International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 2 | ISSN : 2456-3307

Securing the Peers Against Sybil Attack Using Sybil Trust

Ponemaharani D, Siddique Ibrahim S. P., Kirubakaran R

Computer Science and Engineering, Kumaraguru College of Technology, Coimbatore, Tamilnadu, India

ABSTRACT

The work is based on networking to predict a trust to establish Peer to peer (P2P) e-commerce Electronic commerce or ecommerce is a term for any type of business, or commercial transaction that involves the transfer of information through the Internet applications exist at the other end of the Internet with vulnerabilities to passive and active attacks. The attacks occur using interactions between the trading peers as a transaction takes place. In this paper propose a Sybil attack, an active attack, it means some data is missing in transferring the data from one place to another place this is called active attack. And passive attack means data is not missing in transferring the data from one place to another place this is called passive attack. a central authority control is used in existing system. In this proposed system two techniques we are using Sybil trust central authority control and Homogeneous configuration. In this approach, duplicated Sybil attack peers can be identified as the neighbor peers become familiar and hence more trusted to each other. Security and performance analysis shows that Sybil attack can be minimized by this proposed neighbor similarity trust. Each peer has an identity, which is either honest or Sybil.

Keywords: Peer to peer (P2P), Sybil attack, active attack, passive attack.

I. INTRODUCTION

"Network security" refers to an activity designed to protect the usability and integrity of your network and data. It includes both hardware and software technologies. Effective network security manages access to the network. It targets a variety of threats and stops them from entering or spreading on your network. Network Security covers a variety of computer networks, both public and private, that are used in everyday jobs.

Peer-to-peer network is created when two or more PCs are connected and share resources without going through a separate server computer. It is a decentralized communication model. The P2P network, allows each node to function as both a client and a server. Sybil attack is an attack where a reputation system is subverted by forging identities in P2P networks. It is a type of security threat when a node in a network claims multiple identities. Sybil attack is an active attack, in which some data is missing in transferring the data from one place to another. Sybil Trust is a defence against Sybil attack in P2P e-commerce. It helps to weed out the Sybil peers and isolate malicious peers from Sybil peers. Here the proposed approach defines the duplicated Sybil attack peers can be identified as the neighbour peers become well known and hence more trusted to each other. Security and performance analysis shows that Sybil attack can be minimized by this proposed neighbour similarity trust.

In Existing system, mainly concentrates on social networks and trusted certification, has not been able to prevent Sybil attack peers from doing transactions. It is based on networking to predict a trust to establish P2P. Electronic commerce or ecommerce is a term for any type of business or commercial transaction that involves the transfer of information across the Internet applications exist at the edge of the Internet with vulnerabilities to passive or active attacks.

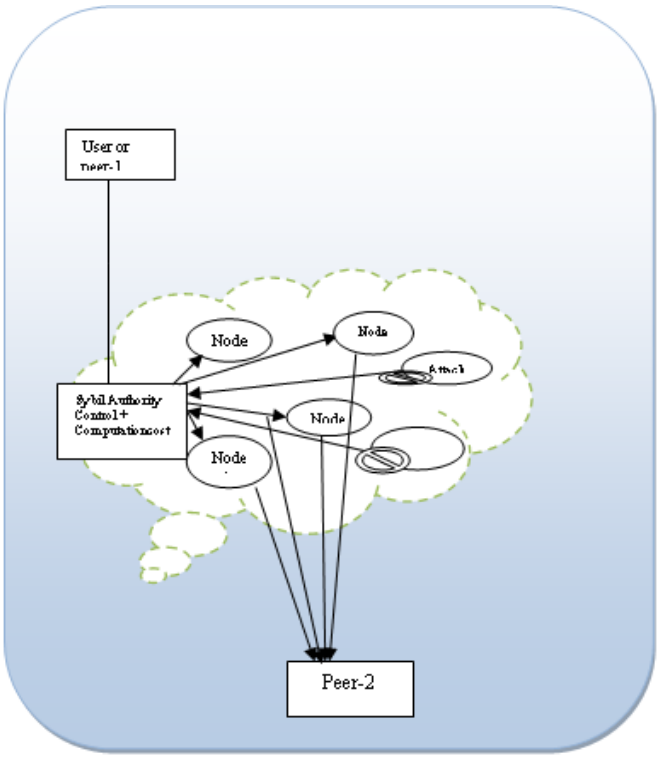
In proposed system, mainly focuses on active attack in P2P e-commerce. When a peer is compromised, all the information will be extracted. Sybil attack proposes active attack and passive attack. Active attack means some data is missing in transferring the data from one place to another place. Passive attack means data is not

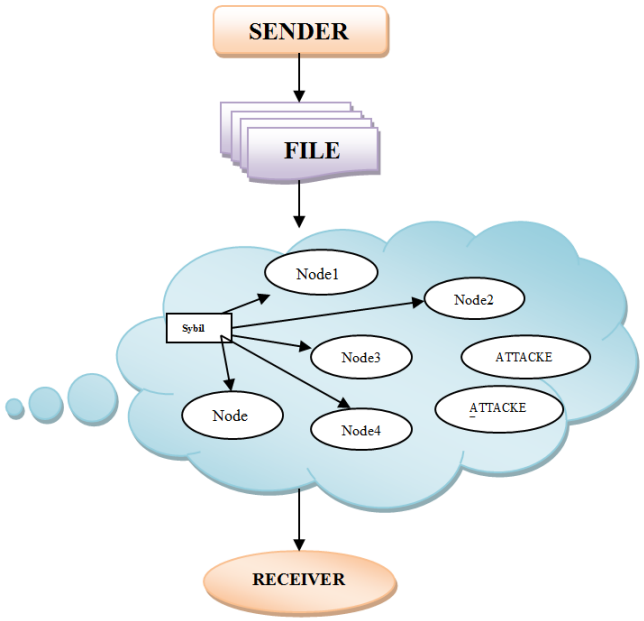
missing in transferring the data from one place to another place. Techniques used: Sybil trust authority control and Homogeneous configuration.

II. METHODS AND MATERIAL

SYSTEM DESIGN AND METHODOLOGY

System Architecture





Sybil Trust Central Authority Control:

The principal building block of Sybil- Trust approach is the identifier distribution process. In the approach, all the peers with similar behavior in a group can be used as identifier source. They can send identifiers to others as the system regulates. If a peer sends less or more, the system can be having a Sybil attack peer. The information can be broadcast to the rest of the peers in a group.

Advantages:

- Time consumption is determined by the process of Sybil trust.
- Ensure the peer connection to establish attack detection.
- Each Pear having the unique Key.

B. Flow Diagram

It does not show information about the timing of processes, or information about whether processes will operate in sequence or in parallel. In the DFDs the first sender can send data files on network.

III. RESULTS AND DISCUSSION

1. Implementation

A. Basic Description of Sybil Attack

Sybil attack is a dangerous digital world out there. Security and antivirus software is important for any network. One way security can break down is a Sybil attack. It is a type of security threat when a node in a network claims multiple identities. Most networks, like P2P network, rely on assumptions of identity, where each computer represents one identity. It happens when an insecure computer is hijacked to claim multiple identities. Problems arise when a reputation system is tricked into thinking that an attacking computer has a disproportionally large influence.

Similarly, an attacker with many identities can use them to act maliciously, by either stealing information or disrupting communication. It is important to recognize a Sybil attack and note its danger in order to protect. It may not have as much direct effect as a virus or Trojan attack, but this type of attack can affect the fabric of internet commerce and communication. It

have appeared in many scenarios, with wide implications for security, safety and trust.

B. Constrained Shortest-path Energy-aware

ROUTING ALGORITHM

While traditional routing protocols try to minimize the end-to-end delay or maximize the throughput, most energy-aware routing protocols tries to extend the life time of network by minimizing the energy consumption sacrificing other performance metrics and at the same time, maintain good end-to-end delay. The result of a constrained shortest-path energy-aware routing algorithm is acceptable under all performance metrics and presents a performance balance between the traditional routing algorithm and the energy-aware routing algorithms.

An optimal routing problem is proposed for determining routing order for a source and multiple destinations. The proposed energy function mainly prevents the solution path from having loops and partitions. Experiments are performed on 3000 networks of up to 50 nodes with randomly selected link costs.

The proposed algorithm particularly shows significant improvements on the route optimality and convergence rate over conventional algorithms when the size of the network approaches 50 nodes.

Routing in Wireless Networks contains challenges, including limited energy constraints, network density, wireless channel errors. Different approaches exist in literature to overcome these challenges, such as data centric, location based and hierarchical routing. Most routing protocols in Wireless Sensor Networks are dealing with energy efficiency and network lifetime. In this paper, we present a shortest path routing algorithm based on Chandy-Misra's distributed shortest path algorithm regarding both node weight and edge weight. X percent of edge's weight and (100 - X) percent of node's weight form a total cost between neighbor and source node which is used in order to generate the shortest paths and construct a spanning tree. Variation of X percent, node weight and edge weight provide resilience for shaping needed paths and change the spanning tree's structure. When at least one node is close to critical energy level or a fault occurs, the routing algorithm is re-executed and new paths are generated. In order to obtain energy efficient paths, high network lifetime and finding out the overheads, we analyze the simulation results by assigning the battery level to node weight, communication cost to edge weight and %10, %30, %60 and %80 to X separately.

The nodes of the wireless sensor network follow a shortest path algorithm to transfer the data from the source to the destination. Wireless transmission of the data through the shortest path is aimed towards an energy aware routing procedure.

It explores the potential of using genetic algorithm to solve the shortest path problem in wireless sensor network. In multihop networks, such as the Internet and the Mobile Ad-hoc Networks, routing is one of the most important issues that has a significant impact on the network's performance. An ideal routing algorithm should strive to find an optimum path for packet transmission within a specified time so as to satisfy the Quality of Service (QoS). There are several search algorithms for the shortest path (SP) problem: the breadth-first search algorithm, the Dijkstra's algorithm and the Bellman–Ford algorithm, to name a few.

The energy efficient genetic algorithm routing prolongs the network lifetime Genetic Algorithm is a problem solving method which is based on the concept of natural selection and genetic. It gives an overview of shortest path algorithm with genetic algorithm and some existing algorithm.

Nodes are generally constrained in on-board energy supply, efficient management of the network is crucial in extending the life of the sensor. We present a novel approach for energy-aware and context-aware routing of sensor data. The approach calls for network clustering and assigns a less-energy-constrained gateway node that acts as a centralized network manager. Based on energy usage at every sensor node and changes in the mission and the environment, the gateway sets routes for sensor data, monitors latency throughout the cluster, and arbitrates medium access among sensors. Simulation results demonstrate that this approach can achieve substantial energy saving.

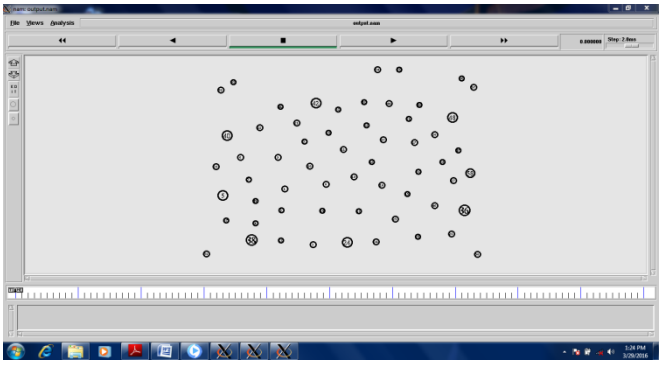
It tries to find the minimum energy path to optimize energy usage at a node. In this paper we take the view

that always using lowest energy paths may not be optimal from the point of view of network lifetime and long-term connectivity. To optimize these measures, we propose a new scheme called energy aware routing that uses sub-optimal paths occasionally to provide substantial gains. Simulation results are also presented that show increase in network lifetimes of up to 40% over comparable schemes like directed diffusion routing. Nodes also burn energy in a more equitable way across the network ensuring a more graceful degradation of service with time.

It looks at communication protocols, which can have significant impact on the overall energy dissipation of these networks. Based on this findings that the conventional protocols of direct transmission, minimum-transmission-energy, multi-hop routing, and static clustering may not be optimal for sensor networks, we propose LEACH (Low-Energy Adaptive Clustering Hierarchy), a clustering-based protocol that utilizes randomized rotation of local cluster based station (cluster-heads) to evenly distribute the energy load among the sensors in the network. LEACH uses localized coordination to enable scalability and robustness for dynamic networks, and incorporates data fusion into the routing protocol to reduce the amount of information that must be transmitted to the base station. Simulations show the LEACH can achieve as much as a factor of 8 reduction in energy dissipation compared with conventional outing protocols. In addition, LEACH is able to distribute energy dissipation evenly throughout the sensors, doubling the useful system lifetime for the networks we simulated.

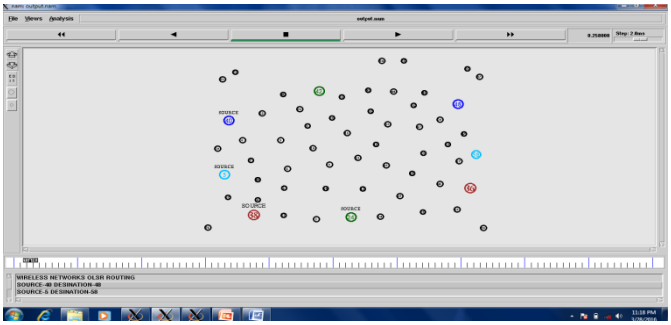
2. Results

A. Initial Node Creation



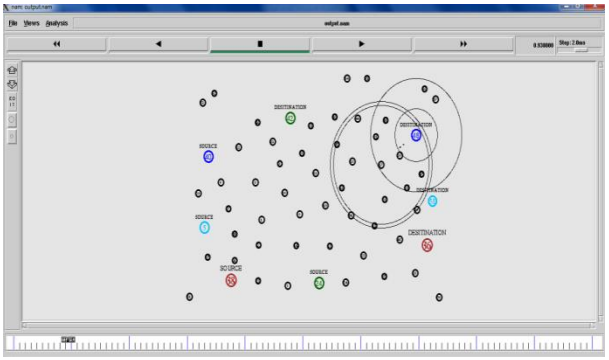
It shows the creation of nodes that are used to transfer files in a network.

B. Node With Source And Destination



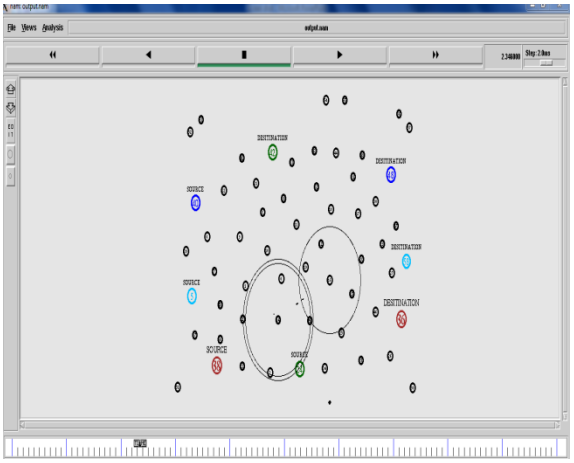
It denotes source and destination nodes which act as a sender and receiver.

C. Communication



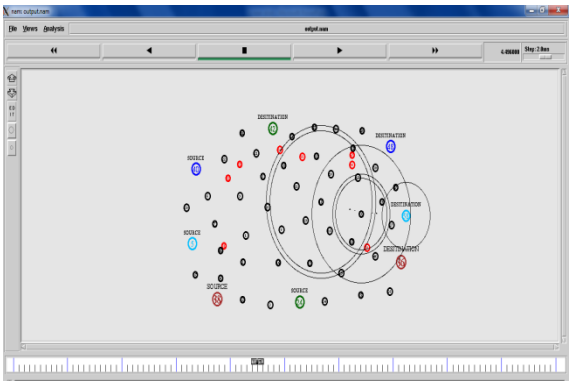
It shows the generation of acknowledgement to the router node and to the sub nodes.

D. Packet Drop



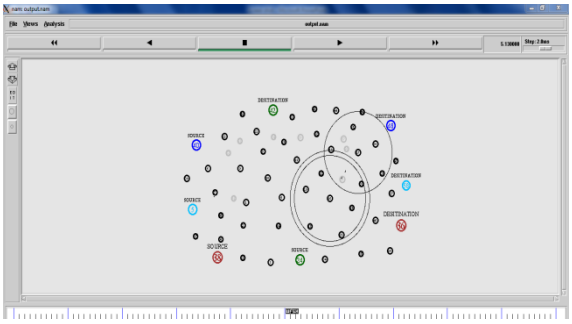
It shows the transmission of Data between the nodes.

E. Introduction of Attackers



It shows that some of the nodes are entering into the network which are attacker.

F. Elimination of Attackers



It shows the elimination of attackers who were entered into the network.

IV.CONCLUSION

This approach exploits the relationship between peers in a neighbourhood setting. The results on real-world P2P e-commerce confirmed fast mixing property hence validated the fundamental assumption behind Sybil Guard's approach. We also describe defence types such as key validation, distribution, and position verification. This method can be done at in simultaneously with neighbor similarity trust, which gives better defence mechanism. For the future work, we intend to implement Sybil Trust within the context of peers, which exist in many groups. Neighbor similarity trust helps to weed out the Sybil peers and isolate maliciousness to specific Sybil peer groups rather than allow attack in honest groups with all honest peers.

The future enhancement of this paper was to present Sybil Trust, a defence against Sybil attacking P2P e-commerce. Compared to other approaches, this approach is based on neighborhood similarity trust in a group P2P e-commerce community. In the future project what we have done means admin upload the products what type is useful for public database users. Border Gateway Protocol (BGP). Business or transactions conducted directly between a company and consumers who are the end-users of its products or services

V. REFERENCES

[1]. Guojun Wang Et al.,"Neighbor Similarity Trust against Sybil attack in P2P ECommerce"., vol.26, no. 3,pp. 824-833,Mar 2015.

[2]. J.Douceur, "The sybil attack," in Proc. Revised Papers 1st Int. Workshop Peer-to-Peer Syst., 2002, pp. 251–260.

[3]. B. Yu, C. Z. Xu, and B. Xiao, "Detecting Sybil attacks in VANETs,"J. Parallel Distrib. Comput., vol. 73, no. 3, pp. 746–756, Jun. 2013.

[4]. S. D. Kamvar, M. T. Scholosser, and H. G. Molina, "The Eigen-Trust algorithm for reputation management in P2P networks," in Proc. 12th Int. World Wide Web, May 2003, pp. 640–651.

[5]. H. Yu, M. Kaminsky, P.B. Gibbons, and A. Flaxman, "SybilGuard: Defending against Sybil attack via social networks," IEEE/ACM Trans. Netw., vol. 16, no. 3, pp. 576–589, Jun. 2008.

[6]. F. Musau, G. Wang, and M. B. Abdullahi, "Group formation with neighbor similarity trust in P2P e-commerce," in Proc. IEEE Joint Conf. Trust, Security Privacy Comput. Commun., Nov. 2011, pp. 835–840.

[7]. http://gnunet.org>node

[8]. https://www.computer.org > csdl > uic-atc