Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 12, December 2015, pg.88 – 102

Prevention of Sybil Attacks in VANETS Using Genetic Approach

Sakshi Gupta[1], Taranjit Singh Aulakh[2]

[1]Deptt. Of CSE, Bgiet, Sangur, Punjab, India.

[2]Assistant Professor

Deptt. Of CSE, Bgiet, Sangrur, Punjab, India.

[1] sakshibgiet@gmail.com; [2] taranaulakh@gmail.com

ABSTRACT: Vehicular additional on demand routing produces heavy routing traffic by blindly flooding the entire network with RREQ packets during route discovery. The routing over vehicular ad associated with dissemination of routing packets is quite huge especially when topology changes. Whenever a link or a route break occurs, a route recovery is performed which in turn invokes the alternate route selection from the available nodes on the basis of the neighboring node which is first to send route reply packet from destination if there are more than one node sending packet at same time then node with higher available bandwidth will be selected. Hence the overall problem of this research work is to prevent the network from heavy load occurred due to Sybil attack at the network server. In this paper, we recommend a privacy-preserving system in the direction of detecting Sybil attacks in VANETs under a commonly utilized framework in the existing work. The framework assumes that vehicles communicate with each other in a multi-hop manner.in this we have utilized genetic algorithm's fitness function to optimize the network nodes. The results are being evaluated on the basis of parameters such as throughput, energy consumption, error rate, and end to end delay. The whole stimulation model takes place in MATLAB 7.10 environment.

Keywords: VANET, Security, Genetic Optimization Algorithm, Sybil attack

1 INTRODUCTION

Users need protection as well as safe keeping on the road in upcoming era and it might be promising by executing protected plus safe Vehicular Ad hoc Networks applications that is a growing technology. This technology is a huge region intended for assailants who attempt to modify the contents of the safe and non-safe applications to misguide the consumers of some particular network by means of their malevolent assaults. In recent times, road vehicles were the jurisdiction of mechanical engineers. On the other hand, with the dropping charges of electronic constituents as well as the perpetual preparedness of particular creators in the direction of upsurging road safety and also in the direction of differentiating themselves commencing their opponents, vehicles are becoming ‘‘computers on wheels’’, or rather ‘‘computer networks on wheels’’ [1]. Vehicular Ad hoc Networks have some particular prospective towards not solitary to simplify the decision taking jobs of drivers, then again towards improving highway road driving safety. Nevertheless, scientists [1, 2] have pointed out in which Vehicular Ad hoc Networks are confronting a big amount of security dangers that might damage the competence of Vehicular Ad hoc Networks as well as even life well-being. One of these intimidations is Sybil attacks, in that a malevolent automobile entitlements several fictitious individualities. Sybil attacks could possibly be destructive to a variability of Vehicular Ad hoc Networks applications. For instance, a desirous driver know how to assemble in which a number of vehicles are wandering adjacent that also generates a delusion of traffic overcrowding. At that time, additional vehicles would probably select a substitute path way as well as relinquish the road intended for the desirous driver. In the meantime, the contrived vehicles are in point of fact under the mechanism of one malevolent node, the malevolent node might have additional control of several other network protocols.

For instance, the huge amount of Sybil nodes might probably deviate the consequences of voting-reliant procedures commencing the truth; the Sybil nodes might also inaugurate Denial of Service assaults in the direction of impairing the customary functions of information distribution protocols, for example [3, 4, and 5]. Sybil attacks might possibly become reason for severe safety dangers. For instance, in the application of deceleration warning frameworks [2], in some specific conditions a vehicle lessens the aforementioned speed considerably, it would probably transmit a threatening in the direction of the subsequent vehicles. Receivers would probably transmit the message in the direction of vehicles which are further behind. On the other hand, this advancing process could be get involved through a huge number of malevolent Sybil vehicles. In this approach, the malevolent challenger could possibly generate an enormous road accident on the highway, hypothetically instigating abundant loss of life.

Conventionally in Ad hoc Networks and Sensor Networks, three categories of defense in contradiction of Sybil assaults are acquaint with, together with: identity registration, radio resource testing, as well as position verification [6]. Radio resource testing is dependent upon the supposition in which a radio cannot direct or receive concurrently on more than one channel. This one does not implantable towards Vehicular Ad hoc Networks meanwhile a desirous driver might cheaply attain numerous radios. Identity cataloguing alone could not preclude Sybil assaults, for the reason that a malevolent node might acquire several identities through some non-technical approaches such as stealing. Additionally, strict cataloguing became reason for serious privacy anxieties. In position certification, the network authenticates the position of every single node and this also guarantees that every particular physical node is bound with only single identity. An amount of position (or distance) verification methods [7, 8, 9, and 10] have been projected lately. Sybil assaults are fairly dangerous intended for a variability of network applications. Hard work have been done in the direction of perceiving Sybil nodes in MANETs and Sensor Networks. Fundamentally, in Vehicular Ad hoc Networks, Sybil assaults might effortlessly generate a delusion of traffic overcrowding. Furthermore, Sybil assaults might have a foremost impression on additional existing VANET protocols, counting MAC layer, routing layer, along with application layer. For instance, in the literature, the multi-hop broadcast protocol [5], the reliable MAC protocol [3], the bandwidth sharing protocol [11], and the data dissemination protocol [4] are all subject to Sybil attacks, for the reason that they altogether be dependent on nodes' collaboration in the direction of forwarding packages as well as a malevolent node might easily crack them through utilizing its huge number of counterfeit nodes.

In this paper, we recommend a privacy-preserving system in the direction of detecting Sybil attacks in VANETs under a commonly utilized framework in the existing work [12]. The framework assumes that vehicles communicate with each other in a multi-hop manner.in this we have utilized genetic algorithm's fitness function to optimize the network nodes. The results are being evaluated on the basis of parameters such as throughput, energy consumption, error rate, and end to end delay.

1.1 Applications of VANETs

The uses of VANETs into taking after classes:

1. Real-time movement: The constant activity information can be put away at the RSU and can be accessible to the vehicles at whatever point and wherever required [1].
2. Co-agent Message Transfer: Slow/Stopped Vehicle will trade messages and co-work to help different vehicles. Despite the fact that unwavering quality and dormancy would be of significant concern, it may mechanize things like crisis braking to dodge potential mischances. So also, crisis electronic brake-light may be another application.
3. Post-Crash Notification: A vehicle included in a mishap would telecast cautioning messages about its position to trailing vehicles with the goal that it can take choice with time under control and additionally to the thruway watch for tow away backing.
4. Road Hazard Control Notification: Cars advising different autos about street having avalanche or data with respect to street highlight warning because of street bend, sudden downhill and so forth.
5. Cooperative Collision Warning: Alerts two drivers conceivably under accident course with the goal that they can patch their ways.
6. Remote Vehicle Personalization/ Diagnostics: It helps in downloading of customized vehicle settings or transferring of vehicle diagnostics from/to base.
7. Internet Access: Vehicles can get to web through RSU if RSU is filling in as a switch.

8. Digital guide downloading: Map of locales can be downloaded by the drivers according to the prerequisite before making a trip to another region for travel direction. Likewise, Content Map Database Download goes about as an entryway for getting profitable data from versatile problem areas or home stations.
9. Real Time Video Relay: On-interest film experience won't be restricted to the limitations of the home and the driver can request continuous feature transfer of his most loved motion pictures.
10. Value-included ad: This is particularly for the administration suppliers, who need to pull in clients to their stores. Declarations like petrol pumps, roadways eateries to declare their administrations to the drivers inside correspondence range. This application can be accessible even without the Internet.

1.2 Advantages in VANETs

There are several advantage

1 Highly dynamic topology .The rapid of the vehicles alongside the accessibility of decisions of different ways characterizes the element topology of VANETs [6].

2 Frequent separated system. The rapid of the vehicles in one way characterizes the element topology while then again requires the regular prerequisites of the roadside unit absence of which results a continuous separations.

3 Mobility demonstrating and Prediction. The forecast of vehicle position and their developments is extremely troublesome. This highlights of portability demonstrating and forecast in VANETs is in view of the accessibility of predefined guide's models. The rate of the vehicles is again an imperative for productive system outline.

4 Communication Environment. When we are having a portability model, yet we are not done. As the versatility model may have distinctive highlights relying on street construction modelling, roadways, or city situations. Imparting in these circumstances must be taken consideration.

5 Hard deferral imperatives. At the season of crisis, conveyance of messages on time is a basic issue. Thusly, handle such circumstances rather speaking just about high information rates in not sufficient.

6 Interaction with on board sensors are the method of interchanges. Sensors can read information identified with speed of the vehicle, course and can impart to the server farm. Subsequently sensors can be utilized as a part of connection development and in steering conventions.

7 Unlimited Battery Power and Storage Nodes in VANETs don't endure force and capacity impediment as in sensor systems; thusly enhancing obligation cycle is not as pertinent as in sensor systems.

2 SYBIL ATTACK IN VANET

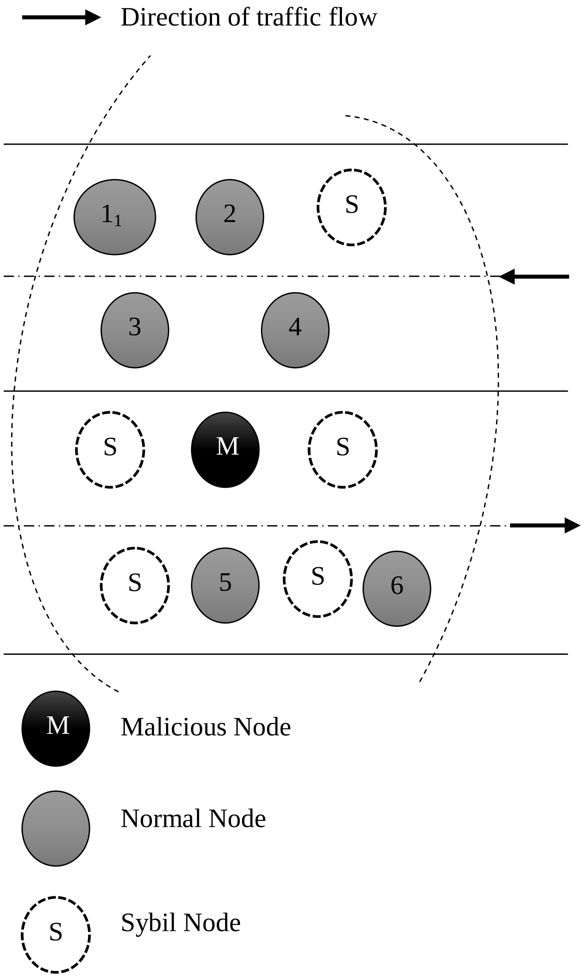


Fig.1 An example VANET under Sybil attacks.

It is an unsafe advanced world out there. Security and antivirus programming is essential for any system. Restricted security can separate is in a Sybil attack. False information reported by a single malicious vehicle may not be sufficiently convincing. Applications may require several vehicles to reinforce a particular information, before accepting it as truth. However, a serious problem arises when a malicious vehicle is able to pretend as multiple vehicles called a Sybil attack, and suitably reinforce false data. If benign entities are unable to recognize a Sybil attack [13], they will believe the false information, and base their decisions on it. Hence, addressing this problem is crucial to practical vehicular network systems. Sybil attack is a kind of security risk when a hub in a system guarantees various characters.

Most systems, similar to a shared system, depend on assumptions of personality, where every PC speaks to one character. A Sybil attack happens when an unreliable PC is captured to claim different characters. Issues emerge when a reputation system, (for example, a record sharing reputation on a system) is deceived into believing that an attacking PC has a disproportionally vast impact. Correspondingly, an attacker with numerous personalities can utilize them to act maliciously, by either taking data or disturbing correspondence. Sybil attacks have showed up in numerous situations, with wide usage for security, wellbeing and trust. For instance, a web survey can be fixed utilizing various IP locations to present countless. A few organizations have likewise utilized Sybil attack to increase better appraisals.

3 PREVIOUS WORK DONE

James Newsome et.al [13], talked about the Sybil attack in system C. Piro, C. Shields, and B. N. Levine additionally clarified the Sybil attack is an attack in which a single entity can control a considerable division of the system by showing different identities. DSR routing is a basic algorithm .The DSR Route Request control packet is changed by including another field that will be utilized to focus the acknowledgement level of accessible bandwidth. Keeping in mind the end goal to test the proposed model, a recreation model is actualized utilizing the Network Simulator (NS-2.28).

BinTian et.al [14], In this paper demonstrates that as of late, with advances in IT sector and WSN to advance the fast advancement of low power, low value, multifunction sensor, and remote sensor systems have been generally utilized as a part of general. The proposed model recognize Sybil attacks in WSN. At last, the hypothetical investigation and investigations affirm this system can adequately recognize Sybil attacks and enhance the security of remote sensor systems.

Hadlee,N.A. et.al [15], This paper demonstrates that Sybil attack is the most conspicuous and testing attack in open-access distributed system. In Sybil attacks, a malicious client makes various fake personalities called Sybil characters prompting the majority of the legitimate hubs in the system to be controlled by them.

Sinha,S et.al, [16], In this paper the creators considered security as a standout amongst the most difficult issues in Mobile Adhoc Network (MANET) because of the absence of concentrated power and constrained assets. This paper talks about distinctive types of security attacks in MANET and gives accentuation especially on the Sybil attack which is a standout amongst the most destructive attack. This paper likewise acquaints another methodology with distinguish Sybil attacks in view of bunching and also resource testing.

Thiyam Romila Devi et.al, [17]clarified about the GA. The population is the accumulation of candidate solutions that we are considering throughout the calculation. Over the generations of the calculation, new individuals are "conceived" into the population. Better the fitness function better the optimization.

Sujatha, K.S et.al, [18], they propose a procedure to dissect the introduction to attacks in AODV. The proposed framework is taking into account Genetic Algorithm, which investigates the practices of each hub and gives insights about the attacks. The execution of MANET is investigated taking into account GAC.

Istikmal et.al, [19] This paper shows about examination consequence of AODV, DSR and DSDV that connected an Ant-algorithm which are AODV-Ant, DSR-Ant, and DSDV-Ant. DSDV speaks to of proactive routing protocol taking into account table driven. The outcome demonstrates that proactive routing enhance execution.

Ali Akbar et.al [20], discussed about defense methods against Sybil attack in VANETs. According to the studies in this area, each method has some advantages and disadvantages for implementing. Resource testing methods are not sufficient to implement for Sybil attack detection with high accuracy in VANETs. Authentication methods are more reliable and useful for message integrity, authenticity and privacy and there are suitable methods in this category for practical implementation in urban areas.

4 PROPOSED MODEL

The simulations were carried out by using MATLAB as the language that we use to develop the proposed framework. Below, we have given the methodology followed by the proposed framework flow chart. The methodology of the proposed work is given in steps below:

Step 1 : Start

Step 2 : Initialize with entering number of network vehicle nodes to configure.

Step 3 : Then, we search Sybil nodes in the cache memory of the network. A graph will appear showing the X and Y coordinate.

Step 4 : Once, Sybil nodes are found in several round. Then, evaluate parameters in Sybil attack such as energy, throughput, end to end delay and error rate.

Step 5 : After evaluation with Sybil attack in the network, we apply Genetic Algorithm on the network utilizing Fitness function for optimization purpose.

Step 6 : Then, we evaluate parameters again on the same network after applying Genetic Algorithm on parameters for example, energy consumption, throughput, end to end delay and error rate.

Step 7 : The result is obtained.

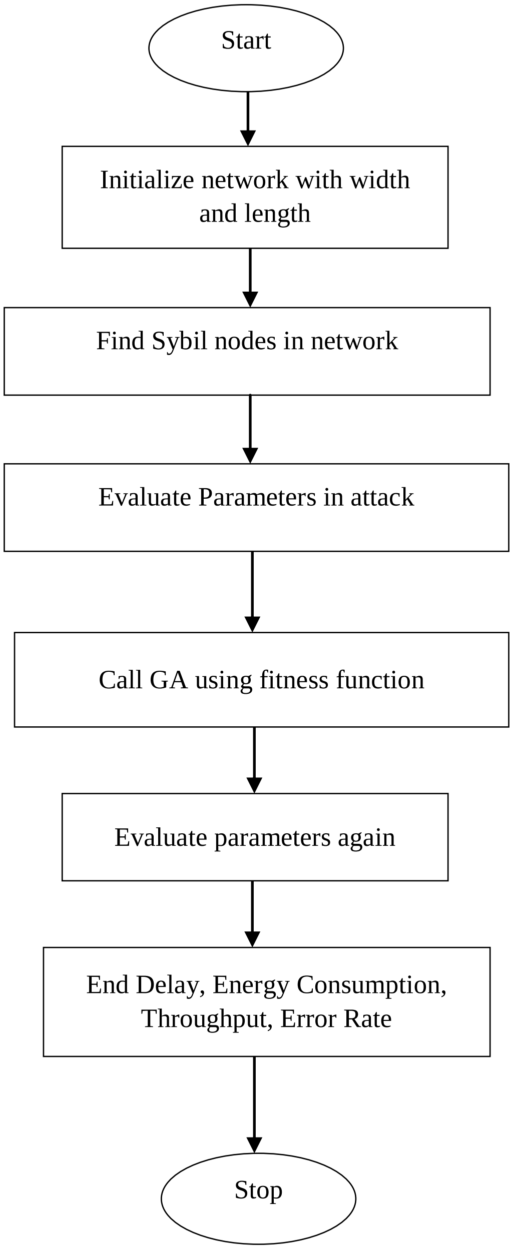

Start
Initialize network with width and length
Find Sybil nodes in network
Evaluate Parameters in attack
Call GA using fitness function
Evaluate parameters again
End Delay, Energy Consumption, Throughput, Error Rate
Stop

Fig.2 Flowchart of Proposed Work

5 RESULTS

5.1 Computation Parameters

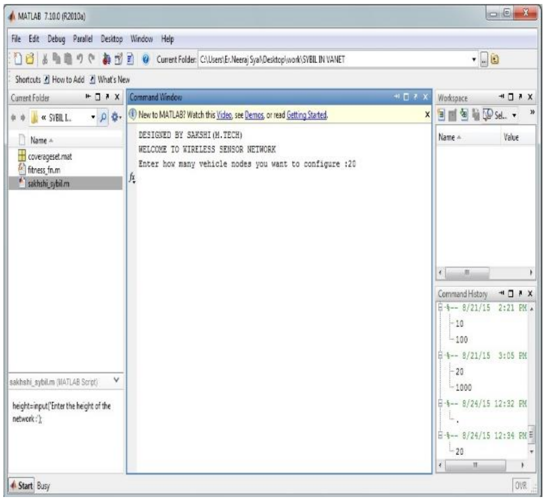
a) Throughput: Throughput is the number of packets sent over the network in given time. Throughput is the average rate of successful messages delivered over a communication channel. Unit: bits per second (bps).

b) End delay: Latency in a network, usually includes four parts: The transmission delay, queuing delay, propagation delay and processing delay. End to End Delay signifies the total amount of time taken by a packet from source to destination.

c) Error rate: the error rate is the number of bits that have errors relative to the total number of bits received in a transmission.

d) Energy Consumption: Energy consumption is the energy consumed by packets to deliver from source to destination.

5.2 Implementations


MATLAB 7.10.0 (R2010a)
File Edit Debug Parallel Desktop Window Help
Current Folder: C:\Users\Er.Neeraj Syal\Desktop\work\SYBIL IN VANET
Shortcuts How to Add What's New
Current Folder
« SYBIL I..
Name
coverageset.mat
fitness_fn.m
sakhshi_sybil.m
sakhshi_sybil.m (MATLAB Script)
Command Window
New to MATLAB? Watch this Video, see Demos, or read Getting Started.
Workspace
Name
Value
Command History
Start Busy
OVR

```
height=input('Enter the height of the network :');
```

```
DESIGNED BY SAKSHI(M.TECH)
WELCOME TO WIRELESS SENSOR NETWORK
Enter how many vehicle nodes you want to configure :20
```

```
%-- 8/21/15  2:21 PM
  10
  100
%-- 8/21/15  3:05 PM
  20
  1000
%-- 8/24/15 12:32 PM
  .
%-- 8/24/15 12:34 PM
  20
```

Fig. 3 Main GUI

In above figure, we have provided the GUI of the proposed system. In this, we have to enter how many vehicle nodes you want to configure and we have entered the value 20.

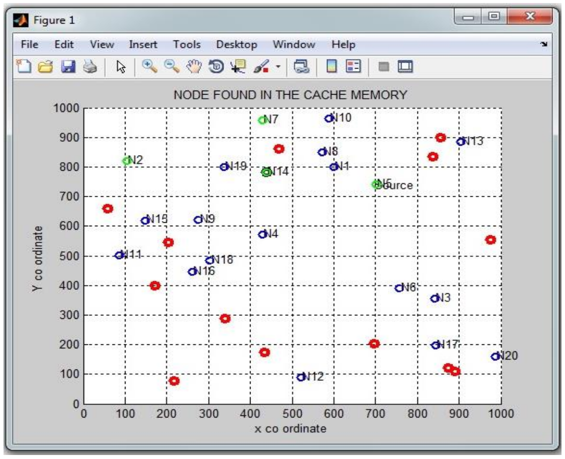
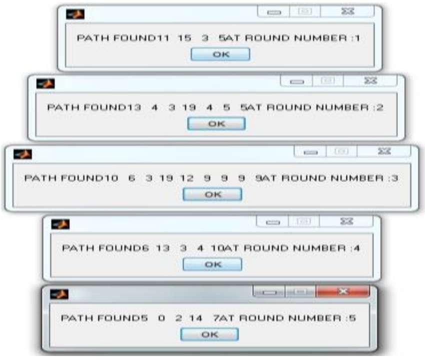


Fig.4 Network deployment, Sybil attack presentation and searching in cache memory

Above figure, initially the network simulation model is formed which contains 20 nodes as given input. Length vs breadth of the network is 1000*1000, the channel (CH) captures the routing information from the initiator (source node) and then sends the data from the source to destination node. Then we have Sybil nodes with k 5 number of rounds to get accurate value of Sybil nodes.

After this, plot maximum Sybil identities as a function of the compromised fraction of nodes f. Note that our theoretical prediction (which is strategy independent) matches closely with the attacker strategy of connecting Sybil nodes in a scale free topology. The red circles represent the nodes which can be either active nodes.



```
PATH FOUND11  15   3   5AT ROUND NUMBER :1
PATH FOUND13   4   3  19   4   5   5AT ROUND NUMBER :2
PATH FOUND10   6   3  19  12   9   9   9   9AT ROUND NUMBER :3
PATH FOUND6  13   3   4  10AT ROUND NUMBER :4
PATH FOUND5   0   2  14   7AT ROUND NUMBER :5
```

Fig.5 Path Found and round number

In above figure we found path among source and destination in 5 rounds as shown above.

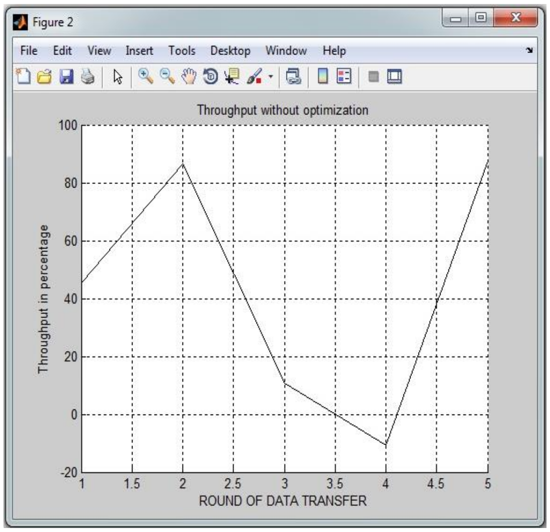


Fig.6 Throughput without optimization

In above figure, we have plotted graph between throughput in percentage with respect to round of data transfer. It is shown that the throughput initially increases as round of data transfer increases and then decreases after Sybil attack is introduced as shown in above figure.

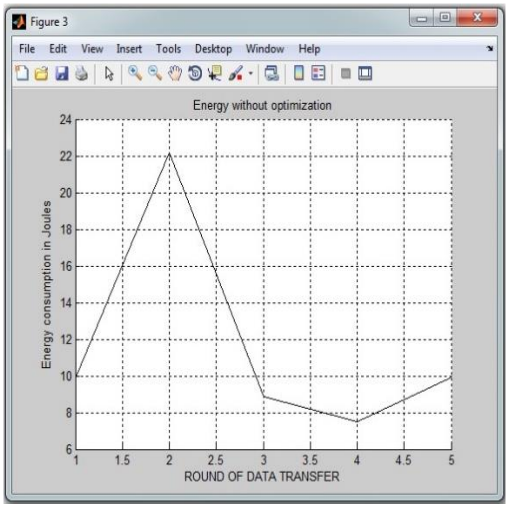


Fig.7 Energy consumed without optimization

In above figure, we have shown a graph showing how energy consumption decreases with respect to round of data transfer increases but when Sybil attack is introduced energy consumption increases with increase in round of data transfer increment. A graph is plotted between energy consumption in Joules and round of data transfer.

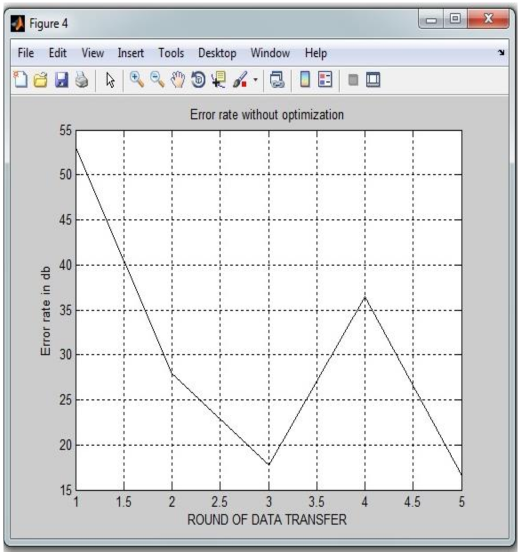


Fig.8 Error Rate without optimization

As shown in above figure, error rate is normally decreases as round of data transfer increases but when Sybil attack happens then error rate start increasing as shown above due to the attack.

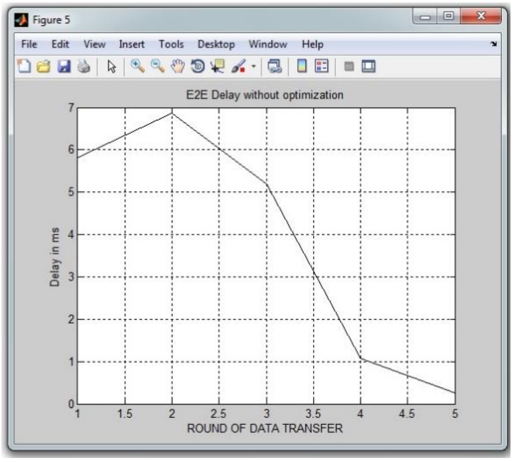


Fig.9 End to End Delay without optimization

From above figure, it has also observed that the end delay increases when Sybil attack is introduced due to greater number of identities the number of Sybil attackers.

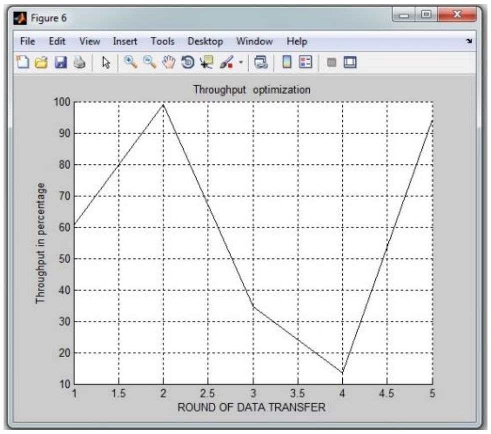


Fig.10 Throughput with optimization

The Sybil attacker nodes causes decrease in the throughput of the network. It is because number of collisions is more in system and it is optimized using GA algorithm as shown above. Above figure shows that throughput value with GA. Total data from the source to the receiver more than the time it takes until the recipient receives the last packet. Less time translates into higher productivity.

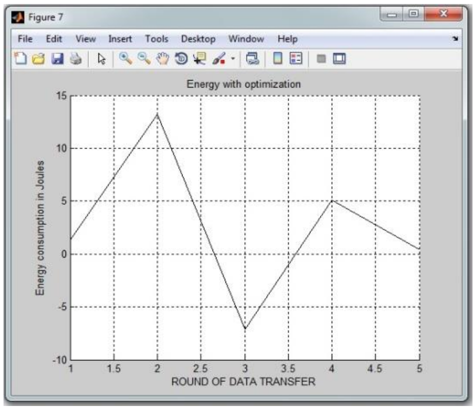


Fig.11 Energy consumption with optimization

In this after introducing Sybil attack energy consumption increases but after utilizing genetic algorithm for optimization it decreases energy consumption as round of data transfer increases.

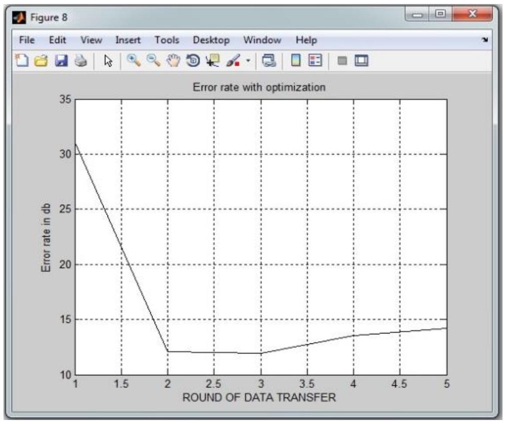


Fig.12 Error Rate with optimization

As above figure shows that error rate increases constantly but when Sybil attack occurs then it increase rapidly as shown. But when we utilize genetic algorithm for optimization the error rate decreases.

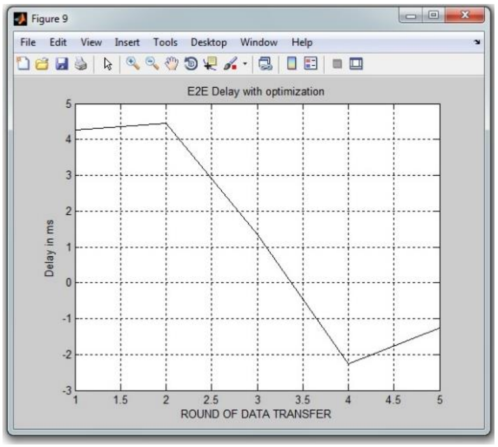


Fig.13 End to End Delay with optimization

The End to End Delay is a significant parameter for evaluating a protocol which must be low for good performance. Above figure shows the end to end delay with GA/DSR. This increase in delay is due to the Sybil nodes through which then passes to the destination node. However increase in the numbers of nodes also increases the difference of delay**.**

6 CONCLUSION& FUTURE SCOPE

Peer-to-peer systems play an ever-increasingly important part of our daily lives. However, most of the peer-to-peer systems are vulnerable to Sybil attacks. In order to design more efficient and practical Sybil defenses, we proposed an implementation based on Genetic algorithm. In this paper, the issues related to security like Sybil attack has been reviewed. Then an Intrusion Detection System (IDS) especially for Sybil attacks is implemented using Genetic Algorithm, and then tested with networks of varied node configurations in VANET architecture. The algorithm will be tested for more number of nodes and the performance analysis will be done in terms network load, throughput, node density, BER and packet drop ratio of the algorithm as the node number is increased. It is concluded that Sybil attack prevention is achieved at greater rate when GA has been used.

Future scope lies in the use of the hybridization of Genetic algorithm with other routing protocols like AODV or DSDV. As they are also vulnerable to this type of attacks.

REFERENCES

[1] M. Raya, J.-P. Hubaux, The security of vehicular networks, in: Proc. of the 3rd ACM Workshop on Security of ad Hoc and Sensor Networks, SASN 2005, pp. 11–21, 2005.

[2] B. Parno, A. Perrig, Challenges in securing vehicular networks, in: Proc. of the Fourth Workshop on Hot Topics in Networks, HotNets-IV, 2005.

[3] R.M. Yadumurthy, A. Chimalakonda, M. Sadashivaiah, R. Makanaboyina, Reliable mac broadcast protocol in directional and omni-directional transmissions for vehicular ad hoc networks, in: Proc. of the 2nd ACM International Workshop on Vehicular ad Hoc Networks, VANET 2005, pp. 10–19, 2005.

[4] J. Zhao, G. Cao, VADD*: vehicle-assisted data delivery in vehicular ad hoc networks*, IEEE Transactions on Vehicular Technology 57 (3) (2008).

[5] G. Korkmaz, E. Ekici, *Urban multi-hop broadcast protocol for inter-vehicle communication systems*, in: Proc. of the 1st ACM International Workshop on Vehicular ad Hoc Networks, VANET 2004, pp. 76–85, 2004.

[6] P. Golle, D. Greene, J. Staddon, *Detecting and correcting malicious data in VANETs*, in: Proc. of ACM International Workshop on Vehicular ad Hoc Networks, VANET 2004, pp. 29–37, 2004.

[7] S. Brands, D. Chaum, *Distance-bounding protocols,* in: Proc. of Workshop on the Theory and Application of Cryptographic Techniques on Advances in Cryptology, Springer-Verlag, Inc., 1994, pp. 344–359.

[8] P. Bahl, V.N. Padmanabhan, RADAR: *an in building rf-based user location and tracking system*, in: Proc. of IEEE Infocom 2000, pp. 775–784, 2000.

[9] N. Sastry, U. Shankar, D. Wagner, *Secure verification of location claims,* in: Proc. of the 2003 ACM Workshop on Wireless Security, WiSe 2003, pp. 1–10, 2003.

[10] S. Capkun, J.-P. Hubaux, *Secure positioning of wireless devices with application to sensor networks*, in: Proc. of Infocom 2005, pp. 1917–1928, 2005.

[11] M. Torrent-Moreno, H. Hartenstein, P. Santi, *Fair sharing of bandwidth in VANETs,* in: Proc. of ACM Workshop on Vehicular Ad Hoc Networks, VANET 2005, pp. 49–58, 2005.

[12] J. Zhao, G. Cao, VADD: *vehicle-assisted data delivery in vehicular ad hoc networks*, IEEE Transactions on Vehicular Technology 57 (3) (2008).

[13] Scott M.Thede, "*An Introduction to Genetic Algorithm*" IN 46135, JCSC 20, 1 (October 2004).

[14] BinTian;Yizhan Yao ; LeiShi ; ShuaiShao in " *A Novel Sybil Attack Detection Scheme In Wsn*".Broadband Network & Multimedia Technology (IC-BNMT), 2013 5th IEEE International Conference on17-19 Nov. 2013.

[15] Hadlee, N.A.; Kayalvizhi, S. in"*Increasing Sybil attack detection probability in open acess distributed system*" IEEE, 2011.

[16] Sinha, S; Paul, A; Pal, S. in "*Sybil attack in manet: detection and prevention*"Computational Intelligence and Information Technology, 2013. CIIT 2013. Third International Conference.

[17] ThiyamRomila Devi1, Rameswari Biswal2, Vikram Kumar3, Abhishek Jena, "*Implementation Of Dynamic Source Routing In Mobile Ad Hoc Network (MANET)*", International Journal of Research in Engineering and Technology , Volume: 02 Issue: 11 ,pp.339-345, Nov-2013.

[18] Sujatha, K.S. ; Dept. of Electron. &Commun. Eng., Anna Univ. of Technol., Chennai, India; Dharmar, V. ; Bhuvaneswaran, R.S in "*design of genetic algorithm for manet*"

[19] Istikmal ; Sch. of Eng., Telkom Univ., Bandung, Indonesia ; Leanna, V.Y. ; Rahmat, B.in *"comparison of proactive and reactive protocol in manet".*

[20] Ali Akbar Pouyan, Mahdiyeh Alimohammadi, "*Sybil Attack Detection in Vehicular Networks*", Computer Science and Information Technology 2(4): 197-202, 2014.