Applications of Secure Multi-Party Computation in Advanced Distributed Models

Yingpeng SANG

yingpeng@jaist.ac.jp

March 6, 2005

1 The Aim

The aim of this research is to employ specific solutions to some problems on Secure Multi-party Computation in advanced distributed models, such as grid and wireless sensor network.

The first problem is to test the privacy state of a person in pervasive sensor networks, under which different types of sensor networks may be deployed for different purposes so that a person's privacy claims are dynamic. It's better to provide a general scheme to address all of a person's privacy concerns and make the person aware of whether he has been under some observations. However, it's another currency that sensor nodes are becoming physically invisible (Smart dust, for example) or should be hidden for military or commercial reasons. How, then, could he know his state when the observation is invisible?

The second problem is about how to securely mine sensitive data on the infrastructure of grid. Grid-based data mining approach can be used to shift the data mining workloads to external computational grid from database servers. However, the data may be sensitive and should be kept as privacy of the database servers.

2 Solutions on the problems

To our knowledge, little work has been done to address the originator privacy when its concern is dynamic under the circumstances of pervasive sensor networks, especially when the sensing area privacy should also been considered. Our scheme is based on the protocol of secure two-party point-inclusion problem.We apply the point-inclusion protocol to test the originator privacy state in pervasive sensor networks.

As for the second problem, Support Vector Machine (SVM) is the major concern. SVM is one effective tool for classification and regression in data mining. When SVM is employed on the external computational grid, some security schemes should be taken on the data set sent from the inside database server. The security schemes we will use consist of homomorphic encryption and data perturbation.

3 Progress of 2004

In the first half year, papers about previous work are collected and read. The topics of these papers concerns grid computing, ubiquitous computing, wireless sensor network, privacy preserving data mining, secure multi-party computation, and cryptography, etc.

In the second half year, a scheme about the test of privacy state in wireless sensor network was shaped and evaluated based on a simple architecture. After that, the algorithm of SVM is integrated into applications on data mining, and tested for jobs such as classification and novelty detection.

4 Future directions

For the privacy state test scheme for wireless sensor network, a large number of security-related problems are still open. Denial-of-service attack on the server may be employed by an adversary, so it should be prevented effectively. Besides, the scheme solves only a point-inclusion problem on the planar surface. Some cubic solutions should also be studied.

For the secure data mining on grid employing SVM, workload of data transferring from the inside database servers should be reduced. The hosts in the external computational grid are assumed semi-honest, so schemes should also be considered to prevent them from malicious cheating or violating in the protocol.

References

[1] Yingpeng Sang, Hong Shen, A Scheme for Testing Privacy State in Pervasive Sensor Networks, *Proc. of the international conference on Advanced Information Networking and Applications (AINA 2005)*, Taipei, Taiwan, Mar. 2005.

[2] Yingpeng Sang, Hong Shen, Pingzhi Fan, Novel Impostors Detection in Keystroke Dynamics by Support Vector Machine, *Proc. of the 5th international conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT 2004)*, Singapore, Dec. 2004.