International Journal on Emerging Technologies (Special Issue on *RTIESTM-2016*) **7**(1): 99-107(2016)

ISSN No. (Print) : 0975-8364
ISSN No. (Online) : 2249-3255

Sybil Attack Prevention using neural network Algorithm

Randeep Kaur* and Gurbinder Singh Brar**
**Research Scholar, Department of CSE, AIET, Faridkot, (PB), INDIA.*
**8Assistant Professor, Department of CSE, AIET, Faridkot, (PB), INDIA.*

(Corresponding author: Randeep Kaur)
(Received 04 October, 2015 Accepted 04 November, 2015)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: Mobile ad hoc network additional on demand routing produces heavy routing traffic by blindly flooding the entire network with RREQ packets during route discovery. However, in presence of mobility, multipath protocols incur mobile additional package drops as well as end to end delay because of their reliance on hypothetically stale routes from caches. Since routing is a basic service in such a network, which is a prerequisite for other services, it has to be reliable and trustworthy. This arises the necessity for secure routing protocols. In addition to that network security is also needed to avoid several attacks such as wormhole, black hole, Sybil and several others. A Sybil attack refers to a network attack against identify in which a malicious client obtains several fake identities and also generates fake nodes that are inserted between authentic nodes in the system simultaneous. It has also been observed that Sybil attacker has increased the End to End Delay as well as energy consumption and reduced the Throughput of the network. So, it is essential to create a new approach to defend against them and their effect on the network.
In our proposed work, we have utilized DSR protocol and neural network to solve network issues and enhance its results while under in a Sybil attack. And results have been evaluated after Sybil attack occurs inside the network as well as after Neural network optimization is applied on the network utilizing specific parameter such as: throughput, energy consumption, end to end delay and error rate. The whole stimulation work is done utilizing mat lab software.

Keywords: MANET, DSR, Sybil Attack, Neural Network, End Delay, Throughput.

I. INTRODUCTION

In the most trivial networks (such as point-to-point links), some technique/approach is required for routing the packages commencing the source towards the final destinations. This also contains maintenance in addition to discovery of routes together with associated costs. And that is known as 'infrastructure based' wireless network, the task of routing is allocated to faithful nodes which are known as access points (AP). Configurations of the access points are much less dynamic as compared to their possibly movable, end-point nodes.

A very promising category of wireless networks, which has appeared is depended upon an Ad Hoc topology; these networks are known as Wireless Ad Hoc Networks. The word Ad Hoc comes from the detail that there is no fixed infrastructure for sending or routing the packages. Generally there are a variety of types of exclusively designated systems readily available. These kinds of are depending on the subsequent such as MANET, WSN and VANET.

In our paper we mainly focus on MANET frameworks. A Mobile Ad hoc Network is a compilation of self-governing mobile nodes that can converse to each other via radio waves. The mobile nodes that are in two-way radio range of each other can nonstop communicate, whereas others need the aid of midway nodes to route their packets. Each of the nodes has a wireless boundary to communicate with each other. These networks are fully dispersed, and can work at any place without the help of any fixed communications as access points or base stations. Below figure shows a simple ad-hoc system with 4 nodes. Node A and node C are not inside range of each other; however the node 2 can be used to forward packets between node A and nodes B The node B will act as a router and these four nodes mutually form an ad-hoc network.

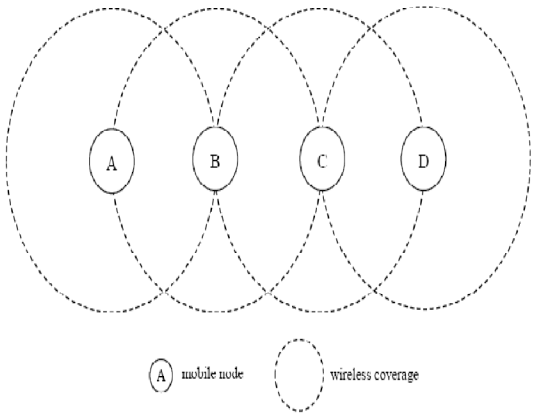

Fig. 1. Mobile Adhoc Network.

There are several challenges in MANET network which are given as:

1 There are no specific central points anywhere the data collection could be completed at.
2 Mobile Adhoc Networks routing protocols depend on the transitional nodes that in turn makes quite easy for the invaders to create incursions.
3 As Mobile Adhoc Networks are moveable that means there is no permanent topology, for the intrusion detection process.
4 Mobile nodes frequently will have restricted power, memory, restricted computing abilities, and so on. This also creates the Identification procedure multifaceted and complex.

In a network where there is no specific standards to judge the legitimacy of a particular node, any device could enter as well as exit the network on their own wish. Mobile Adhoc Networks in their elementary form, do not show any limitation on any kind of mobile device in the direction of preventing it from linkingwith the network. MANETs does not have a central authority that col control its functioning. In such free environments, an intruder node could join the network quite easily.

Depending on the type of attack, the invader could probablydamage the network in several manners. While a lone physical device takes on numerous forged individualities in a single network, it is known as Sybil attack. The attacking node could possiblyact as multiple i.e. more than one physical device, consequently fooling the additional nodes.

In the meantime, there is no principal authority towardscertifyingthat one specific physical entity is bound by only one specific identifier, an attacker could take as numerous identities as it desires. An invader can counterfeit identities in two different manners [1].

The First one is that the invader utilizes just one specific fake identity at a specific time for communiqué with the rest of the network. This false identity is rejectedsporadically and a new one is occupied. The procedure is reiterateduninterruptedly and consequently at a specific time, just one fake identity of the attacker is active in the network. This is entitledas non- simultaneous type of Sybil attack. In the second type of Sybil attack, the invaderinterconnects with the network utilizing all of its counterfeit identities at the same timeacting as numerous devices. It directs packages through these false identities concurrently by travelling through them recurrently. Such kind of attack is known as Simultaneous Sybil Attack.

Hence the overall problem of this research work is to prevent the network from Sybil attack at the network server using DSR protocol and Neural network algorithm. The research work also includes evaluation of the QOS parameters like throughput, bit error rate, and energy consumed.

II. SYBIL ATTACK

Sybil attack is a kind of security risk when a hub in a system guarantees various characters. It is an attack wherein a reputation system is subverted by forging identities in peer-to-peer networks. The Sybil nodes in a Sybil attack are connected to the honest nodes via attack edges. Attack edges are difficult for Sybil nodes to create and hence they are few in number.

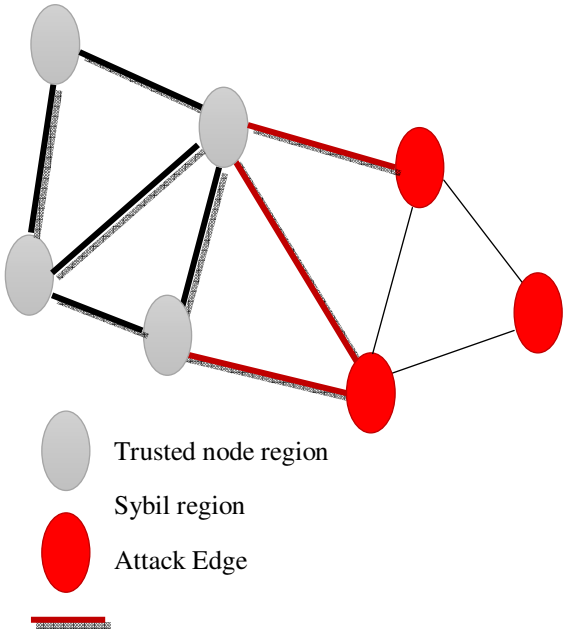

Fig. 2. Sybil Attack.

It leads to Sybil nodes and honest nodes being completely isolated and connected together by a few attack edges. From a trusted node, there are a number of random paths with fixed length known as verifiers. The Sybil guard checks a suspected node by sending random paths from the suspected node. If the random path intersects with verifier then the suspected node is said to be verified once. After the node is verified a particular number of times, the suspected node is said to be trusted node otherwise it is said to be a Sybil node [2].

A. Countermeasure against Sybil Attack

1. Trusted certification: This type of approach assumes in which there is a distinct trusted third party otherwise principal authority that could authenticate the validity of every single participant, as well as further issues a trusted certification for the authentic one [1]. In actuality, such kind of trusted certification could be a distinctive h/w device [3] or else a digital numeral [4]. Note that fundamentally together both of them are a sequences of numerals present on distinctive medias. Beforehand, a contestant joins a peer-to-peer framework to offer votes otherwise towards acquiring its services, his individuality must be tested first [5].
2. Sybil Guard: The Sybil nodes occur in a Sybil attack which are associated to the authentic nodes through attack edges. Attack edges are problematic for Sybil nodes to generate and henceforth they are insufficient in amount. It leads in the direction of Sybil nodes as well as authentic nodes being absolutely remote as well as linked together by a limited attack edges. After a reliable node, there are a amount of arbitrary routes with some particular length which are acknowledged as verifiers. The Sybil safeguard checks a mistrusted node via directing unsystematic paths from the mistrusted node. If in any condition, the arbitrary path interconnects with verifier then the mistrusted node is assumed to be tested once. Afterwards the node is substantiated a specific number of times, the distrusted node is supposed to be trustworthy node or else it is said to be a Sybil node [6].

III. RELATED WORK

Manjeet Singh [7], 2013 A MANET is an infrastructure-less network that comprises of number of mobile nodes with wireless network interface In order to make message among nodes, the nodes animatedly institute paths among one another. The natural history and structure of such networks makes it gorgeous to various types of attackers. Security is a main concern for protected message between mobile nodes. MANET has no clear line of protection, so, it is accessible to both genuine network users and malevolent attackers. In the corporation of mean nodes, one of the main challenges in MANET is to design the robust security solution that can protect MANET from different routing attacks. MANET can operate in segregation or in bringing together with a wired infrastructure, often through an opening node participating in both networks for travel relay. This elasticity, along with their self-organizing capabilities, is some of MANET's major strength, as well as their main security weakness.

Brian Neil Levine *et.al* [25], 2006 in this document, we survey the crash of the Sybil attack, an attack against individuality in which a personality entity masquerade as multiple concurrent identities. The Sybil attack is a basic problem in many systems, and it has so far resisted a generally appropriate solution.

Simranjeet Kaur [8], 2014 In previous work, MANET is definite as the "collection of mobile nodes, communicate with each other by the wireless links". It is a demanding task to achieve security in a Mobile ad hoc network due to its wireless natural history, lack of communications and its topology which changes animatedly. Due to its wireless nature there are lots of attacks which can create lots of evils in the MANET. Among a variety of attacks there is a Sybil Attack which is very destructive for mobile ad hoc network. In this attack a malevolent node obtain multiple identities at a time and increases lot of misjudgements among the node of the network or it may access the characteristics of the other justifiable nodes and create false expression of that node in the network.

Kasiran and Mohamad [9], 2014 performed a performance analysis which shows that the throughput in case of presence of Wormhole attack and Sybil attack is decrease than that in the presence of such a node. However, in this parameter Sybil attack give more impact of performance of MANET rather than wormhole attack. The experiment has shown that at node 100, there is not much different in the throughput performance in both Sybil and wormhole attack. Comparing to the experiment with 20 nodes and 60 nodes, performance of the Sybil attack is much lower than the wormhole attack.

Sinha, S. *et.al,* [10], 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 attack 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.

Piro *et.al,* [11], 2006 anticipated to discover Sybil identities through witnessing node undercurrents. Nodes are observance pathway of identities that are very frequently seen together (Sybil identities) as contrasting to the authentic separate nodes which usually transport without obstruction in dissimilar directions. Conversely, the structure will harvest great false positives wherever node density is extraordinarily high, for instance a conference hall or nodes travels in a similar direction, for example an assembly of soldier going in the direction of a target.

D. B. Jagannadha Rao *et.al* [12] have defined the standard procedure of Route Discovery as well as Route Maintenance utilizing DSR. In this, it is revealed by what means they permit wireless movable nodes to mechanically form an entirely self-establishing utilizing DSR. The objective is to generate an assimilated set of procedures which gives permit to mobile computers, as well as the applications which are running on them and also can easily interconnect with each one of other. A study of DSR protocol is as well done .A set of rules is suggested by utilizing ACK reply pathway as a backup path as soon as an original route flops in Mobile networks. In the old-style DSR protocol, a backup route utilized to relocation information the minute a route is wrecked. If the backup route unsuccessful at that time it will also affect the whole network performance of the network. Amend the DSR supposed to be Modified DSR protocol (MDSR) by means of the ambition that the base node be able to accept the ACK response from target node the minute an original route is wrecked, that means data packets are able to be relocated alongside by means of the ACK path. The procedure lessens the waiting time of information broadcast in advance of the actual route is re-created as the packet delivery ratio will possibly be enhanced. Consequences exhibited that the novel protocol has much enhanced performance than the DSR protocol.

Po-Wah Yau *et.al* [13] gives the components to trusting routers and relay as it talked about the issues included in utilizing reputation as a part of Adhoc systems.

Like if a hub is malicious then the working together hub should not with them in the event that it so then entire system will collapse.

S. Marti *et.al* [14] talks about the impact of malicious hub conduct and gives an answer on the basis of reputation mechanism. Firstly, it examines the two different scenarios & then thought about them. On the premise of this it gives an answer for investigating the different values and computing the different values. Reputation system is likewise utilized in the restricted system where both positive & negative conduct is extremely influences the reputation values. It arranges the hubs into diverse situations a danger model for Ad hoc directing routing were depicted.

IV. STIMULATION MODEL

The simulations were carried out by using MATLAB as the language that we use to develop the proposed framework. In the simulation the following steps are to be followed by user:

Step 1: Firstly initialize the network by entering the number of nodes as well as implement Dynamic Source Routing protocol on the network.

Step 2: Then the source and destination is chosen by the network and a network is deployed.

Step 3: After this, number of rounds will run showing different optimal path according to distance for the network.

Step 4: Then a graph is plotted by the user.

Step 5: Then the Sybil attack which produces the number of multiple copies in the network which increases the load as well as some of the data packet is dropped due to Sybil attack in the network.

Step 6: If packet dropping condition take place and some packets are lost. And if not then send it to the chosen destination.

Step 7: Then, Plot graph for proposed parameters.

Step 8: Call neural network for optimization purpose.

Step 9: Then, again Evaluate parameters and plot graph with optimized network nodes. The specific parameters used are throughput, energy optimization, error rate and end to end delay.

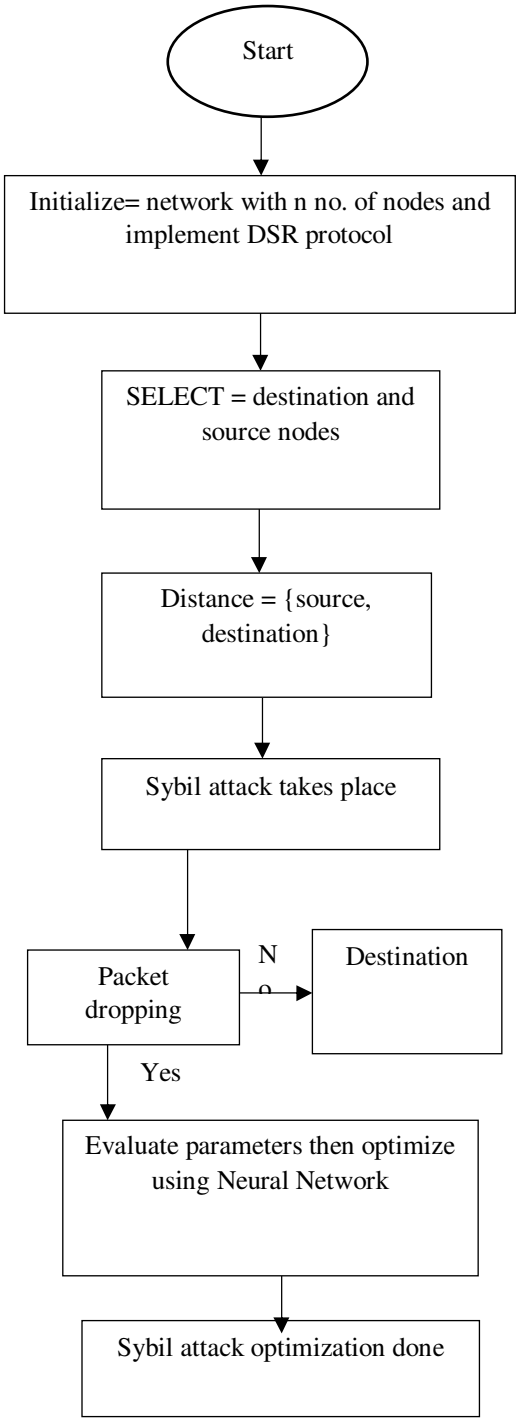

Fig. 3. Flowchart of Proposed Work.

RESULTS

SNAPSHOTS

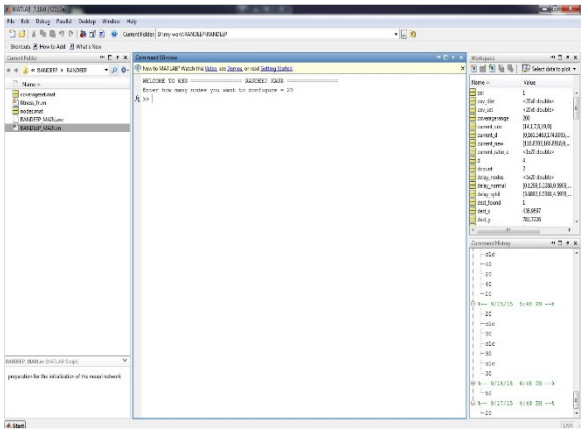

Fig. 4. Main GUI.

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. Once we have entered the Node deployment process start using DSR protocol as we can see in next figure.

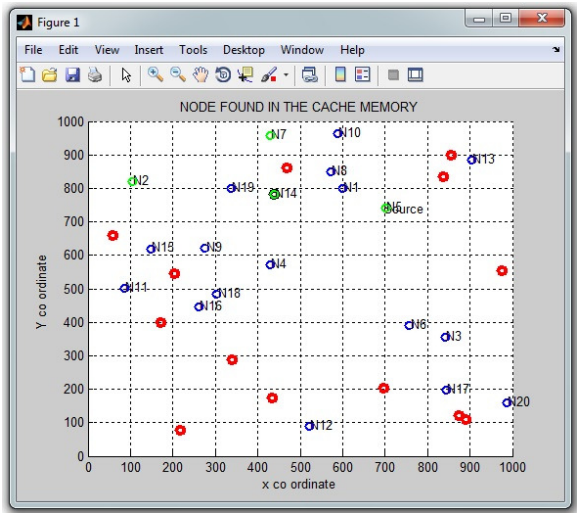

Fig. 5. Network deployment, Sybil attack representation and node found in cache memory.

Above figure, initially the network simulation model is formed which contains 20 nodes as given input and. 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 number of rounds to get accurate value of Sybil nodes.

Initially, it searches nodes in network, then after this source is plotted in the network just after that Sybil Attack take place in the network and then we have Sybil attack nodes that has been found in cache memory as shown in above figure. In above figure, red represent Sybil attack nodes, green represent several alive nodes, and blue represent left out normal nodes.

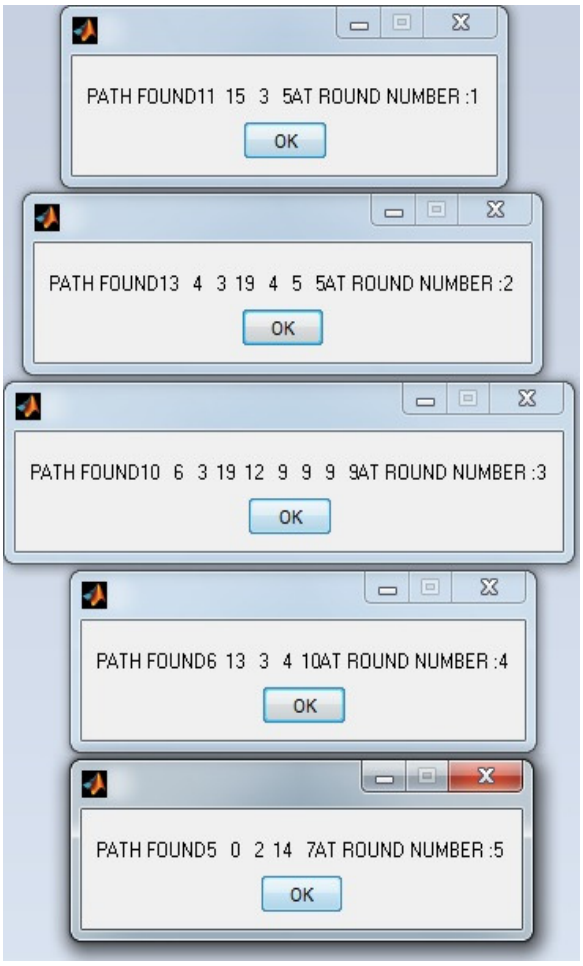

Fig. 6. Path Found and Round Number.

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

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

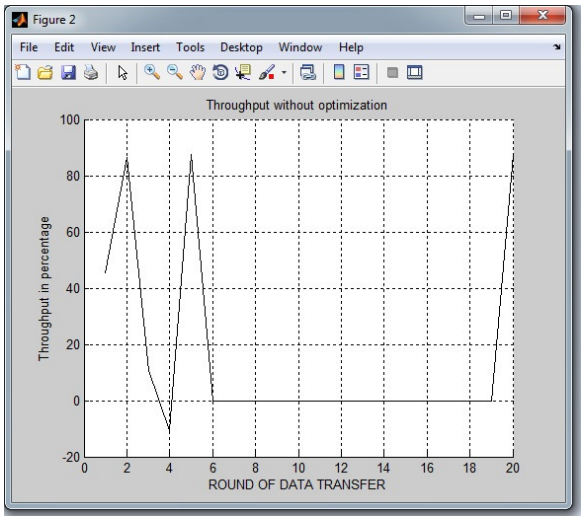

Fig. 7. Throughput without optimization.

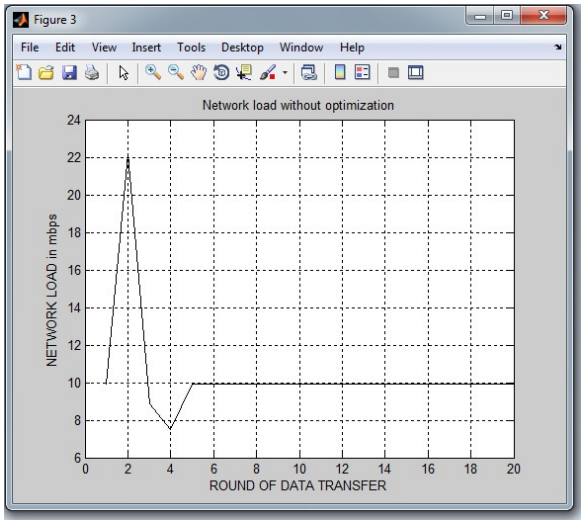

Fig. 8. Network Load without optimization.

In above figure, we have shown a graph showing how network load when Sybil attack is introduced network load increases with increase in round of data transfer increment. A graph is plotted between network load and round of data transfer. 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.

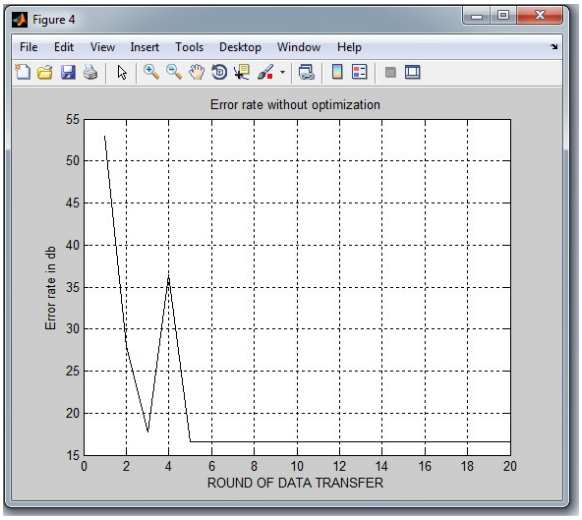

Fig. 9. Error Rate without optimization.

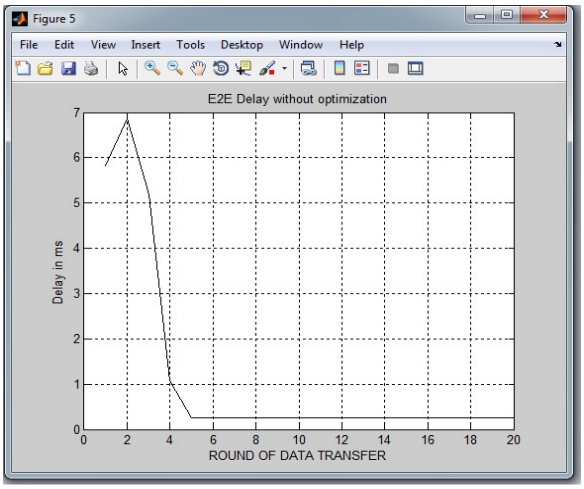

Fig. 10. End to End Delay without optimization.

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 vehicles in the network.

In figure, we have applied neural network training on the affected network to optimize the network nodes.

The Sybil attack nodes causes decrease in the throughput of the network. It is because number of collisions is more in system and it is optimized using NN algorithm as shown above. Above figure shows that throughput value with NN. At 5th round it gives throughput value around 95 as shown in above.

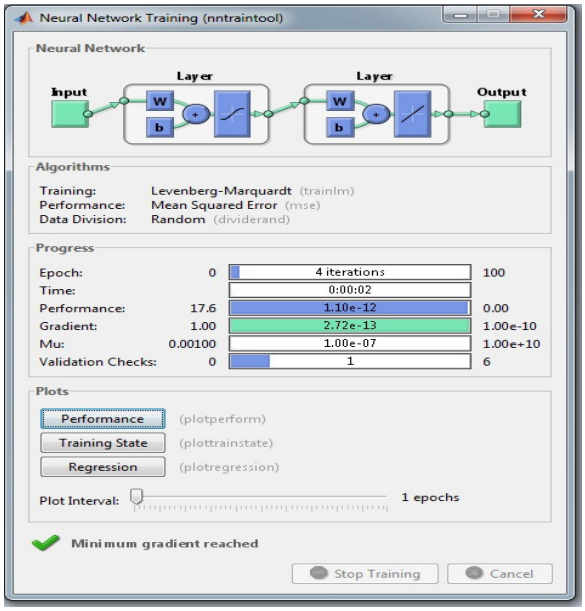

Fig. 11. Neural Network training applied on the affected network.

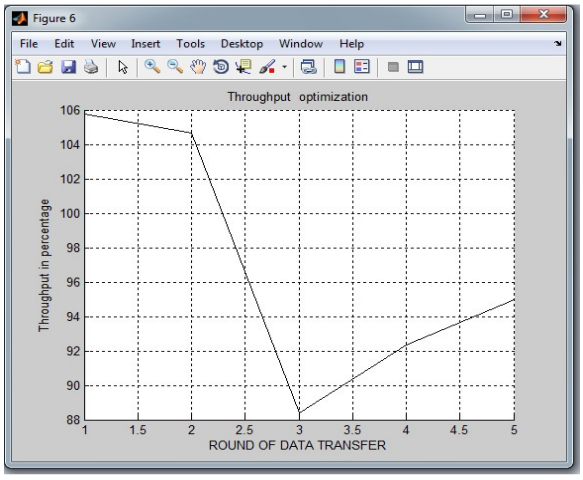

Fig. 12. Throughput with optimization using Neural Network.

In figure, we have shown a graph showing how energy consumption increases when Sybil attack is introduced in the network with increase in round of data transfer increment. A graph is plotted between energy consumption in Joules and round of data transfer. Above figure shows that energy consumption value with NN. At 5th round it gives energy consumption value around -2.

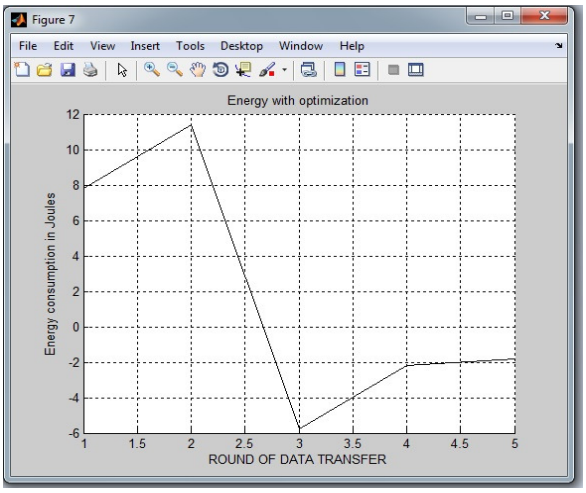

Fig. 13. Energy Optimization using NN.

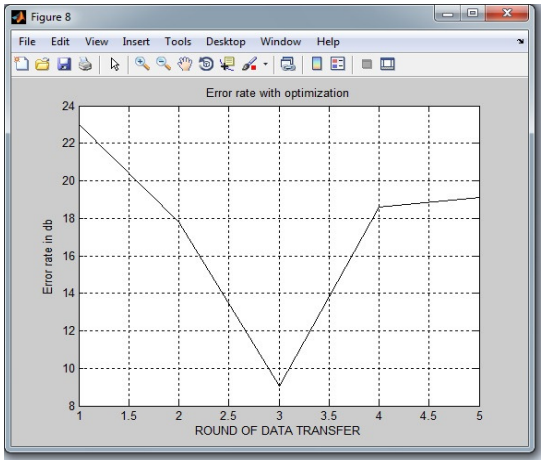

Fig. 14. Error rate optimization using NN.

As above figure shows that error rate increases constantly but when Sybil attack occurs then it increase rapidly as shown. But when we utilize NN algorithm for optimization the error rate decreases. Above figure shows that error rate value with NN. At 5th round it gives error rate value around 19. Above figure shows the end to end delay with NN. This increase in delay is due to the congestion nodes through which then passes to the destination node. However increase in the numbers of nodes also increases the difference of delay. The End to End Delay is a significant parameter for evaluating a protocol which must be low for good performance. Above figure shows that End to end delay value with NN. At 5th round it gives End to end delay value around 2.2.

COMPARISON GRAPH

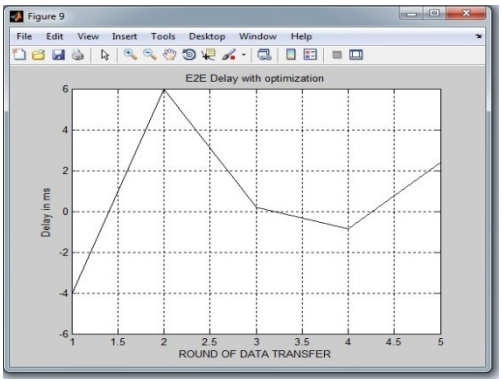

Fig. 14. End delay optimization using NN.

Table 1: Various Parameter Table.

Parameter for 5th rounds	**Without Optimization**	**Neural network Optimization**
Throughput	80	95
Energy Consumption	10	-2
Error rate	20	19
End delay	0.5	2

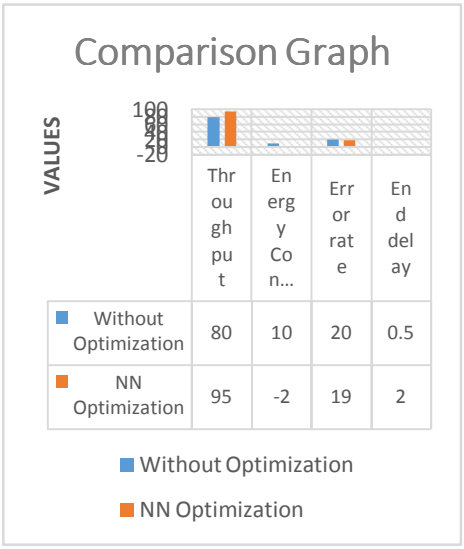

Fig. 15. Comparison Graph between without optimization and after applying NN optimization.

In above table we have shown the value of various parameters on specific 5th round on without optimization and after applying NN optimization.

In above comparison graph, we have shown results on the basis of specific parameters such as throughput, energy consumption, bit error rate, and end delay and compared the results of network with existence of Sybil attack and results of optimized network with existence of Sybil attack.

CONCLUSION AND FUTURE SCOPE

MANET is susceptible to numerous attacks because of its infrastructure less nature and in the direction to have secure and protected Communication and transmission it is requisite be safe network. It has been observed that Sybil attacker has reduced the Throughput and increased the End to End Delay as well as energy consumption of the network. In Sybil attack, it utilizes numerous identities of additional node existing in the network to interrupt the data transmission as well as it also lessen the trust of authentic nodes present in the network.

In this thesis, we advance a simple protocol named as Dynamic Source Routing protocol using neural network optimization on the network which is affected by Sybil attack. In this first we run the system by applying Dynamic Source Routing protocol, and once Sybil attack occur in the network then we will apply neural network for optimization purpose which will remove fake individualities/ nodes from the specific network. And results have been evaluated after sybil attack occurs inside the network as well as after Neural network optimization is applied on the network utilizing specific parameter such as: throughput, energy consumption, end to end delay and error rate. Later, we compared these results using graph as shown in result section. The whole stimulation work is done utilizing mat lab software.

In future work, we can apply BFO or GA with DSR routing protocol or we can use different protocol with neural network like AODV, DSDV etc. and implement it on network with the existence of Sybil attack to get better and enhanced results

REFERENCES

[1]. Newsome, J., Shi, E., Song, D., Perrig, A., "The Sybil Attack in Sensor Networks: Analysis and Defenses," presented at the *3rd Int. Symp. Information Processing in Sensor Networks (IPSN),* pp. 259–268, 2004,

[2]. Gangandeep, Aashima, Pawankumar "Analysis Of Different Security Attacks In MANETs On Protocol Stack A-Review", *International Journal of Engineering and Advanced Technology (IJEAT)* ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012.

[3]. W. Chang and J. Wu, "A Survey of Sybil Attacks in Networks", Sensor Networks for Sustainable Development, M. Ilyas (ed), CRC Press.

[4]. J. Ledlie and M. Seltzer, "Distributed, secure load balancing with skew, heterogeneity and churn," in Proc. of IEEE INFOCOM, vol. **2**, 2005, pp. 1419–1430.

[5]. J. Douceur, "The sybil attack," Peer-to-Peer Systems, 2002.

[6]. H. Yu, M. Kaminsky, P. B. Gibbons, A. Flaxman, "SybilGuard: Defending Against Sybil Attacks via Social Networks", SIGCOMM'06 ACM, 2006.

[7]. Manjeet Singh et.al," A Surveys of Attacks in MANET", *International Journal of Advanced Research in Computer Science and Software Engineering,* 2013.

[8]. Levine, Brian Neil, Clay Shields, and N. Boris Margolin. "A survey of solutions to the sybil attack." University of Massachusetts Amherst, Amherst, MA (2006).

[9]. Simranjeet Kaur et.al "Defending mechanisms against Sybil attack in next generation mobile ad hoc networks." IETE *Technical Review* 25.4 (2014): 209-215.

[10]. Zolidah Kasiran and Juliza Mohamad (2014), "Throughput Performance Analysis of the Wormhole and Sybil Attack in AODV", *2014 Fourth International Conference on Digital Information and Communication Technology and it's Applications (DICTAP), IEEE,* pp.81-84.

[1]. Somnath Sinha, Aditi Paul, and Sarit Pal, "The Sybil Attack in Mobile Adhoc Network: Analysis and Detection" in Conf. Rec. IEEE 2013.

[1]. C. Piro, C. Shields, and B. N. Levine, "Detecting the Sybil attack in mobile ad hoc networks," in *Proc. Secure comm Workshops*, 2006, pp. 1–11.

[1]. D. B. Jagannadha Rao(et.al), "A Study on Dynamic Source Routing Protocol for Wireless Ad Hoc Networks" , International *Journal of Advanced Research in Computer and Communication Engineering,* Vol. **1**, Issue 8, PP.522-529,October 2012.

[1]. Po-Wah Yau and Chris J. Mitchell, "Reputation Methods for Routing Security for Mobile Ad Hoc Networks".

[1]. James Newsome, Elaine Shi, Dawn Song and Adrian Perrig, "The Sybil Attack in Sensor Networks: Analysis and Defenses" IPSN"04, April 26-27, 2004, Berkeley, California, USA.