International Journal of Research in Computer Science
eISSN 2249-8265 Volume 5 Issue 2 (2015) pp. 7-17
www.ijorcs.org, A Unit of White Globe Publications

A COMPARATIVE ANALYSIS OF SYBIL ATTACKS ON VANET

[1]Rohika Bhatt, [2]Parveen Thakur

[1]*M.Tech, CSE Department, Baddi University of Emerging Sciences and Technology, Solan, INDIA*
[2]*Assistant Professor, CSE Department, Baddi of University Emerging Sciences and Technology, Solan, INDIA*
[1]*Email: rohikaverma1984@gmail.com*
[2]*Email: parveen.thakur@baddiuniv.ac.in*

Abstract: *In this research work a sincere attempt is made to review the problem of attacks in VANET domain since, network security in VANETs is of immensely challenging. The distributed nature of VANET allows each of the vehicle nodes to function both as a host as well as router to remain connected with other nodes. As nodes very frequently move in and out of the range of each other, consequently network topology also changes frequently compromising the security of the network. And it is prone to lot security gaps. This paper discusses the type of attacks and their possible solutions for mitigating the attack in context of Sybil attack. An alternative method after systematic review of the proposed in this research work shows that anonymity factor can be increased and sequence mining can detect the Sybil attack with low computational overhead and low false rate.*

Keywords: *vanet, sybil attacks, passve attacks, RSU, intrusion detection*

I. INTRODUCTION

Today is world of connected objects including watches, `cameras [5], automobiles [6] and even medical equipment [7] ? The connected entities are essential for the growth and progress of mankind. Vehicular ad-hoc network (VANET) [1] comprises of vehicles (nodes), road side units (RSUs) [2], and certification authorities (CAs) [3]. VANET is a specific type of MANET [8] that can also be classified as ephemeral network, because of frequent migration of nodes due to mobility. VANET essentially provides communication between:

1. Vehicle to Vehicle
2. Vehicle to Road Side Units (RSUs)

VANET represent one of the ways to implement Intelligent Transport System (ITS), a technique based upon IEEE 802.11p standard for Wireless Access for Vehicular Environment (WAVE) for imparting information and communication technology to transport infrastructure and vehicles. These networks are characterized by no fixed infrastructure, relying solely on them self for implementing network connectivity. The decentralized nature of VANET allows each of the nodes to function both as a host as well as router. As nodes very frequently move in and out of the range of each other, consequently network topology also changes frequently. The density of the network will also change with change in traffic density. These characteristics make network security in VANET very challenging. Security issues ranging from sensor data protection [9], secure communication [10], tamperproof hard [11] and software, security affects all part of the system.

There is high possibility of many kinds of attacks on VANETs. It is therefore of utmost importance that VANET security should be capable of handling every type of attack. VANET security is different from wireless and wired networks because of its unique characteristics of mobility constraints, infrastructure less framework and short duration of link between nodes. Before designing any security solution for VANETs, we need to know various types of security issues, their capabilities and the type of attackers. In rest of the paper Section 2 deals with the type of attackers, Section 3 explains different types of attacks and Section 4 specifically provides an insight and problem scope of detecting Sybil attacks, while Section – 5 Introduces to novel method of detecting Sybil attack.

Attackers create problems in the network by getting access to the communication medium. Attackers can be categorized according to scope, nature, and behavior of attacks as follows: [3, 4].

1. Passive Attackers [12] - They do not participate in the communication process, but only eavesdrop to gather information from the network. This information then may be shared with other attackers. Since these attackers do not participate in

the communication process they are called as passive attackers.

2. Active Attackers [13] – Some attackers on the other hand may disrupt the communication process by either loading packets containing wrong information into the network or by deleting the authentic packets form the network. These are called as active attackers and can further be classified into three types:
   a. Insiders [14] – These are authentic users of the network with authentic public keys and access to other members of the network.
   b. Outsiders - Outsider attackers are intruders and can launch attacks of less diversity.
   c. Malicious – These attackers are not personally benefitted from the attack, their intention is to harm other members of the network or disturb the functionality of the VANET.

Based upon the area targeted, the attacker may be classified as local or global. Local attacker launches an attack with limited scope, an attack is restricted to a particular area. However, Table 1 below shows the ways in which a Sybil attack can happen in context of VANET.

Table 1: Sybil Attack Methods

S.NO	Sybil Attack Method	Description
1	Using Fake Identity to do Sybil attack	In this method the attacker uses large number of pseudonymous identities for getting large influence in the VANET.
2	Using Identity Theft to do Sybil attack	For Getting access into the network, the attackers may use credentials stolen from existing source to become part of the network and do the malicious act
3	Conspired Sybil Attack, sock puppets	A sock puppet is an identity used for purposes of deception by portraying conversations that seems to useful but have malicious intent. In this the Sybil attackers victims stake holders to again access to the network.
4	Message Integrity Compromise	Integrity of the message/data means that it has not been altered in any way. By way of deletion or addition, frame deletion or addition, or replay attacks.In this attack process the messages send from one vehicle to another vehicle node is comprised to launch attack.
5	Insider Attacker	In this case, there is some entity within the network, that has malicious intent and due to inside knowledge of the system the detection is not easy and he/she is successful in influencing the network services with negative impact.

Typically, it is clear from the above table that a malicious user may create many identities to act as source node and spread their wrong actions. There is always a need for a system that provides the security while transferring message from source to destination to maintaining confidentiality of commination resources and media. Following are the description methods with which such systems that help in detection Sybil attack may be used.

Table 2: Sybil Attack Detection Methods

S.NO	Sybil Detection Method	Description	Merits	Demerits
1	Statistical Analysis [14] [18]	It is method in which data can explained, described & summarized and conclusions can be drawn	The main advantage is predictive analytics to anticipate future problems in network	It may have large sampling error, constructs of validity may not be good. Even if high correlation is found in factors, some time it does not prove that it is cause of this the attack occurred.
2	Data Mining [23]	It is way of discovering insights & knowledge for dataset which can help identify sybil attack	Can work with variables which do not even have correlation	Large Data sets over head.

3	Data Stream Analysis [23]	It is the process of extracting knowledge structures from continuous, rapid data records in real time frame.	Get Response in Real time before sybil attack may bring more adversity and can work on Incremental heuristic search	Large Data sets overhead, Limited offline analysis.
4	Machine Learning [17]	The difference in this case is NOT in the techniques of data mining or machine learning but in what to do with the results, in case of machine learning we want patterns of datasets to represent normal and abnormal states to reach at some decision.	Works without explicit programming approach for detection of Sybil attack.	Not easy to work with unstructured large data in which unknown patterns are hidden.
5	Probability Based Method [21] [22]	It deals with problem that concerns both detecting whether or not a change has occurred, or whether several changes might have occurred, and identifying the times of any such changes which may help in detecting the Sybil attack.	Used when there isn't an exhaustive population list available in real time for taking decision on Sybil attack.	More expensive and time-consuming over head
6	Sequence Mining [16]	Helps to find most frequent or infrequent patterns of activities	Can be used for Repeat-related problems	Over head of large dataset in terms of memory and retrieval /response time
7	Ranking {Trust, Reputation Voting } [15] [19]	In this method Trust points are given based on some algorithm, which helps to detection malicious nodes	Machine to machine voting system and man to machine voting systems of trust can be build	A Compromised network will lead to failure of the trust system.
8	Thresholding [20]	In this dynamic thresholding algorithm with heuristics evaluation can be used for detection of Sybil attack	Simple to implement	Wrong calculation of thresholds due to large variability may lead to numerical stability problem of algorithm.

Intrusion and detection systems may be from one of the methods mentioned above, However, these Systems may be also characterized based on the way are storing their data or the place where there computational intensive algorithms are running from. Following table illustrates on this aspect.

Table 3: Types of Intrusion Detection Systems

S.NO	Types of Intrusion Detection Systems	Description
1	Central	In this system, all the nodes are communicating with the central server /node directly
2	Distributed	In this system, there is no client –server concept, but multiple location of detection /analysis of the data for multiple end point of the network.
3	N –Tier	In this, there are large networks and sub networks having n-tiers coordinating with each other for detecting and periodically synchronize with each other for better response to adversity.

II. LITERATURE SURVEY

TPB is widely used in social psychology and marketing research to predict and understand human behavioral intention and then behavior [22]. It's an extension of TRA [2]. TPB proposes that actual usage behavior is determined by behavioral intention and perceived behavioral control. Behavioral intention is

determined by three factors: attitude, subjective norms and perceived behavioral control. Each factor is in turn generated by a number of beliefs and evaluations [16], [18] (see Fig.1)

"VANET : Security and its possible solutions" by Ajay Rawat et al. [23], demonstrated that VANET is a subset of MANET and for its applications it requires wireless medium which makes them vulnerable to several attacks. Security is the important concern in VANET. In their paper they gave comprehensive study of several attacks and their solutions.

"Vehicular Behaviour Analysis to Enhance. Security in VANET's" by Robert K. Schmidt, et al. [24] proposed a framework for behaviour analysis of other vehicles. In their system they combined the output of multiple behaviour analysis modules, each vehicle is assigned a trust worthiness value which may be additionally exchanged, among all vehicles, building up reputation. They classified vehicles into three categories trustworthy, untrustworthy or neutral. Application take trust rating into consideration and react to incoming information.

"Privacy Aware VANET security: Putting Data Centric Misbehavior and Sybil Attack Detection Schemes into Practice" by Rasheed Hussain, et. al. [25], witnessed that malicious users inject false information and launch several attacks change their behavior to misbehavior. They proposed two strategies to avoid misbehavior in VANET, i.e centric strategy and other Data centric approach.

"Data centric Misbehaviour detection in VANET's" by Sushmita Ruj et. Al [26], proposed that it is important to detect false information than to identify misbehaving nodes. In their paper they introduced the concept of data centric misbehavior detection and proposed algorithms which detect false messages and misbehaving nodes by observing their actions. In this system each node independently decide behavior whether information received is correct or false.

In signature based Rule Matching Technique in Network Intrusion Detection System" by Chauhan et al. [27], demonstrated that signature is the pattern that is inside the data packet-usually, IDS depends upon signatures to find out intruder activity. Pattern matching is time critical operation of IDS, Pattern of known attack is stored in database of IDS.

III. PROBLEM SCOPE

After conducting this systematic survey, it was found that one of the main reason by which a Sybil may become successful depends on the number of malicious identities present in the network, and another factor that may be level of anonymity of the various components with in the VANET.It was is also clear that malicious intent communication will has come abnormal sequence of events as compared to the routine event sequence. Other than these events information stored in trace files /database need to scanned again and again, the refreshes of data analysis is also one factor which need to addressed. Moreover, some methods that rely on the thresholding methods run the problem of not been numerical stable for their calculation of infection points, from where one can identify abnormal behavior from normal behaviors of nodes, especially when anonymity of the nodes is low and there is latency in detection and altering the system for some adversity. There is need for overcoming all these kindly of issues using a algorithm that is stable for calculating the thresholds and also takes cares of the event sequences occurring in the VANET. Based on this problem, the final scope and objectives of this research work must considered as follows:

1. Develop a numerical stable thresholding algorithm based on robust statistics method like IQR for Threshold calculations.
2. Using Sequence mining detect Sybil attack foot prints.
3. Compare the work with state of the art [20].

IV. IMPLEMENTATION

In this section of the paper, we will be delineated the working of proposed work which likewise endeavors to overcome the limitations of the past work done around there. The execution of the proposed thesis work is portrayed in the accompanying flow diagram shown below:

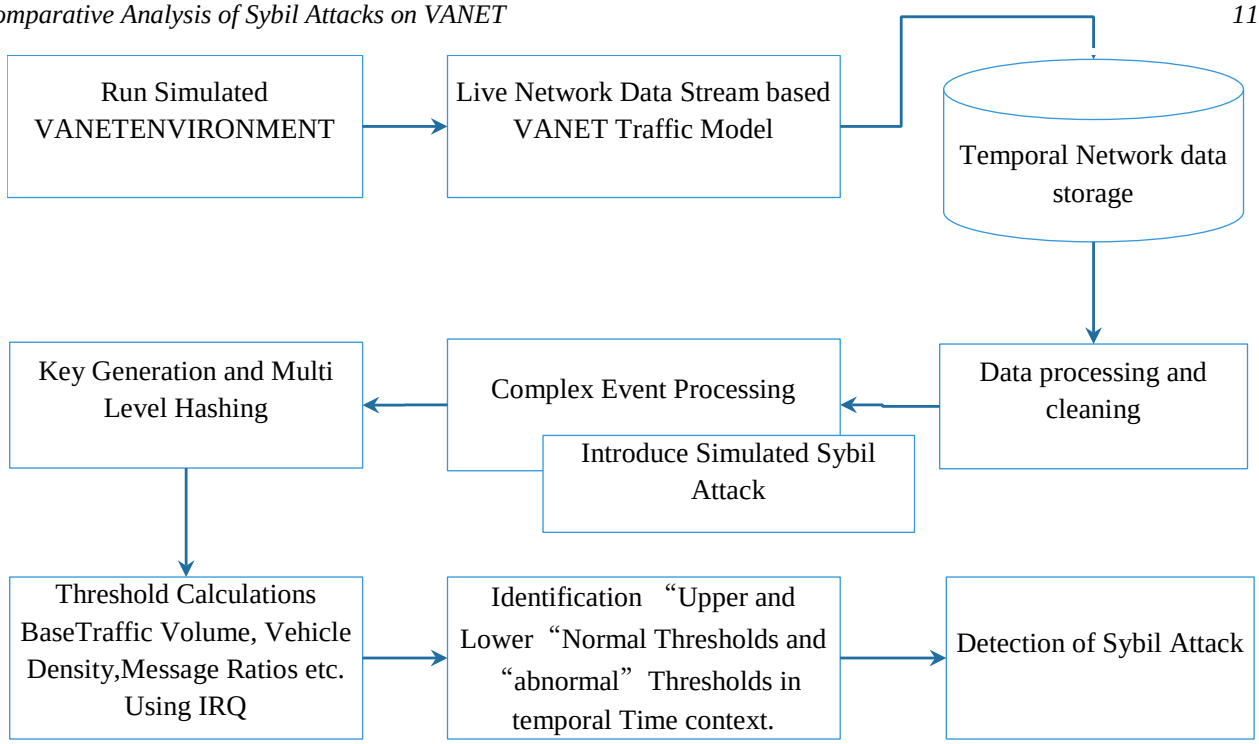

Figure 1: Basic Flow of the work

As illustrated in the Figure 1, the first step in developing this research work is to build a simulated test bed for building the algorithm. Other steps includes as follows :

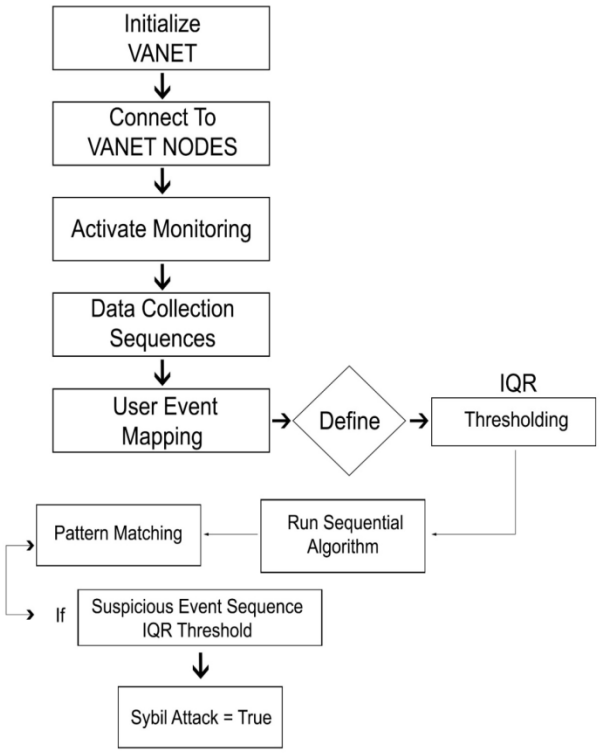

Figure 2: Flow of the Proposed Detection System

A. Explanation of the Implementations Steps :

Implementation of VANET Environment and Services for Vehicle Users Ids :

1. **Creation of VANET:** It is entity which sends communication data to the Road Side Units and Data Centre for Sybil attack analysis.
2. **Creation of Road Side Unit:** A Road Side Unit (RSU), is the operational Centre having physical machines which send and receive data from the vehicles for running routine operations of the VANET network.
3. **Intrusion Detection Component (IDC):** This piece of technology basically implements the proposed algorithm, which systematically discards the older values with respect to the decay parameter. Thus the data remains fresh and size is reduced, it been part of Monitoring Unit (MU) run need to identify the point (Threshold) where it must declare, which sequence of events show foot prints of Sybil attack. Figure 3, shows how the event information is stored by the RSU and is send to IDC using coding associated with particular event.

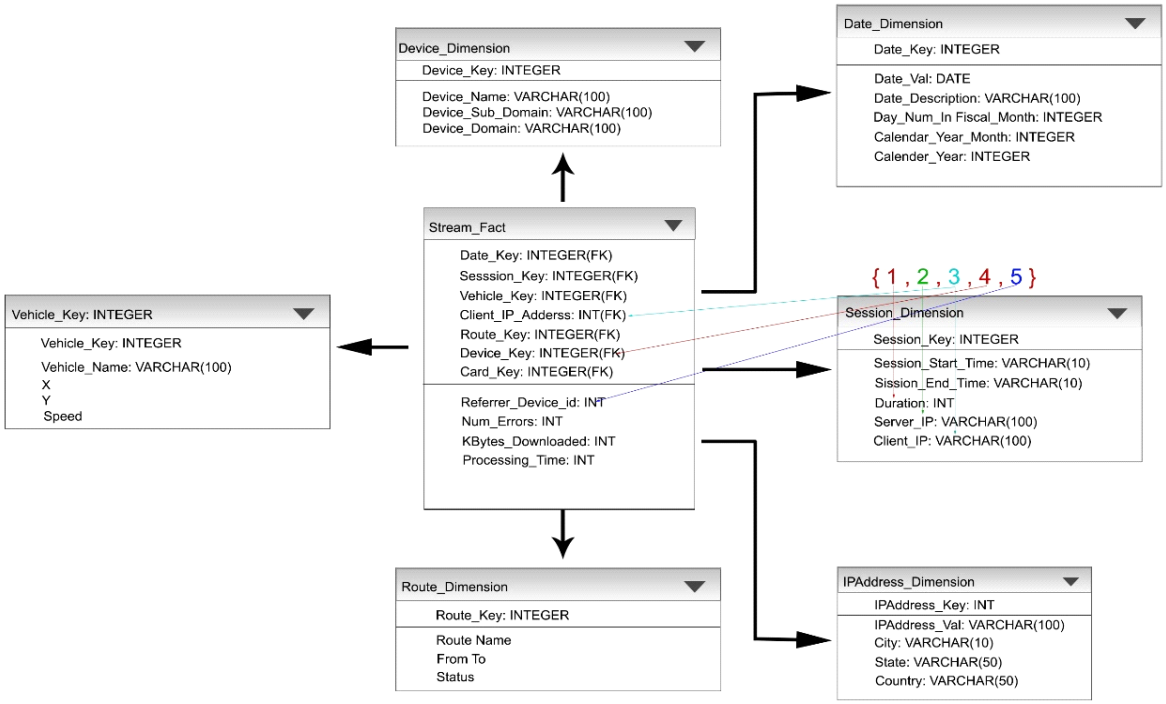

Figure 3: Scheme for Capturing Sequence Data for Detecting Sybil attack Activities

Working of IDC: IDC is essentially a java based soft component that has following sub–parts:

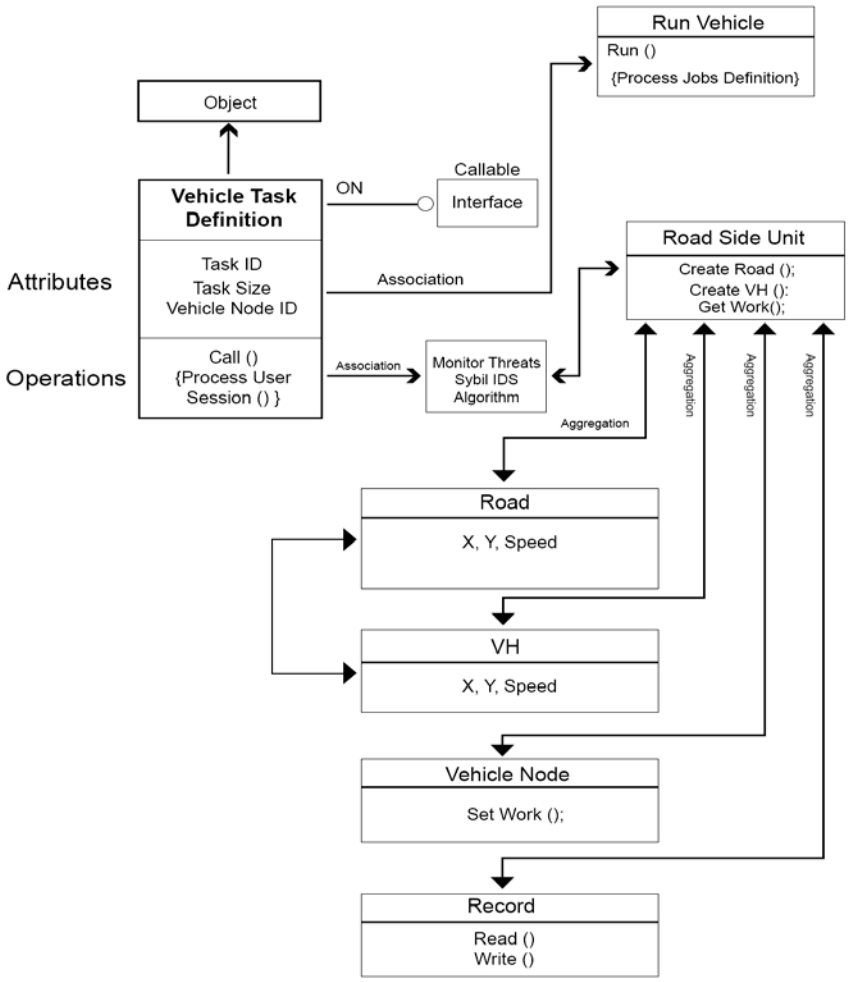

Figure 4: Class Diagram of VANET based Intrusion Detection System developed in Java [3]

In our current context finding "normal "and "abnormal "limits or thresholds (IQR method based) is considered the based for detecting Sybil attack, therefore an "abnormal value " in a distribution of Traffic Statistics, Traffic Density Statistics is a number that is more than 1.5 times the length of the box away from either the lower or upper quartiles. Specifically, if a number is less than Q1 - 1.5×IQR or greater than Q3 + 1.5×IQR, then it is "abnormal value of particular parameter. Following the explanation of above class diagram of make of monitoring system work for detecting Sybil attack issue.

• Vehicle Node Class: This is the basic unit of VANET network, the vehicles which have On board Units.

• Route Side Unit/Box Class: Vehicular communication systems are a type of network in which vehicles and roadside units are the communicating nodes, providing each other with information, such as safety warnings and traffic information. As a cooperative approach, vehicular communication systems can be more effective in avoiding accidents and traffic congestions than if each vehicle tries to solve these problems individually.

• Sybil Attack Monitoring Class. This is the class implementing the IQR and Sequence mining detection. There are several different methods for calculating quartiles. However, we has used the methods described by Moore and McCabe to find quartile values. The first quartile, also called lower quartile, is equal to the data at the 25th percentile of the data. The third quartile, also called upper quartile, is equal to the data at the 75th percentile of the data of parameter that helps in detection of the Sybil attack

• Record Class help to "record" or store the incoming data streams of activities of VANET.

V. RESULTS :

This section discusses the results obtained from the series of simulations done so far. However, let us first check the simulation parameters of work done.

Table 4: Simulation Parameters

S.No	Parameters	Dense Vehicles	Sparse Vehicles
1	Road Lane Length	2000	20,2000
2	Communication Radius	200	50
3	Road Lane Width	3	3
4	Vehicle Speed Rate (m/s)	25-30	25-30
5	Pseudonym(s)s per vehicle	20	20
6	Vehicle Packet Rate (pkt/s)	3	3
7	Total Simulation Time	400 Sec	800 Secs
8	Hash Function	SHA-1	SHA-I
9	Time Interval	20 sec	20 sec
10	Number of Attackers	7	7

A. Evaluation parameters :

1. **Over Head of RSU/B:** The Figure below shows the number of packets processed by an RSB. From the figure, obviously the number of packets received by an RSB increases with the increase in the number of attackers or the number of benign vehicles.

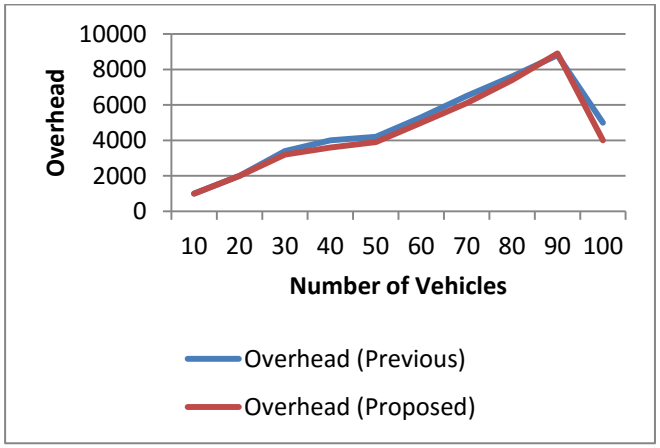

Figure 5: Overhead of RSU

2. **Anonymity of Vehicles:** This is a metric of privacy, it is necessary to have a framework allowing RSBs to detect a Sybil attack, without knowing the association between pseudonyms and unique vehicle IDs (i.e., without compromising privacy). The framework design needs to be scalable in terms of the workload it imposes on the DMV/MU [20], and needs to be robust against RSB compromise. Moreover, it is important to quickly detect the attack and perform subsequent punishments/revocations to minimize the impact of the attack. A benign vehicle can use only one pseudonym to sign one event. If a vehicle uses multiple pseudonyms to sign an event such can be traced by sequence mining algorithm proposed here in our work. After, a malicious vehicle is detected, the DMV/MU should revoke all its pseudonyms. Since, there are multiple vehicles reporting the same event, the action is considered to be a Sybil attack, and the vehicle is deemed to be malicious as per sequence of their activities.

Therefore, Anonymity is calculated based on following definition.

Given a set of vehicles {Vi}1≤i≤NV, a set of attribute values A and a one-way attribute function F : {Vi}→ A, the vehicle set is said to achieve N - anonymity if and only if for each attribute value a ∈ F ({Vi }), there are at least N occurrences of a in F ({Vi }), where NV is the number of vehicles. The details observations are shown below as table as well as graph.

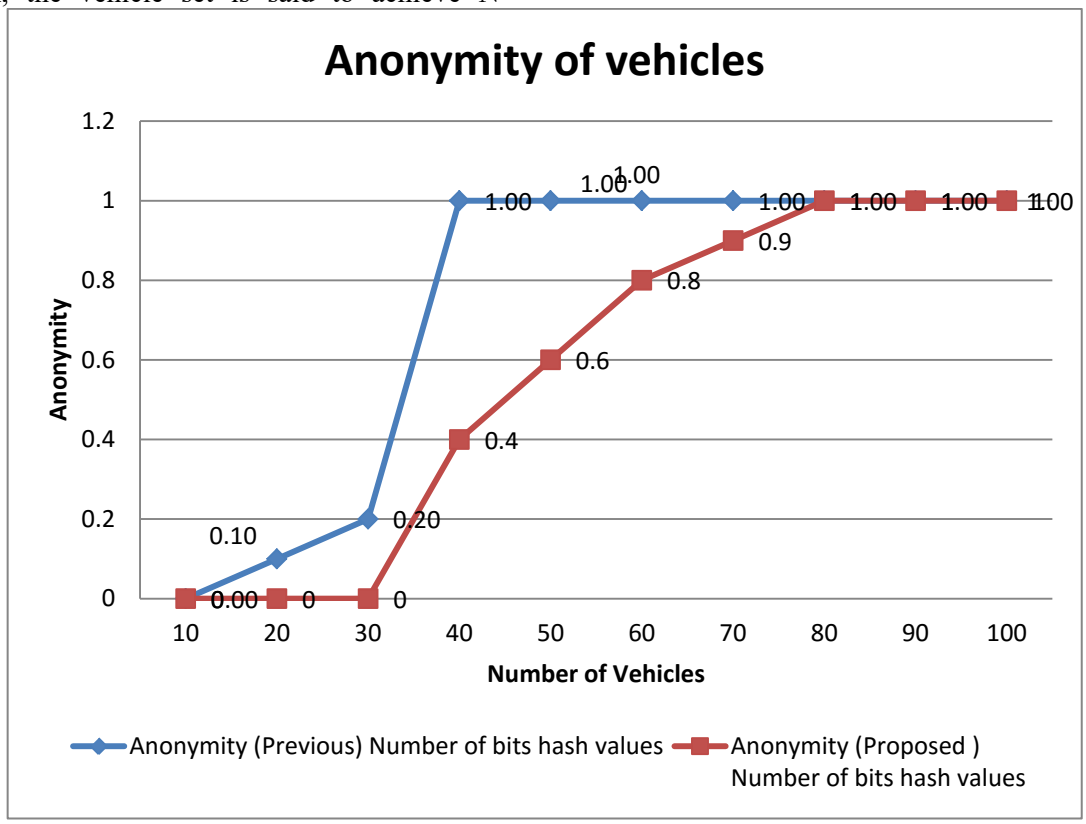

Figure 6: Anonymity of Vehicles

VI. DISCUSSION

Control the access. It's common sense that no employee should have the level of access necessary to nuke your entire VANET computing system. We need to make sure there are checks and balances in place and that sensitive information is accessible only to those who truly need it in order to be able to do their job properly. Our purpose algorithm is a low-cost, low-effort approach for resource-strapped companies to look for threats posed by malicious insiders. As in our current work a sequencing threshold rule algorithm is used in learning the behavior pattern of users, in order to build user/broker VANET base profiles. An pattern coordinating calculation were then used to match the chronicled conduct of the VANET users/client with the present conduct, so as to distinguish VANET clients that disguise in the framework as normal VANET users/clients. The results demonstrate that it was conceivable to recognize patterns and threshold for identification of the Sybil attack.

VII. CONCLUSION

It is clear from the above values that early detection of Sybil activities sequences leads generation of less number events related to creation, granting and revoking of the keys, more than this following can be considered as main conclusion and interpretation of the above graphs and work done.

It is known fact that, more is the traffic of message, more is the number of sequences of the activities occurring in network, more will be the need to scan and do various operations like generating public and private keys, distributing of keys and exchange of keys etc.., therefore, there is need to think over, the computational overhead involved. Average Number of Instances Scanned: The above observations show how many activities were recorded by the intrusion detection system. As the size of the database /trace increases the scanning becomes slow, may need to multiple scans or use projections of frequent items encoded as activities for this purpose. The average number of normal instances detected is important, so that we have less number of false alarms. The observations show how many activities were found to be "normal" VANET activities and recorded by the

intrusion detection system. These activities show no suspicion of Sybil attack. Detection of normal actives is routine but the real challenge comes when finding an abnormal activity in real time and fastest possible time. Then, most importantly the average number of abnormal instances of Sybil attack activities detected is also observed. This observation from the simulations shows how many activities found to be "abnormal" VANET activities and recorded by the intrusion detection system. These activities show suspicion as the pattern of click steam of the VANET user is not similar to what it should be in routine. Hence, there is possibility of "Sybil attacker " or malicious person who is not following right full activity path sequence is trying to be part of Sybil attack. The observations also show that the proposed algorithm is better in detecting even a small unsolicited sequence pattern of the VANET user and there is less possibility of "False alarm rate ". Since, as per the data/trace only on average of 3-4 activities which were "abnormal" were injected while running the simulation. The proposed algorithm was able to find it correctly. Here "abnormal "means unnecessary sending so many messages so that the attacker is able to isolate the victim vehicle. It is also worth mentioning that the average time in Detection of the Sybil cannot be ignored here in this report. This series of experiments shows how much time the algorithm took to find the "abnormal" VANET activities and recorded by the intrusion detection system is also critical for reducing the overhead. Here "abnormal "means unnecessarily sending so many messages so that the attacker is able to isolate the victim vehicle. The idea here is based on the concept of building large number of floods of packets & large number of collusions that would lead to isolation of victim. It is clear from the above graph the execution time in detection is faster in the proposed algorithm, It is helps to identify the collusions of the packets occurring to reoccurring sequences of activities of Sybil attack.

- It is clear from the above computational overhead also get reduced due to sequence mining of the events occurring between the nodes in spite of the fact that nodes are maintaining anonymity.
- It is clear from the simulations runs that the number of observation of sequences is quite large.
- It is also apparent from the graph the average ratio of the malicious activity leading to Sybil attack and normal activity is very small, which makes the work the algorithm challenging as there is huge similarity of the sequences in the events occurring in VANET.
- In this research work we have been able to build a detection system that can do pattern discovery on the fly based on the sequencing analysis of the trace of the event activities of a VANET vehicle user, the proposed algorithm is work efficiently in giving fast response time as it is apparent from running series of experiments and simulations However, care must be taken for following things also otherwise the algorithm will fall apart.

VIII. FUTURE SCOPE

The proposed IDS are able to detect the Sybil attack in the vehicular networks. When the network size is small the attacks are detected efficiently by the IDS but with the increase in the number of network nodes the numbers of attackers also increases and so are their attacking attempt which makes IDS a little less effective as it misses some of the attacks. The proposed IDS still need some improvements. The accuracy of the system decreases as we go on increasing the network size. Moreover the database in the IDS also increases with the network size and becomes difficult to handle. So in the future work some alterations needs to be done in the present proposed system. The system should be able to perform accurately in heavy traffic scenarios.

IX. REFERENCES

[1]. T. Leinmuller, E. Schoch, and C. Maihofer, (2007)"Security requirements and solutions concepts in vehicular ad hoc networks". In Proceedings of Fourth Annual Conference on Wireless on Demand Network Systems and Services.

[2]. P. Papadimitratos, V. Gligor, and J.-P. Hubaux,(2006) "Securing vehicular communications— assumptions, requirements, and principles". In Proceedings of the Workshop on Embedded Security on Cars (ESCAR)

[3]. M. Raya and J.-P. Hubaux,(2007)" Securing vehicular ad hoc networks". Journal of Computer Security, 15(1), 39–68.

[4]. A. Aijaz, B. Bochow, F. Dtzer, A. Festag, M.Gerlach, R. Kroh, andT. Leinmuller,(2006) "Attacks on inter-vehicle communication systems—an analysis". In Proceedings of the 3rd international Workshop on Intelligent Transportation (WIT).

[5]. Haberle, T.; Charissis, L.; Fehling, C.; Nahm, J.; Leymann, F., "The Connected Car in the Cloud: A Platform for Prototyping Telematics Services," in Software, IEEE, vol.32, no.6, pp.11-17, Nov.-Dec. 2015.

Vezzani, R.; Cucchiara, R., "Event driven software architecture for multi-camera and distributed surveillance research systems," in Computer Vision and Pattern Recognition Workshops (CVPRW), 2010 IEEE Computer Society Conference on, vol., no., pp.1-8, 13-18 June 2010.

[6]. Chun-Hung Wang; Mong-Fong Horng; Jeng-Wei Lee; Yu-Chan Liu; Ren-Shang Tsai; Wei-Tong Wang; Lan Chang; Yaw-Huang Kuo; Pau-Choo Chung; Kuo-Feng Ssu, "Development of Intelligent Home Health-Care Box Connecting Medical Equipments and Its Service Platform," in Advanced Communication Technology, The 9th International Conference on, vol.1, no., pp.311-315, 12-14 Feb. 2007.

[7]. Chaurasia, B.K.; Tomar, R.S.; Verma, S.; Tomar, G.S., "Suitability of MANET Routing Protocols for Vehicular Ad Hoc Networks," in Communication Systems and Network Technologies (CSNT), 2012 International Conference on, vol., no., pp.334-338, 11-13 May 2012.

[8]. Yeongkwun Kim; Injoo Kim, "Security issues in vehicular networks," in Information Networking (ICOIN), 2013 International Conference on, vol., no., pp.468-472, 28-30 Jan. 2013.

[9]. Na Ruan; Nishide, T.; Hori, Y., "Threshold ElGamal-based key management scheme for distributed RSUs in VANET," in Mobile and Wireless Networking (iCOST), 2011 International Conference on Selected Topics in, vol., no., pp.133-138, 10-12 Oct. 2011

[10]. Wagan, A.A.; Mughal, B.M.; Hasbullah, H., "VANET Security Framework for Trusted Grouping Using TPM Hardware," in Communication Software and Networks, 2010. ICCSN '10. Second International Conference on, vol., no., pp.309-312, 26-28 Feb. 2010.

[11]. Zhu Xiaoling; Hu Donghui; Hou Zhengfeng; Ding Liang, "A location privacy preserving solution to resist passive and active attacks in VANET," in Communications, China, vol.11, no.9, pp.60-67, Sept. 2014

[12]. Cao, Zigang; Xiong, Gang; Guo, Li, "MimicHunter: A General Passive Network Protocol Mimicry Detection Framework," in Trustcom/BigDataSE/I???SPA, 2015 IEEE, vol.1, no., pp.271-278, 20-22 Aug. 2015.

[13]. Dietzel, S.; Gurtler, J.; van der Heijden, R.; Kargl, F., "Redundancy-based statistical analysis for insider attack detection in VANET aggregation schemes," in Vehicular Networking Conference (VNC), 2014 IEEE, vol., no., pp.135-142, 3-5 Dec. 2014.

[14]. Feiri, M.; Petit, J.; Schmidt, R.K.; Kargl, F., "The impact of security on cooperative awareness in VANET," in Vehicular Networking Conference (VNC), 2013 IEEE, vol., no., pp.127-134, 16-18 Dec. 2013

[15]. Sayegh, N.; Elhajj, I.H.; Kayssi, A.; Chehab, A., "SCADA Intrusion Detection System based on temporal behavior of frequent patterns," in Mediterranean Electro technical Conference (MELECON), 2014 17th IEEE, vol., no., pp.432-438, 13-16 April 2014.

[16]. AlMheiri, S.M.; AlQamzi, H.S., "MANETs and VANETs clustering algorithms: A survey," in GCC Conference and Exhibition (GCCCE), 2015 IEEE 8th, vol., no., pp.1-6, 1-4 Feb. 2015.

[17]. Mukherjee, B.; Heberlein, L.T.; Levitt, K.N., "Network intrusion detection," in Network, IEEE, vol.8, no.3, pp.26-41, May-June 1994.

[18]. Krishna, T.R.V.; Barnwal, R.P.; Ghosh, S.K., "MDS-Based Trust Estimation of Event Reporting Node in VANET," in Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on, vol., no., pp.315-320, 16-18 July 2013.

[19]. 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.

[20]. Erritali, M.; El Ouahidi, B., "A review and classification of various VANET Intrusion Detection Systems," in Security Days (JNS3), 2013 National, vol., no., pp.1-6, 26-27 April 2013.

[21]. Raut, S.B.; Malik, L.G., "Survey on vehicle collision prediction in VANET," in Computational Intelligence and Computing Research (ICCIC), 2014 IEEE International Conference on, vol., no., pp.1-5, 18-20 Dec. 2014.

[22]. Jeong, H.J.; WooSeok Hyun; Jiyoung Lim; Ilsun You, "Anomaly Teletraffic Intrusion Detection Systems on Hadoop-Based Platforms: A Survey of Some Problems and Solutions," in Network-Based Information Systems (NBiS), 2012 15th International Conference on, vol., no., pp.766-770, 26-28 Sept. 2012.

[23]. Ajay Rawat, Santosh Sharma, Rama Sushil, "Vanet: Security Attacks and its Possible Solutions," Journal of Information and Operations Management, Volume 3, Issue 1, pp-301-304, 2012.

[24]. Schmidt, Robert K., Tim Leinmüller, Elmar Schoch, Albert Held, and Günter Schäfer. "Vehicle behavior analysis to enhance security in vanets." In Proceedings of the 4th IEEE Vehicle-to-Vehicle Communications Workshop (V2VCOM2008). 2008.

[25]. Hussain, Rasheed, Sangjin Kim, and Heekuck Oh. "Privacy-aware VANET security: Putting data-centric misbehavior and sybil attack detection schemes into practice." In Information Security Applications, pp. 296-311. Springer Berlin Heidelberg, 2012.

[26]. Ruj, Sushmita, Marcos Cavenaghi, Zhen Huang, Amiya Nayak, and Ivan Stojmenovic. "On data-centric misbehavior detection in VANETs." In Vehicular Technology Conference (VTC Fall), 2011 IEEE, pp. 1-5. IEEE, 2011.

[27]. Chandrapal U. Chauhan, V.A.Gulhane, "Signature Based Rule Matching Technique in Network Intrusion Detection System." International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 4, pp 412-41, April 2012.

How to cite

Rohika Bhatt, Parveen Thakur, "A Comparative Analysis of Sybil Attacks on VANET ". *International Journal of Research in Computer Science*, 5 (2): pp. 7-17, December 2015.