ISSN:2249-5789
Manpreet Kaur et al , International Journal of Computer Science & Communication Networks,Vol 5(2),79-81

Attacks on Phoenix Coordinate System

Manpreet Kaur
Research Scholar
LPU
manpreet.7467@gmail.com

Akhil Sharma
Assistant Professor
LPU
akhilsharma90@outlook.com

Abstract

The network coordinate system provides the easy and efficient mechanism for estimating the network latencies by assigning the virtual coordinates to every node in the network. The network latency is calculated in terms of RTT. Most of the systems relays on Euclidean model, which contains the problem of TIV. To overcome this problem, matrix factorization was introduced which has better prediction accuracy. However, the accuracy of such systems often based on good corporation of coordinates and it is assumed that they always provide correct information. But when a malicious node provides incorrect information the performance may degrade. In this work, we study the impact of different malicious activities on the phoenix coordinate system.

Keywords: Network Coordinate Systems, Phoenix, RTT, Anomaly Detection, Triangular inequality violations.

1. Introduction

A number of latency sensitive peer-to-peer applications such as network monitoring, locality-aware server selection, application layer multicast, BitTorrent based file sharing [1] etc built on topology sensitive overlays network. Most of these applications rely on the network delays i.e. the round trip times (RTTs). They use the information about client and server network positions so that they can redirect the client to the servers that is close to client without measuring the direct paths between them. Due to present of various network factors like the bandwidth, network traffic, measuring and tracking of RTTs in a changing environment is not possible. These requires high rate of frequent measurements.

To overcome this dilemma, The Virtual Coordinate System, VCS or Internet Coordinate System, ICS are introduced. They used to characterize the network distance among the internet hosts in terms of Round Trip Time or RTT. They root the network distance into geometrical coordinate space so that the more accurate calculations can be made. The Network distance, i.e. round trip time and delay during transmission, is a property of a network that can affects the overall performance and scalability of an application.

The coordinate based approaches fit well in case of peer-to-peer applications, where the nodes compute their coordinates and piggybacked it and the end host can essentially compute the network delays. They also provide short and snappy information about the distances and resolve the measurement overheads. They provide enviable properties such as scalability, stability, robustness along with accuracy and less measurement overheads.

But these systems are major target for attacks. It is assumed that the nodes participating in system, always corporate with each other and also provide correct information about them. This behaviour of coordinate systems makes them open to malicious activities. The outsider can attack the system by injecting malicious software which can disturb the systems operation. Even an insider can also execute attacks by behaving like a trustful neighbour which is very effective.

In this paper, we study such type of malicious activities on phoenix system. Phoenix is a purely distributed system does not require any fixed set of landmarks for operation. Phoenix is based on matrix factorization and achieves high accuracy. We study the impact of various attacks on phoenix. In [9, 10], these attacks are referred against other coordinates system i.e. Vivaldi and NPS. We will mitigate these attacks against phoenix system by simulation and check the performance of the system.

The rest of the paper is organized as follows. Section II, provides an overview of the coordinate systems and detail of phoenix system. In section III, we present the classification of attacks. We described about our approach in section IV and Section V concludes the paper.

2. Related Work

In this section, we give a brief description about the internet coordinate systems and their working.

2.1 Network Coordinate Systems

The NC systems predict the network distance by embedding hosts into a coordinate space. Different models are being used for calculating the NCs. On the

bases of infrastructure these are broadly divided into two classes: centralized systems and decentralized systems [2].

In centralized coordinate systems, a fixed set of landmarks are used for calculating coordinates while other nodes calculate coordinates according to these landmarks. The landmarks are the trusted nodes in systems. First of all, the coordinates of landmarks are calculated by minimising the error between the predicted and measured distance. Then other participating nodes compute their coordinates by minimising error between predicted and measured distance to these landmarks. GNP [2], Lighthouse [5] ICS are the centralized NCS, which require fixed landmarks for the calculation of coordinates.

In decentralized systems, no landmark nodes required. Every node has equal rite in computing the coordinates. Any node that wants to compute its coordinates can select some nearby nodes and use them to figure out their own coordinates. Finding an appropriate neighbour is the prominent job. The neighbour nodes are selected by using different methods like Arbitrary chosen nodes, closely reside nodes and combination of both a hybrid approach, and are some different neighbourhood selection policies. Various decentralized NCS are: Vivaldi [3], PIC [4], NPS [1] etc. In these systems the nodes compute the coordinates with reference to each other.

2.2. System Overview

Phoenix is a dot product based NC system which is a completely decentralized system and doesn't require any fixed set of infrastructure nodes. A new node can calculate its coordinates after gathering latency information from a few other nodes. Any node with calculated NC can act as reference node for the other nodes to participate in NC calculations. As a result, phoenix is capable for large scale applications because the computations overhead are distributed among all nodes in system.

Basically, phoenix maps every node into two d-dimensional row vectors X and Y. The one is outgoing vector (X) and the other is an incoming vector (Y). The predicted distance between two nodes i.e. from node i to node j is the dot product of the outgoing vector of node i and the incoming vector of node j [6].

For the first m early nodes, $N \leq m$ where N is total nodes in system it uses the NMF [7] method for calculating NC. The new node communicates with each other to obtain the distance matrix. It will not disturb the decentralization of system and every node has the equal chances to be selected as reference node. Later, a weight-based mechanism [8] was introduced to compute the coordinates of the ordinary hosts. This achieves high prediction accuracy and minimizes the relative error.

3. Existing Attacks

Kaafar et. al. in his paper [9] [10] listed some attacks that malicious node can execute on the NC system. This means that the nodes in the system are not totally trusted nodes. There may be some malicious nodes present along with them which behave as a trusted participant but always provide false information when requested. The attacks are classified as:

1. Disorder Attack: This attack seeks to create an environment as a form of Denial of Service (DoS). This attack maximizes the relative error in the system. The intruder can achieve this attack either by introducing delay during communication or by not providing correct information to other nodes.

2. Isolation Attack: This attack isolates a particular node from the rest of the other nodes. The attacker convinces a particular node that it is in isolation zone. The primary goal of this attack is that after getting this information the victim communicates to an accomplice node, the partner in crime in order to update its position in the network as it seems to be the closest node in network. So that it can perform other network attacks on it like man-in-middle attack, packet dropping and traffic analysis etc. The attacker node can achieve this attack either by sending the delay probe or by falsifying the coordinates. So that when a victim node computes its coordinates it calculates a lager value that is extremely away from the other nodes but near to the attacker node.

3. Repulsion Attack: In this attack, the attacker tries to decrease the attractiveness of the target node. For this, it tries to convince the target node that it is far away from the other nodes in the network and also not participating in applications progress. It tries to show the performance and position of the node worst than the actual condition. This can be done by sending delay probes via victim or by manipulating the information about coordinates sent to other nodes. Theoretically, the isolation and repulsion attacks are equivalent. In this attack, the coordinates choose by intruder host if distant from origin.

4. System Control: This attack is achievable on the coordinate systems mostly on hierarchical systems which permit any node to be a landmark. The rule is to take a control over a node that can influence the coordinates of various other nodes. Hence, having control over few nodes can affect the whole system

performance. In case of NPS, which is a hierarchical system, the nodes try to get in higher level of system so that they can fool the maximum number of legitimate nodes.

4. Proposed Work

In this section, we present the approach which can be used to set up this experiment. For this we are using Phoenix coordinate system along with two globally present real time data sets one is King and other is PlanetLab, which contain pair-wise round trip latencies of DNS and other nodes over the internet. For this, once the nodes calculates their own coordinates. They shared their coordinate's information with new coming nodes and the neighbours that are already present in system. When system is in stable state the experiment starts. In first scenario, during information sharing the intruder will change the information and pass it on. The nodes refer this false information and the system starts deviate. The other way, we will limit the legitimate node to communicate with other nodes by restricting not to response the generated requests. By breaking the communication bridge, the nodes will not able to come to stable state. Next, we will attack a legal node from two-way and force it to compute higher values and address these false values of coordinates to the other nodes. We will allow propagation of these errors in system. We will examine the working of phoenix system throughout and conclude the results.

5. Conclusion and Future Work

A network coordinates system provides benefits to wide range of applications. However, the various mechanisms protect Vivaldi and other systems from malicious activities. But they do not provide higher accuracy than the Phoenix system. In this paper, we study the impact of various attacks with respect to phoenix and analyze its performance. It is expected that execution of such attacks will degrade the performance of the system. We will try to implement this on simulator and analyze the various factors of performance of system.

6. References

[1] Ng, TS Eugene, and Hui Zhang. "A Network Positioning System for the Internet." In USENIX Annual Technical Conference, General Track, pp. 141-154. 2004.

[2] Ng, TS Eugene, and Hui Zhang. "Predicting Internet network distance with coordinates-based approaches." *INFOCOM 2002*. Twenty-First Annual Joint Conference of the IEEE Computer and Comm. Societies. Proceedings IEEE Vol. 1. IEEE, 2002.

[3] Dabek, Frank, Russ Cox, Frans Kaashoek, and Robert Morris. "Vivaldi: A decentralized network coordinate system." In ACM SIGCOMM Computer Comm. Review, vol. 34, no. 4, pp. 15-26. ACM, 2004.

[4] Costa, Manuel, et al. "PIC: Practical Internet coordinates for distance estimation." Distributed Computing Systems, 2004. Proceedings. 24th International Conference on. IEEE, 2004.

[5] Pias, Marcelo, et al. "Lighthouses for scalable distributed location." Peer-to-Peer Systems II. Springer Berlin Heidelberg, 2003. 278-291.

[6] Chen, Yang, Xiao Wang, Xiaoxiao Song, Eng Keong Lua, Cong Shi, Xiaohan Zhao, Beixing Deng, and Xing Li. "Phoenix: Towards an accurate, practical and decentralized network coordinate system." In NETWORKING 2009, pp. 313-325. Springer Berlin Heidelberg, 2009.

[7] Lee, D.D., Seung, H.S.: Learning the parts of objects by non-negative matrix factorization. Nature 401(6755), 788–791 (1999).

[8] Chen, Yang, Xiao Wang, Cong Shi, Eng Keong Lua, Xiaoming Fu, Beixing Deng, and Xing Li. "Phoenix: A weight-based network coordinate system using matrix factorization." Network and Service Management, IEEE Transactions on 8, no. 4 (2011): 334-347.

[9] Kaafar, Mohamed Ali, Laurent Mathy, Thierry Turletti, and Walid Dabbous. "Real attacks on virtual networks: Vivaldi out of tune." In Proceedings of the 2006 SIGCOMM workshop on Large-scale attack defense, pp. 139-146. ACM, 2006.

[10] Kaafar, Mohamed Ali, Laurent Mathy, Thierry Turletti, and Walid Dabbous. "Virtual networks under attack: disrupting internet coordinate systems." In Proceedings of the 2006 ACM CoNEXT conference, p. 12. ACM, 2006.