http://dx.doi.org/10.21172/ijiet.81.028

A Novel Mechanism of Detection of Sybil Attack in Vanet using Timestamp Approach

Shikha Sharma
M.TECH Scholar
Department of Computer Science ACET, ASR

Shivani Sharma
Assistant Professor
Department of Computer Science ACET, ASR

Abstract: Security is a condemnatory situation in the network at the instant of transference. Miscellaneous grouping of attacks become visible in the network. In this paper we will examine about Sybil Attack. The proposed technique is the major idealization of our effort to provide elevated security to the network from Sybil attack using timestamp approach. Our proposed effort focused to diminish the issue of misconception using timestamp series algorithm. The simulation results show the proposed technique prolonged the Sybil attack as well as the existing comparison in the paper.

KEYWORDS: Vehicular Ad-hoc Network (VANETs), Sybil attack.

I. INTRODUCTION

Vehicular Ad-hoc Networks (VANETs)
is a shade of Adhoc Networks that demanded adequate examination and evolution. The transmission with the Vehicle Node to Vehicle Node in VANET is very invigorating because of its rapid mobility and prompt structure division [1]. VANET is a type of MANET which stands for Vehicular adhoc network which utilize nodes are in the disposition of cars so as to generate a vehicular network. A Vehicular ad-hoc network is a sort of Mobile ad-hoc network, in which close vehicles or cars are provided communication between them, among vehicles, also between some stable appliances called Road side units (RSU's)[2]. Vehicular ad-hoc network that contribute Vehicles to Vehicles (V2V), Road-side Unit to Road-side Unit(R2R) and Vehicles to road-site Unit (V2R) communication. In contemporary further misfortune occurrences are originate significantly. Due to this, roads are originated to be further crowded and occupied [3]. In VANET Road side
Units (RSUs) are firmed up on the trail circle and On Board Unit (OBU) is furnished inner side vehicle and each vehicle is assumed to grip OBU. Road Side Units and On Board Unit are congregate with data processing units, sensors and radio connection [2].This is attained by utilizing Dedicated Short Range Communication (DSRC) protocol [6]. VANET require aggregate of transmission in sequence to carry both security, and non-safety applications .Accompanied by anomaly of enquiry such as red-light notification and icy-road which are based on V2I communications because of the certainty that they require the road side unit (RSU), nearly all of the protected applications be composed in the live stream of a beacon which includes velocity, location, and more distant vehicle position figures by vehicles. They hold up by single-hop V2V communication [4]. Moreover, to attain the deliberate expansion in traffic safety VANETs should be durable i.e., it should be firmed put down the structure away of performance on a immense scale. [5]
Security is an important concern in VANETs as it should evade any emanate of any details. In sequence to conserve and make sure integrity, confidentiality the vehicles must be validated at first with RSU. After validation the vehicle is subjected a pseudo id by the RSU. Here pseudo id is used to put the actual id of the vehicle in sequence to make certain more safety. [6]

VARIOUS THREATS IN VANET
To acquire more desirable protection from assaulter we must have the apprehension about the assaults in VANET versus privacy necessity. Attacks on identical safety demands are given below [14]. The crucial hazards to the VANETs are:

- Message Forging (Bogus Information)
- Impersonation (Pretention)
- Packet Dropping
- Sybil Attack
- Hidden Vehicle Problem
- On-Board Tampering etc.

Message Forging: This is one of the nearly familiar attacks which are essentially anxious with the current data. Malicious nodes stimulated the message imminent from the sender and transfer to the other vehicles in the range so that all the other nodes get the erroneous data and VANET system will crumbled.

Hidden Vehicle: This is one of the nearby significant warnings associated to VANET security. In this, assaulter swindle the sender vehicle that it is in superior locale to dispatch the safety messages so dispatcher vehicle terminate its signal transmission to restraint the crowd in the network but the assaulter delude distinct nodes by rapid imprecise data or even not transferring any caution messages at all. In other phrase, sender vehicles become concealed to distinct or its location existence stimulated. Sometimes assaulter may be also concealed to others by possessed itself in tunnel and defraud with safety messages which is swindle to impairing the system.

On-Board Tampering: This concern is predominantly associated to the reliability and isolation of the safety communication. OBUs (On-Board Units) are furnished with hardware framing also they have software properties executes above. Each of the OBU has its personal key pairs (public-private keys) called incognito for their identity and if it is interfered, the OBU conducts unusual and it may be injured to the entire system. [12]

SYBIL ATTACK

Sybil attacks, in which a mischievous vehicle fabricate an vision of transportation congestion by erecting innumerable individuality.[7] Each node dispatched information with numerous characters, in this way distinct nodes noticed that there are multiple nodes in the network at the identical time.[8] In a Sybil attack, there are two kind of nodes that are malicious node or Sybil assaulter and Sybil node:

1. Malicious node/Sybil attacker: The node which take off the individuality of distinct nodes.
2. Sybil node: further identities fabricated by the
hostile nodes are well known as Sybil nodes. [9]

Sybil attack set down a significant clash on the act of the VANET by constructing an mirage of existing of various vehicles in the network. The clash of this assault is that after imitation the personalities or situations of other vehicles in vehicular network, this assault may conduct to alternative kind of assault [10].

These are few assaults that may be accomplished in a VANET domain by an assaulter. Different panaceas have been stated by writers for these assaults. In this paper we shall assumed only Sybil attack in brief.[11]

II.RELATED WORK

Amrit Suman et.al [1] presented that the safety and security of messages is the idolized necessity for vehicular network. Security and privacy of the messages are the two analysed motivating strong vehicular network designs. This paper confers routing protocols, and the network warnings that can be utilized the work staging of V ANET. This paper also report correlative production of routing protocol in appearance of Sybil.

Nirav.J patel et.al [3] described that demonstrating certitude is a provocation while one or more fake nodes completely to derange path location or data conveyance in the network. A lot of research has been accomplished for secure routing activity with trust-based approaches. In this paper, we present survey of different contraptions to elaborate various ad-hoc routing protocols for secure routing process by intensify the trust among various nodes in VANETs.

AshrithaM et.al [6] Security and privacy are the two important reviews in V ANETs. Due to highly dynamic environment in V ANETs ciphering time for verification is more. At the same time most of the privacy preserving schemes is supine to Sybil attacks. In this paper we propose a lightweight authentication blueprint between vehicle to RSU, vehicle to vehicles and to frame a secure Communication system. In this approach we make use of timestamps concept and also deflate the estimating cost for validation in highly compact traffic regions. The privacy of the vehicle is preserved by not imparting its real identity.

Nai-Wei Lo et.al [14]represented that to approved eco-friendly driving VANET environments, that is, to extricate fuel and time in this text, we contemplated an event-based reputation system to avert the dispersion of bogus traffic cautioning messages. In this system, a dynamic reputation evaluation contrivance is made known to arbitrate even if an approaching traffic message is momentous and ethical to the driver. The proposed system is constituted and classified through experimental simulations. The simulation results show that, with a proper reputation remodelling components and applicable threshold backdrop, our proposed system can expertly defend against falsify messages disseminate on various VANET environments.

Xia Feng1 et.al [16] Sybil attack can counterfeit traffic rundown by dispatching casuistic messages with numerous coherences, which usually doer traffic corners and even bulges to vehicular collisions in vehicular ad hoc network (VANET). It is very extensive to be fortified and encountered, eminently when it is lofted by some contrived assaulters using their canonical selfdom. In this paper, we affirmed an event based reputation system (EBRS), in which dynamic reputation and trusted value for each crisis are employed to crack down the range of bogus messages. EBRS can descry Sybil attack with formulated uniqueness and lifted integrity in the evolution of communication; it also entrenched a crossed the connived Sybil attacks since each event has a exclusive reputation value and trusted value.

III. PROPOSED SOLUTION

Since the case of Sybil attack the node act as fake node and demand for data due to which these false identities also form an misapprehension that more vehicles are existing which leads to execution of more attacks after providing the fake position and fake identities of other nodes. In order to reduce this problem we will use Time Stamp Series Algorithm. In our algorithm if any vehicle in the network Contains many timestamps of last RSUs(Road Side Unit) it means it is suspected as Sybil attack .If any message contain very similar time stamp series it will treated as highly doubted Sybil attack. In our algorithm the RSUs will provide digitally signed and private key will generated for each timestamp. In our algorithm time stamp will be assigned by RSUs only and vehicles will not be capable of using timestamp obtained by other vehicles. The vehicle generate traffic message "Record "and broadcast it on periodic request of vehicles or occasionally record contains traffic events and moving direction and speed. So as vehicle passes two RSU the vehicle certificate will contain two timestamp or more than two timestamp. The vehicle message format will be as follow :

TM ={Rcd, dSig(KVi-, Rcd), Cert_Ti,Cert_Ri}

In above message Cert_Ti means that vehicle through a RSU and it contain valid certificate of the signed Rcd (Record) validity of the signed record can be verified By the public key assigned to certificate Cert_Ti and validity of certificate for corresponding RSU.the digital signature dSig(KVi) will avoid malicious Vehicles which will provide fake position and fake identities while broadcasting Record regarding traffic message

Let us identify Sybil attack in two random traffic messages .The two messages are:

TM= Traffic Message

Rcd= Record

Cert_Ti= Certificate

TM1={Rcd,dSigi, Cert_Ti, Cert_Ri}

and TM2 = {Dataj, Sigj, Cert_Tj,Cert_Rj}

The conditions for proving Sybil attack are:

1. If the information of RSU given by the two certificate Cert_Ri and Cert_Rj will be same.
2. If the issued certificate Cert*_Ti and Cert_Tj* are issued by same RSU.

The proposed algorithm not only works efficiently in Sybil attack as well as detection in low traffic scenario but in high traffic also. As in our algorithm only vehicle has to obtain the certified timestamps, and no constraints on demanding timestamps as well. The RSUs has to provide simple working which make it more realistic and economical during the initial VANET deployment stage.

IV. EXPERIMENTAL SETUP

The algorithms performance has been observed and analyzed on the basis of result of simulation which is performed on the NS2. The NS2 framework is initially studied and then framework has been modified along with Timestamp approach in order to analyze various algorithms. Results are observed under low and high Traffic Environment.

S. No.	Parameter	Value(s)
1	Simulator used	NS 2.35
2	Simulation Time	500 Secs
3	Simulation Area	1500 X 1500
4	MAC	802.11
5	Number of nodes	175
6	Speed of Nodes	2 to 16 (m/sec)
7	Mobility Model	Random W7aypoint
8	Transmission Range	250m
9	Packet Size	512 KB
10	Packet Rate	4 packets/sec
11	Traffic Type	CBR

V. RESULT AND ANALYSIS

1. Communication delay

The analysis of delay between EBRS and DTA are shown in fig.1 that shows the delay using DTA is very low as compared to EBRS, but due to increase in vehicle density the communication delay increase in both the cases but in our proposed technique the results are much better.

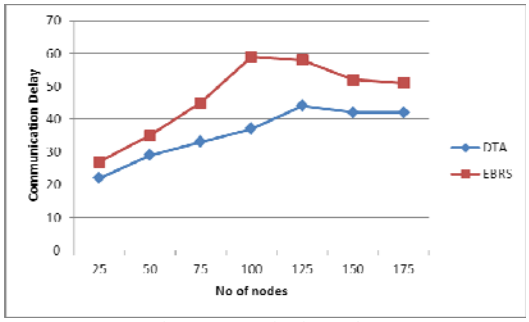

Fig1. Communication Delay

	Communication Delay	
No of Nodes	EBRS(Existing)	DTA(proposed)
25	27	22
50	35	29
75	45	33
100	59	37
125	58	44
150	52	42
175	51	42

2. Delivery ratio

The analysis of Delivery ratio between EBRS and DTA are shown in fig.2 that shows the Delivery ratio using DTA is very low as compared to EBRS but due to increase in vehicle density the communication delay increase in both the cases but in our proposed technique the results are better.

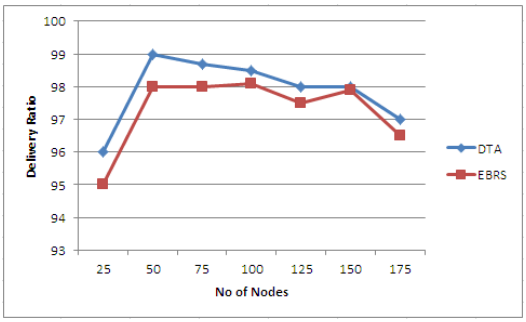

Fig2. Delivery ratio

	Delivery ratio	
No Vehicles	EBRS(Existing)	DTA(Proposed)
25	95	96
50	98	99
75	98	98.7
100	98.1	98.5
125	97.5	98
150	98	98
175	96.5	97

3. Simulation time

The analysis of Data loss between EBRS and DTA are shown in fig.3 that shows the Data loss using DTA is low as compared to EBRS.

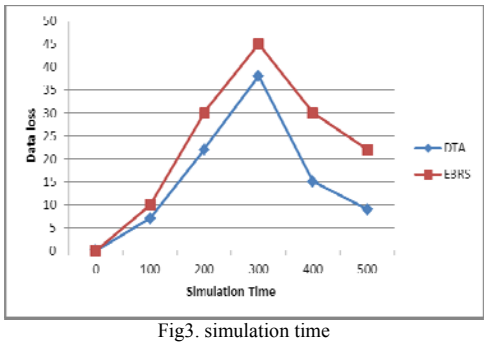

Fig3. simulation time

	Data Loss	
Simulation Time	EBRS(Existing)	DTA(proposed)
0	0	0
100	10	7
200	30	22
300	45	38
400	30	15
500	22	9

CONCLUSION

This paper concludes that many researchers provide their methodologies to solve sybil attack but still our method is one of the major inclusion in detecting malicious nodes in Sybil attack using VANETs. our methodology will overcome this attack and that approach will be improved than the existing approaches.

REFERENCES

[1] Amrit Suman, Chiranjeev Kumar" A Behavioral Study of Sybil Attack on Vehicular Network"2016.
[2] arvinder Kaur, Mandeep Devgan, Dr.Parminder Singh" Sybil Attack in VANET"2016.
[3] Nirav j.patel ,Rutvij H.Jhaveri "Trust based approaches for secure routing in VANET: A Survey" 2015.
[4] Dhavy Gantsou" On the Use of Security Analytics for Attack Detection In Vehicular Ad Hoc Networks"2015.
[5] Sebastian Bittl, Arturo A. Gonzalez, Matthias Myrtus Fraunhofer ESK, Hanno Beckmann, Stefan Sailer, Bernd Eissfeller" Emerging Attacks on VANET Security based on GPS Time Spoofing"2015.
[6] AshrithaM, Sridhar CS" RSU Based Efficient Vehicle Authentication Mechanism for V ANETs"2015.
[7] Mandeep Kaur Saggi, Ranjeet Kaur" Isolation of Sybil Attack in VANET using Neighboring Information"2015.
[8] Priyanka Soni, Abhilash Sharma" A Review of Impact of Sybil Attack in VANET's"may 2015.
[9] Deepika Shrivastava, Ankur Pandey" A Study of Sybil and Temporal Attacks in Vehicular Ad Hoc Networks: Types, Challenges, and Impacts" 284 - 291, 2014.
[10] Priyanka Sirola, Amit Joshi, Kamlesh C. Purohit" An Analytical Study of Routing Attacks in Vehicular Ad-hoc Networks (VANETs)"july 2014.
[11] Deepak Kushwaha, Piyush Kumar Shukla, Raju Baraskar " A Survey on Sybil Attack in Vehicular Ad-hoc Network" july 2014.
[12] Jitendra Bhatia and Bhumit Shah" REVIEW ON VARIOUS SECURITY THREATS & SOLUTIONS AND NETWORK CODING BASED SECURITY APPROACH FOR VANET" mar 2013.
[13] Ram Shringar Raw1, Manish Kumar1, Nanhay Singh1"SECURITY ISSUES AND SOLUTIONS IN VEHICULAR ADHOC NETWORK: A REVIEW APPROACH".
[14] Nai-Wei Lo and Hsiao-Chien Tsai" A Reputation Systemfor Traffic Safety Event on Vehicular Ad Hoc Networks"sept 2009.
[15] Mohamed Salah Bouassida, Gilles Guette, Mohamed Shawky, and Bertrand Ducourthial" Sybil Nodes Detection Based on Received Signal Strength Variations within VANET" 2008.
[16] Xia Feng1 · Chun-yan Li2 · De-xin Chen3 · Jin Tang1" A method for defensing against multi-source Sybil attacks in VANET"2016.