify the node is genuine or not, but attack can happen at any time. Here we use key management technique to identify attacked node at the time of routing using (Public Key Infrastructure) PKI. There If the node has its unique public and private keys it is considered as genuine node or else attacked node and rejects the node. As a merged mechanism node is examined twice. One at routing time and another test is done by the application which is installed in the device.

3.1 Key Management

Beacons have accurate information about motors velocities, positions, and accelerations. They normally present warnings about unstable conditions, which includes emergency braking and lifestyles-threatening avenue situations. In case these warnings are dispatched in absence of a unsafe scenario, they themselves might also come to be a protection breach. This may show up when an attacker sends such fake packets or when device starts off evolved to malfunction. Those users and systems need to be removed from the Network for minimizing the harm caused by them. To overcome this, the safety infrastructure needs to be applied very cleverly. Its

fundamental purpose is to offer key management in this kind of manner that those harm-inflicting entities are eliminated. The OBUs in automobiles and nearby antenna's want to be prepared with keys for performing cryptographic duties for making sure integrity and non-repudiation.

Furthermore, automobiles want to benefit the keys of other vehicles inside the range securely and these keys must be resumed or withdraw in case the corresponding automobile misbehaves. Consequently, key control offers key mechanisms inclusive of certificates issuance, car registration, key distribution and renewal, and node revocation. A number of them are depicted in determine figure 3. For key management, the extensively universal approach is to enforce a PKI. It's far a machine that binds public keys to their respective identities through Key Distribution Centre. Public Key Infrastructure (PKI) assumes an essential job in giving security services like confidentiality, digital signatures, integrity, and authentication. It has the property that given an encryption key, it is infeasible to register the unscrambling key and the other way around. PKI has expanded security and accommodation when contrasted with other encryption techniques. It additionally has the property of non-disavowal where the client has the sole obligation regarding ensuring his or her private key. Clients who are generally spread over a huge zone can safely convey through a chain of trust utilizing PKI.

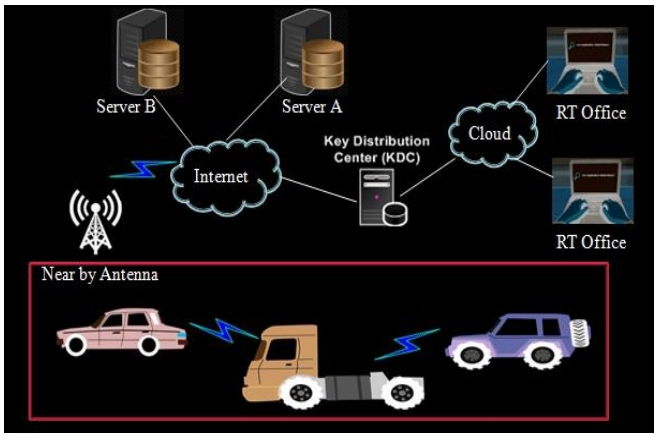

Fig 3: Key Management System

Public Key Infrastructure (PKI)

A PKI is a union of hardware and software program products, regulations and methods. It gives the protection required for secure communications unknown users or widely spread users, Public key cryptography, in comparison, uses pairs of keys: a public key that is extensive to be had, and a different private key recognized only to the individual, software or service that owns the keys. The general public key can be transmitted unencrypted over insecure lines, because it is not a secret, at the same time as the personal key need to be stored secret. As a result, key distribution has dramatically simplified the usage of public key cryptography. Public key cryptography can be used for relaxed distribution of shared secret keys throughout insecure networks. In each of these programs, access to the general public key in no way offers intruder get right of entry to protected data.

3.2 Steps for certificate verification

1. Fetch the vehicle's sub-CA certificate in case it is not registered with the same sub-CA of the looking up node. In case if it is registered, step 3 is executed.
2. Authenticate the sub-CA certificate by taking the help of the root certificate.
3. Validate the vehicle's certificate through the sub-CA certificate.
4. Verify messages of that vehicle by utilizing its public key

3.3 Second Proposed Technique

Versatility of nodes and absence of central monitoring or node approval device results in Sybil attacking intrudes in the system for the most part. Proposed mechanism can be explained as

A. Hash Function Mechanism

Cryptographic hash functions are commonly used in lots of distinctive areas of cryptography: in virtual signatures and in public-key cryptography, for password safety and message authentication, key derivation functions so forth. These days, cryptographic hash features have obtained a massive quantity of attention because of new attacks on broadly used hash capabilities. Properties of the cryptographic hash function are computationally efficient, Collision Resistant, Deterministic, Pre-image Resistant.

Identifying Sybil attack can be done by Hash function mechanism. Intruder utilizes different identities for gaining extra data, assets and access in the system in Sybil attack. We can explain the proposed hash work system as arrival of Nodes from the Network:

1. According to the proposed plan, every individual hub is dependent on Hash work figures and Hash of its MAC address. Correspondence nodes send message that incorporate its determined hash key of MAC address. The target hub gets message from neighbor and discovers hash in it. If the message contains Hash alongside it, it stores the Hash for that neighbor as its personality but if the message is without Hash, the message is disposed off and the node is rejected.
2. If the node has hash function and if it matches with the registered hash node is accepted, if hash value is not matched node gets reject.
3. Here we are placing counter and assigns a threshold value, and counter value increments every time when a message arrives from same node and if the increment counter reaches threshold value node is considered as suspect and moves to suspect list, If increment counter does not reach threshold value node is accepted to receive the data.
4. We assigns a threshold value to the suspect list When the node is in suspect list and still messages comes from same node continuously , and node detection counter is compared with threshold value and if suspect node reaches the threshold value without no doubt node is blocked.

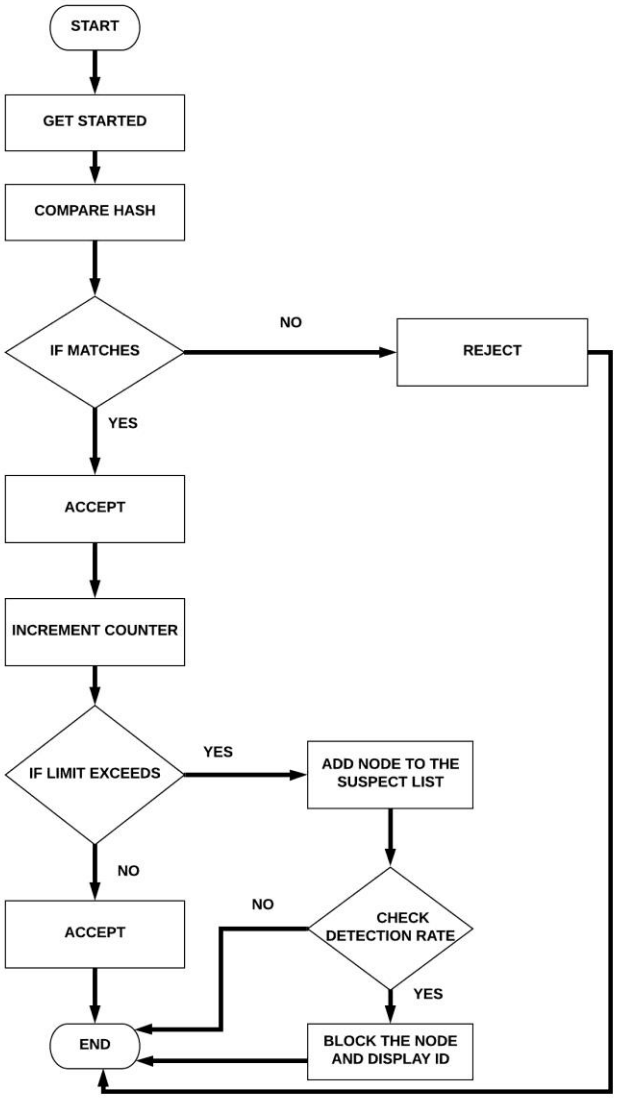

Fig 4: Flow Chart for hash Function Mechanism

5. If the suspected node stops sending messages continuously and does not reach detection rate threshold value node is accepted to transfer data.

IV. RESULTS

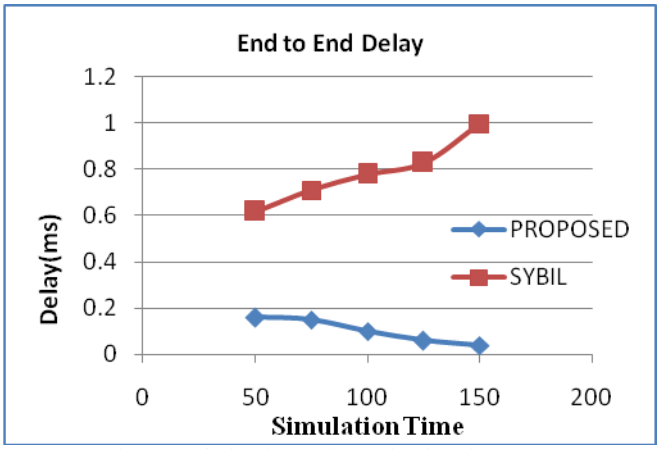

Fig 5: Graph showing End to End Delay Time

One-way delay or End-to-end delay gives the information about the travel time taken by the packet to move across a network from sender to receiver. From the figure 5, we can demonstrates that with the expansion in simulation time, the END-to-END or ONE-WAY delay time is decreasing when the Merged method is working, whereas the END-to-END or ONE-WAY delay time increasing when there is no merged method to block a Sybil attack. Even though there is a SYBIL Attack in the transmission of data between source and destination the end-to-end delay for simulation time of 50ms is 0.18ms in proposed method, where as the end-to-end delay is 0.61ms.

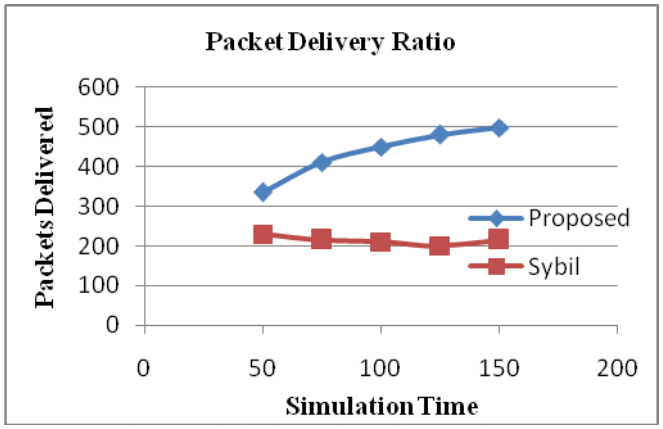

Fig 6: Graph showing Packet Delivery Ratio

The number of packets that are effectively delivered to a target node compared with the number of packets that have been sent by the sender. From the figure 6, we can demonstrates that with the expansion in simulation time, the packet delivery ratio increasing when the Merged method is working, whereas the packet delivery ratio decreasing when there is no merged method to block a Sybil attack. In proposed merged technique the number of packets delivered between the end points is 325 for a simulation time of 50ms, whereas in SYBIL Attack number of packets delivered is 220.

It is defined as the total number of packets delivered over the total simulation time. From the figure 7, we can demonstrates that with the expansion in simulation time, the throughput increasing when the Merged method is working, whereas the throughput decreasing when there is no merged method to block a Sybil attack. In simulation time of 50ms the throughput is 460 packets with proposed method, whereas in SYBIL Attack system the throughput is 340.

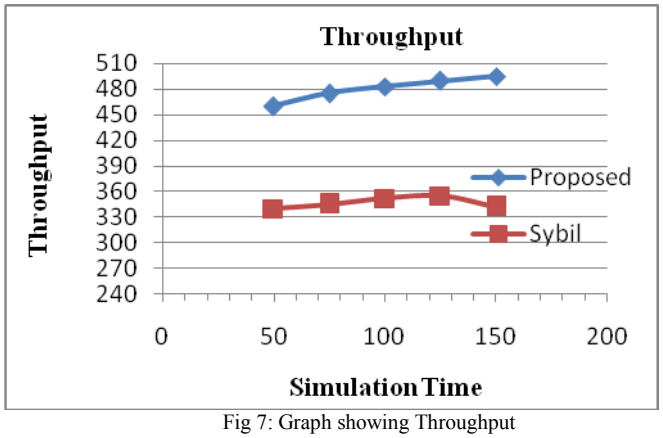

Fig 7: Graph showing Throughput

V." CONCLUSION

In this paper, we have talked about detection and prevention strategies against Sybil assault in VANETs. According to the studies in this area, each method has some pros and cons for implementing. Resource testing strategies are not adequate to execute for Sybil assault discovery with high precision in VANETs. Verification techniques are increasingly solid and helpful for message trustworthiness, credibility and security and there are appropriate techniques in this classification for useful execution in urban zones. Merging the two methods had given a great result and prevents the data and fake information from the attackers. Still there is much research need to be done for future.

REFERENCES

[1]Adnan Nadeem and Michael P. Howarth,``A survey of MANET IntrusionDetection & Prevention Approaches for Network layer Attacks," *IEEE Communication Surveys & Tutorials*, pp.1-19, 2012.

[2] Amit Chauhan, R.P. Mahajan. "A Novel Approach for Securing Mobile Ad Hoc Network with an Enhanced Trust Calculation Method", In *International journal of Computer Technology & Applications*, 3(2) 2012, pp. 682-690.

[3] B. Liu, B. Khorashadi, H. Du, D. Ghosal, C-N.Chuah and M. Zhang, "VGSim: An Integrated Networking and Microscopic Vehicular Mobility Simulation Platform", *IEEE Communication Magazine Automotive Networking Series*, vol. 47, no. 5, (2009) May, pp. 134-141.

[4] J. T. Isaac, S. Zeadally and J. S. Camara, "Security attacks and solutions for vehicular ad hoc networks", *Communications, IET*, vol. 4, no. 7, (2010) April 30, pp. 894, 903

[5] P. Chowdhury, M. Tornatore, S. Sarkar, B. Mukherjee, A. A. Wagan, B. M. Mughal and H. Hasbullah, "VANET Security Framework for Trusted Grouping Using TPM Hardware", *Second International Conference on Communication Software and Networks*, (ICCSN '10), (2010) February, pp. 309-312.

[6] Y. Hao, Y. Cheng and K. Ren "Distributed Key Management with Protection Against RSU Compromise in Group Signature Based VANETs", *IEEE GLOBECOM*- 2008, pp. 4951-4955.

[7] J. Yin, T. El. Batt, G. Yeung and B. Ryu, "Performance Evaluation of Safety Applications over DSRC Vehicular Ad Hoc Networks", Proceeding of the *1st ACM International Workshop on Vehicular Ad Hoc Networks*, (2004), pp. 1-9.

[8] Rajinder Kaur, Dr. ShasiB.Rana , "Overview on Routing Protocols in VANET", in *IRJET*,2015.p 1333-1337.

[9] J. Wang and W. Yan, "RBM: A role based mobility model for VANET", *Proc. Int. Conf. Communications and Mobile Computing*, vol. 2, (2009) January, pp. 437-443.

[10] J. Sun, C. Zhang, Y. Zhang and Y. Fang, "An Identity Based Security System for User Privacy in Vehicular Ad Hoc Networks", *IEEE Transactions on, Parallel and Distributed Systems*, vol. 21, no. 9, **(2010)** September, pp. 1227-1239.

[11] Sun Xi; Xia-Miao Li, "Study of the Feasibility of VANET and its Routing Protocols," *Wireless communication, Networking and MobileComputing, 2008.WiCOM '08. 4th International Conference,*pp12-14 Oct. 2008.

[12] Harri, J.; Filali, F.; Bonnet, C., "Mobility Models for vehicular ad hoc networks: a survey and taxonomy," *Communications Surveys &TutorialsIEEE*, vol.11, no.4, pp.19,41, Fourth Quarter 2009.

[13] Samara, Wafaa A.H. Al-Salihy, R.sures, "Ghassan*Security Analysis of vehicular Ad hoc Networks"2010 International Conference on Network Applications,Protocols and Services.*

[14] SheraliZeadally, Ray Hunt, Yuh-ShyanChen,Angela Irwin, Aamir Hassan," *Vehicular Ad hoc Networks(VANET):Status, Results, Challenges*".Springer Science, Business Media.2010.

[15] Douceur, J. R. (2002). The Sybil attack. Peer-to-peer Systems, Springer: 251-260.

[16] G. Samara and W. Al-Salihy, "A new security mechanism for vehicular communication networks", Proceeding of the *International Conference on Cyber Security, Cyber Warfare and Digital Forensic,2012.*

[17] Armknecht, F., et al. (2007). Cross-layer privacy enhancement and non-repudiation in vehicular communication.Communication in Distributed Systems (KiVS), 2007 *ITG-GI Conference, VDE*. (CyberSec), (2012), pp. 18-22.

[18] I. K. Azogu, M. T. Ferreira and H. Liu, "A security metric for VANET content delivery", *Global Communications Conference (GLOBECOM)*, no. 37, (2012) December, pp. 991, 996.

[19] Gera Jaideep, Dr. B.BhanuPrakash,"Detection of spoofed and non-spoofedDDoS attacksand discriminating them fromflash crowds", in *EURASIP Journal on Information Security*,2018,PP1-12.

[20] R V Kishore Kumar, Dr.GMurali, "A Study on Explosive Detection Utilizing Wireless Sensor Networks",JARDCS, 2018, pp 464-471.

[21] Y. Yao, B. Xiao, G. Wu, X. Liu, Z. Yu, K. Zhang and X. Zhou,"Voiceprint: A novel Sybil attack detection method based on RSSI for VANETs," in Proc. IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), pp. 591.

[22]D. S. Reddy, V. Bapuji, A. Govardhan and S. V. N. Sarma, "Sybil attack detection technique using session key certificate invehicular ad hoc networks," in Proc. IEEE InternationalConference on Algorithms, Methodology, Models andApplications in Emerging Technologies (ICAMMAET), pp. 1-5,2017.

[23] N. Schweitzer, A. Stulman, R. D. Margalit, and A. Shabtai, "Contradiction based Gray-Hole attack minimization for Ad-Hoc Networks," IEEE Transactions on Mobile Computing, vol. 16, no. 8, pp. 2174 – 2183, 2017.

[24] D. B. Rawat, B. B. Bista, and G. Yan, "Securing vehicular ad-hoc networks from data falsification attacks," in Proc. IEEE Region 10 Conference (TENCON), pp. 99-102, 2016.