International Journal of Social Science & Interdisciplinary Research
Vol.1 Issue 12, December 2012, ISSN 2277 3630
Online available at www.indianresearchjournals.com

PROFICIENT AND SECURE PATH FOR DATA COMMUNICATION USING A-COLONY ALGORITM AND ENCRYPTED IP ADDRESS WITH RANDOMISING IN CRYPTOGRAPHICAL ALOGORITM

R. JAMES MARIANATHAN*; A. ARUL LAWRENCE SELVAKUMAR**

*Research Scholar, CMJ University , Shillong, Megalaya

ABSTRACT

The thesis is divided into two sections. The first section deals with back end server security. It is very important to secure the back end server as it is the one that contains important information. Thus it has to be made sure that only authorized people can access the data. Once the data is secured it is important to transmit the data through a reliable and secure route. The second section of the thesis is about finding the efficient data transmission route and to secure the route through which the data is transferred.

KEYWORDS:

INTRODUCTION

1. Back End Server Security

A protective model for back-end servers is accomplished by the novel combination of honeypot deployment, honeypot masquerading, and strict authentication for back-end server access. In our approach, a solution that has been catching on in the network security and computer incident response environment is to employ "Honey Pots." HoneyPots, also known as deception systems, honey-pots or tar-pits, are phony components setup to entice unauthorized users by presenting numerous system vulnerabilities, while attempting to restrict unauthorized access to network information systems.

Now a days Cryptographic processing may become a must done to secured message transmission, as for the demands for the secure communication grow. Cryptography is one of the techniques Cryptography is used to provide various security services. Cryptography widely used random numbers to generate random sequences. Any pseudo-random bit stream along with EX-OR provides a cryptosystem and any good cipher text should look like a pseudo-random bit stream. The randomization Algorithm provides better efficiency of utilizing the algorithms of different complexity to provide average case utilization. The proposal of implementing randomization in crypto graphical algorithms is to improve the overall performance by randomizing the standard algorithms and thus to optimize the high- level message security.

2. Routing Security

In the design of computer networks a fundamental problem is that of transmitting a single information packet from a given source-host to a set of recipient-hosts. Graph theoretic ideas have turned out to be essential in the design of efficient network. A physical network can be modeled as a complete graph where each host is associated with a node and an edge represents the link between the corresponding hosts. In the network design problem the network is designed with 'n' number of nodes and 'A' number of links. To achieve better performance the network should be designed with minimum number of links. If the number of link is minimum there won't be any transmission delay or decrease in throughput. The number of packets transmitted per unit time will also be high. In order to achieve such a configuration it is planned to design a network with minimum number of arcs.

In the existing system the network design is carried out using the clustering and dynamic programming technique. In the clustering technique smaller networks are grouped together to form a large network with minimum number of links. Because of the dynamic programming technique there occurs performance degradation in terms of time, space complexities, throughput, transmission delay etc. To improve the performance and to make the system more reliable it is proposed to design the system using the ant colony algorithm which is mainly used for the optimization.

In order to make the system in a more optimized way the network design is to be carried out using the Ant colony method. The ant colony method is a clever way of finding an optimized solution over a complex network. It models the living style of ants, mimicking how ants find their way to a food source from their colony and back again.

Ants travel from one node to another node to reach the food source. They stumble about randomly choosing paths that they haven't been down before. When an ant reaches a food source, it turns around and follows its own path backwards to the colony laying pheromone trial. The ant then goes back to the food colony again and again following the pheromone. The optimized path is the path, which contains the higher probability of pheromone deposition and low cost leaving the high cost and low pheromone path. Such a path is found out between each pair of the nodes in the network. Data intrusion is a problem in network environment. Hackers can easily obtain the data on a network if the path through which the data is transmitted is known. It is thereby necessary to secure the path through which the data is transmitted. Link Based RPS (Random Path Selection) algorithm is used to secure the path of data transmission.

3. Problem Statement

Data intrusion is a problem in network environment. Hackers can easily obtain the data on a network if the path through which the data is transmitted is known. It is thereby necessary to secure the path through which the data is transmitted. Link Based RPS (Random Path Selection) algorithm is used to secure the path of data transmission.

a. To secure the back end servers are:

- Front end servers are the interface to the clients, such as HTTP servers that provide static pages and control access to more sensitive information; these servers can often be replicated without complication because they provide read-only services and reply upon forwarding for handling interaction with more sensitive Information.
- Denial-of-Service attacks are typically a concerted mass of adversarial requests intended to consume system resources and prevent access by legitimate clients.
- Responding to Attacks, Honeypots address this problem as they can be quickly be taken without impacting day-to-day business operations. Also because the only activity the honeypot captures is the unauthorized or malicious activity, this makes hacked honeypots much easier to analyze.
- Back-end servers handle more complex requests that involve significant state updates and manage sensitive or valuable information; such servers may handle client authentication or oversee a database.
- Secure data transmission over network require strong encryption technique to exchange data. In the existing system encrypts a whole file using a single algorithm, the problem behind this is suppose if hacker know the key means easily encrypts the whole file.
- The proposed method splits the file number of chunks randomly. Also the proposed system uses more then one algorithms to encrypt the data. Initially .it chooses a block the message block randomly and chooses a algorithm randomly from the algorithm list, encrypt the message block using the selected algorithm. After that it sends the encrypted datas to the receiver, in the receiver side the reverse process is performed using the same technique.

b. Routing Security

Once the back end server is secured, the next problem faced is to secure the optimal route required to transmit the data.

Let there be a network interconnecting ‘n’ nodes, given the maximum diameter and the degree. The objective is to minimize the number of arcs (links) required to interconnect the chosen ‘n’ nodes, satisfying the following conditions:

- The network diameter should not exceed ‘d’ and the node degree should not exceed ‘Δ’.
- There should be a communication path from one node to another node, even though any failure occurs in any of the nodes in the network.
- The performance is improved in terms of transmission delay, throughput , reliability etc

4. Objective of the Study

The Authentication Server

- The Authentication Server sends the client authentication information to the masquerading router, Rm. The AS in this model also functions as a ticketing authority, controlling permissions on the application network.
- RANA encryption method allows sending the IP addresses of authorised users to the router in an encrypted format. The router then decrypts the addresses and stores it as MAC addresses. The authentication server uses this public key protocol to encrypt the message for router.
-

The Masquerading Router

- The masquerading router (Rm) is responsible for handling the traffic destined to the back-end server and deciding which traffic is legitimate and which traffic should be deflected to the virtual server.
- The encrypted IP addresses of authorized user are stored in the router. The router then decrypts the addresses and checks all the incoming addresses with the decrypted one.

Back End Server

- The back-end server handles Rqst() and Rply() messages normally with an added layer of security similar to an RBAC system; client information is not stored within the back-end server.
- Instead, the client provides a set of credentials along with the request that allow for comparison to the client's ticket, which is cryptographically generated by the AS and therefore computationally difficult to forge. The original data is encrypted using any public key algorithm.

The Front-End Server

The front-end server (SF) is responsible for forwarding client packets to the masquerading router

The Virtual Server

- The virtual server is a simulated production environment that can perform an imitation of as small or broad functionality as required.
- Its messages are handled in the same way as the back-end server messages.
- In this if the user is unauthorized then the modal of the original message but consisting of false data is being sent to the user. The false data is encrypted using any public key algorithm to give an illusion to the intruder of original data.
- The data security splits the file number of chunks randomly. Also the proposed system uses more then one algorithms to encrypt the data. Initially .it chooses a block the message block randomly and chooses a algorithm randomly from the algorithm list,

encrypt the message block using the selected algorithm. After that it sends the encrypted datas to the receiver, in the receiver side the reverse process is performed using the same technique.

-

5. Secure Routing

To minimize the number of interconnections.

The degree and diameter should not exceed the given value.

Even though any node or link fails, there should exist some communication path (survivability).

Each and every node should maintain a routing table with the pheromone value and the cost.

The path which contain the greater probability of pheromone deposition and low cost should be chosen as the optimized path for the transmission.

To secure the path of data transmission using RPS Algorithm.

Secure Routing

This section encompasses the set of principles, concepts and practices that lead to the development of a high quality system. It is the place where creativity rules, requirements and technical considerations came together in the formulation of a system.

REFERENCES

1. Y. Dodis and S. Khanna(1999),, "Designing networks with bounded pairwise distance," in Proc. 31st Annu. ACMSymp. Theory of Computing (STOC), pp. 750–759
2. Dissertion(2004), Ant algorithm in stochastic and multi criteria environments
3. Eric Rosenberg(December 2005), "Hierarchical topological network design", IEEE transactions on networking.
4. B. Korte and J. Vygen(2000), "Network design problems," in Chapter in Combinatorial Optimization: Theory and Algorithms. NewYork: Springer-Verlag.
5. Morgo dorigo, Mauro Birattari and Thomas Stutzle(November 2006), " Ant colony Optimization artificial ants as a computational technique", IEEE computational intelligence magazine
6. MarcoDorigo and Luca Maria Gambardella, "Ant Colonies for the Traveling Salesman Problem".
7. G. R. Raidl and B. A. Julstrom(2003) , "Greedy heuristics and an evolutionary algorithm for the bounded-diameter minimum spanning tree problem," in Proc. 23rd ACM Symp. Applied Computing,, pp. 747–752.
8. Sorkin, Gregory(January, 1990). ``Bivariate Time Series Analysis of Simulated Annealing Data.".

9. Vittorio Maniezzo, Luca Maria Gambardella, Fabio de Luigi , "5.Ant Colony Optimization "
10. Zhongzhen Yang & Bin Yu Transportation College, Dalian Maritime University, Dalian, 116026, China & Chuntian Cheng Civil Engineering Department, Dalian University of Technology, China, "A Parallel Ant Colony Algorithm for Bus Network Optimization".
11. Kellep A. Charles. "Decoy Systems: A New Player in Network Security and Computer Incident Response" International Journal of Digital Evidence, Winter 2004, Vol. 2, Issue 3.
12. Craig Valli, Nirbhay Gupta. "An initial investigation into the performance of the honeyd virtual honeypot system" In 4th Australian Information Warfare and Security Conference(Ed, Slay, D. J.) University of Adelaide, Adelaide. 2003.
13. Maximillian Dornseif, Sascha A. May. "Modelling the costs and benefits of Honeynets" In The Third Annual Workshop on Economics and Information Security(WEIS04).