A Novel Hybrid Approach of Neural Network and AOTDV for the Detection of Sybil Attack in Ad-hoc Network

Er.Sushil Lekhi[1],Gurjeet Kaur[2]
[1]Assistant Professor,[2]M.Tech Student
[1,2]Department OfComputer Science and Engineering, Rayat Institute of Engineering and Information Technology, Railmajra, S.B.S. Nagar, (Punjab), India
[1]lekhi.engg@gmail.com, [2]waheguru.gurjeet@gmail.com

***ABSTRACT*— Recent advances in information technology has made it possible to transmit the data in wireless -links without the aid of any fixed infrastructure or centralized administrator. Wireless ad hoc networking is a technology that allows fast, easy and inexpensive network deployment. Unfortunately, the advantages of wireless networks also make the task of an attacker simpler, as it is also becomes easier to deploy a malicious node in the environment. There are many attacks which ruin the communication among the nodes of network. Among those attacks there is a Sybil attack that causes severe hazards to the network. Here, we focus on the detection and prevention methods of Sybil attacks on the ad hoc network. In a Sybil attack a malicious node can generate and control a large number of logical identities on a single physical device. The identities used by Sybil attackers are either created by it or uses someone else's identity. In this paper, we are applying the integrated concept of Neural Network for the Sybil attacks detection and AOTDV (Ad-Hoc on demand trust based Distance vector) Protocol in multi routing using Link Share Technique to prevent these fake identity attacks.**

***KEYWORDS*— AOTDV, Ad hoc On demand Distance Vector, Sybil Attack, Neural Network, Ad hoc Network.**

I. INTRODUCTION

Wireless ad hoc networking is a technology that allows for fast, easy and inexpensive network deployment. Ad hoc networks are substantially different from infrastructure wireless networks, where nodes never communicate directly amongst themselves and all communication is performed via specialized nodes known as Access Points. Despite their known limitations in terms of scalability and overall capacity [1], the decentralized nature, minimal configuration, and self-healing abilities of wireless ad hoc networks, makes them suitable for a variety of situations like search and rescue operations, recovery from natural disasters, or military conflicts.However, quorums may easily be defeated if a single adversary can participate in the network with multiple identities, a behaviour known as the Sybil Attack [2]. Therefore, finding efficient techniques to defeat the Sybil Attack is fundamental to build secure wireless ad hoc networks. This is the problem addressed in this work.This research work addresses security issues on wireless ad hoc networks, with special emphasis on the Sybil attack. A Sybil attack is essentially an impersonation attack, in which a malicious device illegitimately fabricates multiple identities, behaving as if it were a larger number of nodes (instead of just one) [3]. A malicious device multiple identities are referred to as Sybil identities or Sybil nodes. According to the taxonomy presented by Newsome et al (2004), there are three possible orthogonal dimensions for this attack: direct vs indirect communication; fabricated vs stolen identities; and simultaneity. In the worst case, an attacker can create an unlimited number of Sybil identities, with only one malicious device [4].In this paper, we have proposed an integrated approach of Ad hoc On demand Trust based Distance Vector and Neural Network for the detection of Sybil attack in the ad hoc network. The neural network learns dynamically on the fly and gives accurate results to isolate out the network nodes suspected of malicious behaviour[5]. AOTDV finds the first k shortest trusted paths are computed out as candidates during one route discovery [6].The rest of the paper is discussed in the following manner: Section II describes the basic concepts involve on the integration of AOTDV and Neural Network. Section III presents the concept of hybrid AOTDV & Neural Network. Section IV discusses about the results and comparison part. Section V concludes the paper.

II. BASIC CONCEPTS

To propose the hybrid algorithm, the concepts of AOTDV and Neural Network are considered that are discussed here.

A. AOTDV

In this protocol, a source can establish multiple loop-free paths to a destination in one route discovery process. Each path has an evaluation vector composed of a hop count and a trust value. A destination will respond with at most k shortest paths as candidates that satisfy the trust requirements of data packets. The shortest one will be selected as the forwarding route. As an intelligent agent, each node evaluates its neighbours' behaviours and selects the shortest trusted path to forward packets [7].

B. Artificial Neural Network

Artificial Neural Networks are the network systems that have the capability to work like human beings. McCulloch and Pits has produced the first artificial neuron in 1943 [8]. In ANNs, Neurons are the building blocks of the concept. ANNs have the feature to process the distributed information into parallel processing techniques. The features and performance of these ANNs is similar to that of nervous system.The key parameters of ANNs are elements of Artificial Neurons (also known as simply neurons), pattern of connectivity among neurons (architecture of ANNs) and method to determine the weight value (known as learning algorithm). ANNs have the

capability to solve any computational problem due to its features to work like human brain like neurons, so it can also be termed as *neurocomputer*.The major applications of ANNs are in the field of Remote Sensing, Cryptography, Robotics, Clustering, Pattern Recognition, Weather Forecasting, Gaming, Signal Processing, Biometric Recognition etc. [9][10]. It can also be applied to any problem having no any strict predefined rules for the problem definition.

III. PROPOSED ALGORITHM

This work proposes to develop a Sybil attack detection system for Ad Hoc network, based on Neural Network. In this Hybrid concept, we have considered the routing protocols of AOTDV and Neural Network. The AOTDV (Ad-Hoc On-Demand Trust based Distance Vector) routing protocol is a reactive routing protocol that uses some characteristics of proactive routing protocols. Routes are established on-demand, as they are needed. However, once established a route is maintained as long as it is needed. Reactive (or on-demand) routing protocols find a path between the source and the destination only when the path is needed (i.e., if there are data to be exchanged between the source and the destination). So in this proposed concept, AOTDV is combined with Neural Network. This proposed algorithm is structured as below:

Step1: Create a group of mobile nodes and One of the nodes is taken as base station.
Step 2: The base station sends DATA packets to all the other nodes for topology verification which are present in the sensor range. Apply the routing criteria of AOTDV.
2.1: Before a source 's' send a data packet to another node, say node 'd', the source looks up in the local routing table 'a' route entry to node 'd'. The qualified route should meet the trust requirement of the data packet. In other words, PathTrust of the qualified route is greater than the requirement of the data packet. If such routes are found, go to step 2.3.
2.2: If there is not such a route, node's' initiates a route discovery for d. If one or more paths are discovered, a route entry for these paths will be created and inserted into the routing table of node s.
2.3: Node's' selects the route with the smallest hop count in the qualified routes.
2.4: If not a qualified route is selected, node s will return no qualified routes.
2.5: If a qualified route is selected (assume that the selected next hop is node n), node s increases NA for node n by 1, inserts the data packet into its trust record list, sets its retry counter to 0 and sends the packet. And then node s listens to the radio channel and checks whether the packet will be forwarded correctly by node n.
2.6: If the packet is forwarded correctly by node n, node s increases NC for node n by 1 and removes the packet in its trust record list. The procedure is over.
2.7: If the packet is not forwarded correctly and its retry counter is less than 1, node s will increase the counter by 1 and retransmit the packet to node n.
Step 3: The node which receives highest packets is chosen as the trust nodes.
Step 4: The trust nodes now become the head nodes with a group of its own member nodes.
Step 5: The member nodes send their ID and power value to the head nodes.
Step 6: The head node checks for nodes with energy value below the threshold value.
Step 7: Apply the concept of Neural network along with AOTDV. The network consist of 3 input neurons, 2 hidden layer and 1 output layer and Feed Forward Back Propagation is selected as network type.
Step 8: If the energy value is lesser than the threshold value, those nodes are detected as Sybil nodes and look for other valid routes in the routing table. Go to step 2.2.
In malicious nodes detection, if the node trust of a neighbour is smaller than the black-list trust threshold h, the neighbour will be regarded as a malicious node, and then be moved into a black list. In particular, every node maintains a local black list. A malicious node in a black list is excluded by its neighbour holding the black list. That is, the packets from a malicious node will not be forwarded by the neighbour; meanwhile, the neighbour will not send packets to the malicious node except broadcast packets. If a node is evaluated very low by all its neighbours, any reply it gives to route requests is discarded, and any request it initiates is ignored.

IV. RESULT & COMPARISON

This section examines the performance of the proposed algorithm. It also provides a performance comparison between proposed algorithms and the existing one.

A. Experimental Setup

The experimental setup is done to detect the attack of the hacker, if found any then with the help of AOTDV algorithm IP address is changed and finally path changed. Network size of 10 and 20 nodes is considered. At each iteration change in time for the sending and receiving of packet is calculated.

B. Sybil Attack Detection

Sybil attack detection process is shown by figure 4.1 to 4.3.

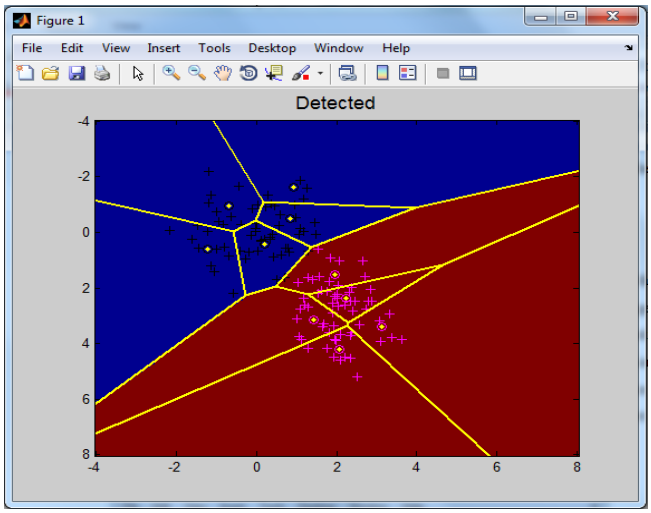

Figure 4.1: Sybil attack detected at initial stage in upper yellow color dots

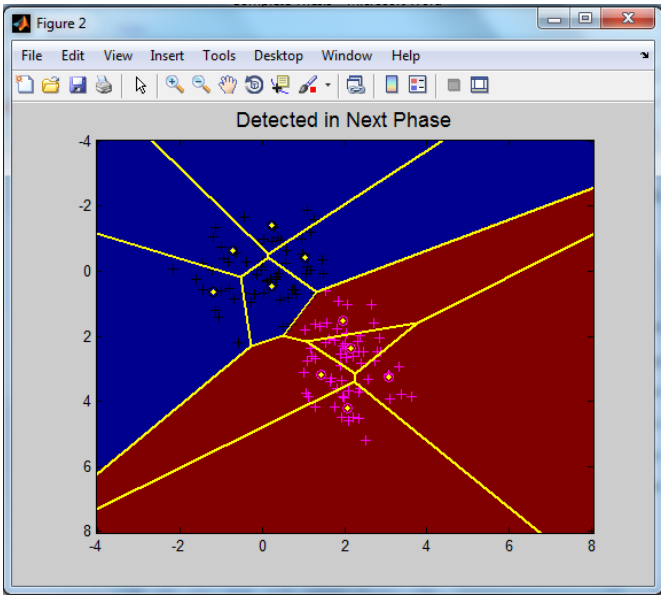

Figure 4.2: Sybil attack detected at next stage of AOTDV in upper yellow color dots

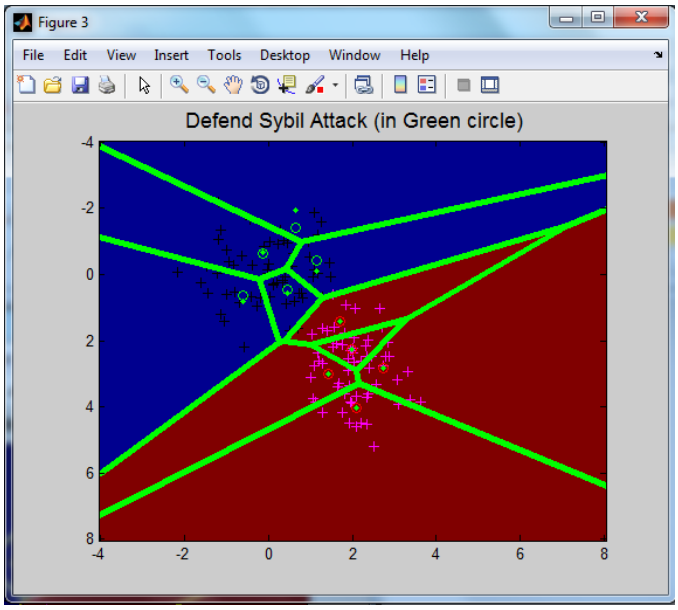

Figure 4.3: Sybil Attack defended as shown by green upper circles

C. Sybil Attack Prevention

Sybil attack Prevention process is shown by figure 4.4 to 4.6. Here, prevention by all the three different concept is shown:

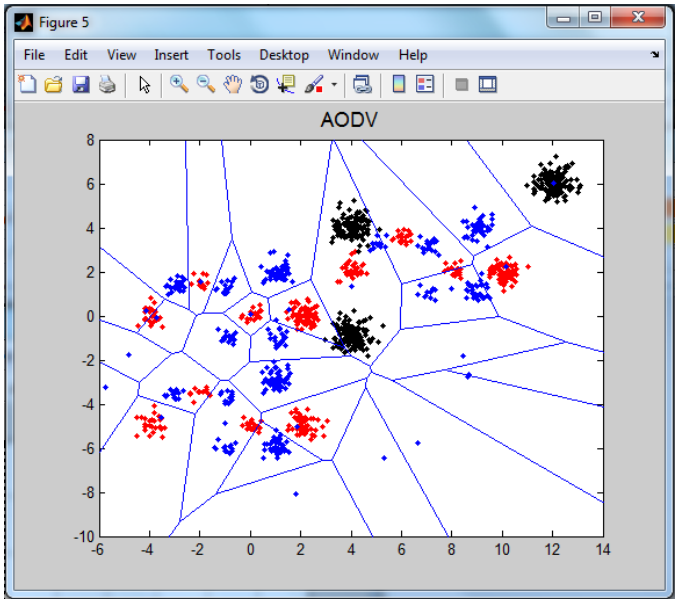

Figure 4.4: Sybil Attack prevention by AODV.

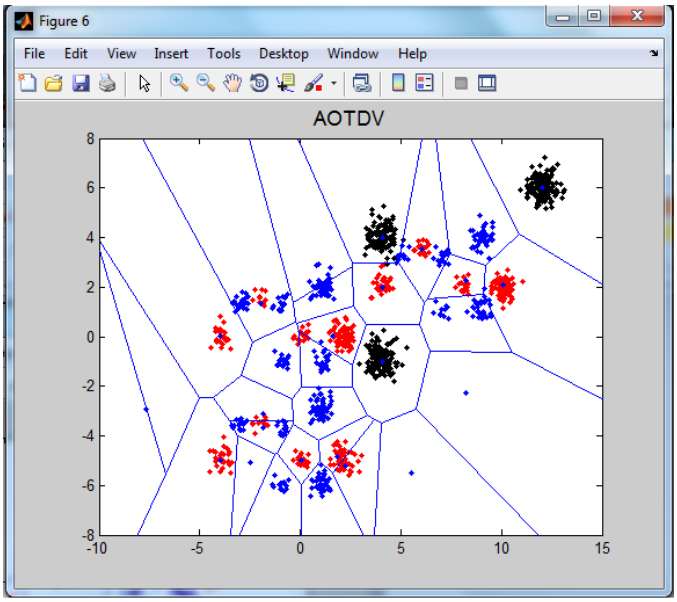

Figure 4.5: Sybil Attack Prevention by AOTDV

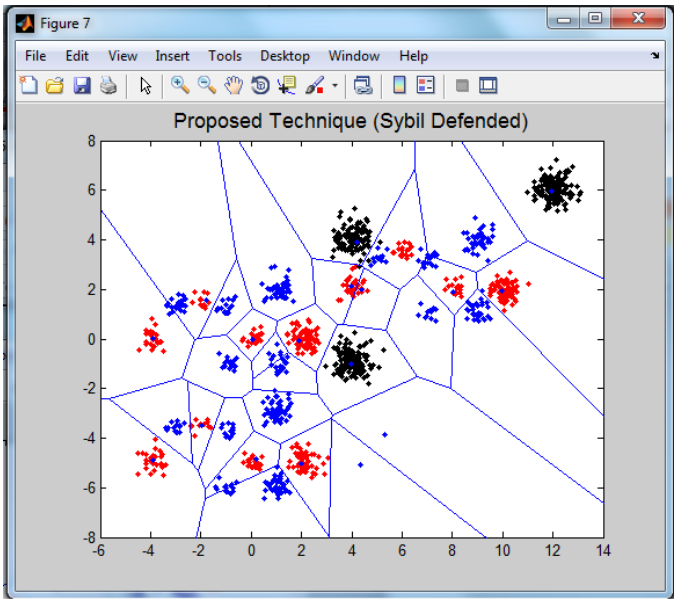

Figure 4.6: Sybil Attack defended by Proposed technique.

D. Evaluation Parameters

To define the accuracy of proposed algorithm, we are defining parameters of Accuracy and Routing Attack Cost These terms are defined for the comparison with simple AODV and AOTDV routing Protocol.

- **Accuracy:** Accuracy can be defined as a measure to detect that how precisely system is generated to detect the Sybil attack.
- **Routing Attack Cost:** It can be defined as ratio of the number of detected attacks for the sending packets in network.

E. Comparison with AODV and AOTDV

To check the accuracy of our proposed algorithm, we have considered the concepts packet transfer from the routing protocol of AODV. The comparison results are shown by figure 4.7 and table 4.1.

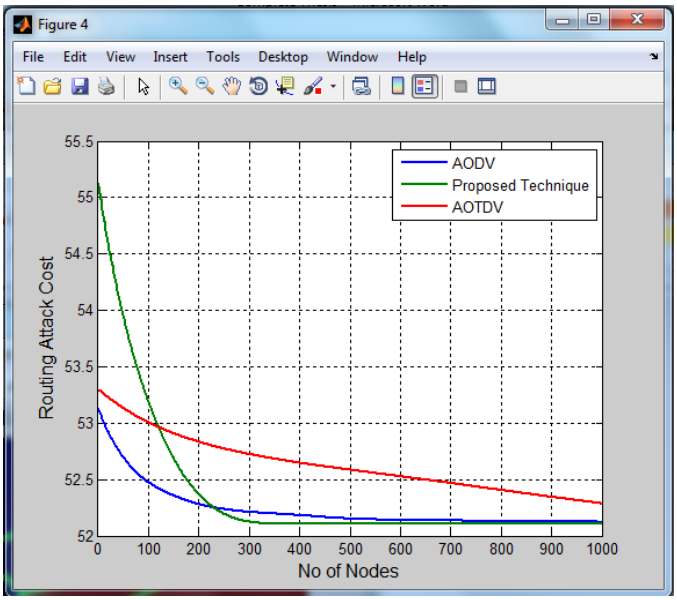

Figure 4.7: Comparison on the basis of Sybil attack detection cost

Table 4.1
Accuracy of AODV, AOTDV, and Proposed Concept

Technique	Accuracy
AODV	0.8926
AOTDV	0.9306
Proposed Concept	0.9398

From the comparison results of figure 4.7, and table 4.1, we can say that our proposed Hybrid neural network based AOTDV concept performs better as compare to simple routing protocol of AODV and AOTDV.

V. Conclusion

The aim of the thesis was to detect and prevent the Sybil attack that interrupts the transfer of routing packets. The proposed algorithms in this research work has successfully completed the all these objectives by giving verification results in the form of evaluation parameters of Accuracy and Routing Attack Cost. We also have shown the proposed algorithm gives better results from AODV and AOTDV routing protocol by showing the graphical representation as shown in figure 4.7 and in table 4.1.The proposed method not only identifies the attack, it also identifies the attack and successfully prevents them. This proposed system provides

the noble solution and identify the attack is clearer by using the neural network technique.

REFERENCES

[1]. Haas, Z. J., Deng, J., Liang, B., Papadimitratos, P., & Sajama, S. (2002). Wireless ad hoc networks. *Encyclopedia of Telecommunications*.

[2]. Douceur, J. R. (2002). The sybil attack. In *Peer-to-peer Systems* (pp. 251-260). Springer Berlin Heidelberg.

[3]. Hu, Y. C., Perrig, A., & Johnson, D. B. (2003, September). Rushing attacks and defense in wireless ad hoc network routing protocols. In *Proceedings of the 2nd ACM workshop on Wireless security* (pp. 30-40). ACM.

[4]. Piro, C., Shields, C., & Levine, B. N. (2006, August). Detecting the sybil attack in mobile ad hoc networks. In *Securecomm and Workshops, 2006* (pp. 1-11). IEEE.

[5]. Haykin, S., & Network, N. (2004). A comprehensive foundation. *Neural Networks*, *2*(2004).

[6]. Yan, Z., Zhang, P., & Virtanen, T. (2003, October). Trust evaluation based security solution in ad hoc networks. In *Proceedings of the Seventh Nordic Workshop on Secure IT Systems* (Vol. 14).

[7]. Li, X., Lyu, M. R., & Liu, J. (2004, March). A trust model based routing protocol for secure ad hoc networks. In *Aerospace Conference, 2004. Proceedings. 2004 IEEE* (Vol. 2, pp. 1286-1295).