Journal of Computer Science 8 (7): 1092-1098, 2012
ISSN 1549-3636

Dynamic Distributed Intrusion Detection System Based on Mobile Agents with Fault Tolerance

[1]Sasikumar, R. and [2]D. Manjula
[1]Department of Computer Science and Engineering,
R.M.D Engineering College, Kavaraipettai, Chennai, Tamil Nadu, India
[2]Department of Computer Science and Engineering,
College of Engineering, Anna University, Chennai, Tamil Nadu, India

Abstract: Problem statement: In earlier days, each and every individual system has particular IDS to the particular system and due to this particular technique there are many drawbacks and much more drawbacks in the system side networks. "All processes used in discovery of unauthorized uses of network or computer devices" Detection of unusual and abnormal activity/events in real-time. Detects break-ins or attacks through various data sources from logs/audit/surveillance and network traffic. **Approach:** The Intrusion Detection System (IDS) has an objective to identify individuals that try to use a system in a way not authorized or those that have authorization to use but they abuse of their privileges. This study proposing the Dynamic Distributed Intrusion Detection System (DDIDS) to improve the system Processing and system Networking. **Results:** An implementation result of the network plays a very important role in order to connect each and every system through a network. For that reason it is said with the experiment that the enhanced intrusion detection system based on Agent gain highly developed detecting performance with fault tolerance. **Conclusion:** The main aim of this study is to design and develop the dynamic distributed intrusion detection system that would be accurate, low in false alarms, not easily cheated by small variations in pattern, adaptive and be of real time and also increase the system efficiency and increase the system network efficiency.

Key words: Intrusion Detection System (IDS), Mobile Agent (MA), Decision-making Agent (DA), Replication Agent (RA), distributed IDS, fault tolerance

INTRODUCTION

The intrusion detection is defined as the process of intelligently monitoring the events occurring in a computer system or network, analyzing them for signs of violations of security policy. The primary aim of intrusion detection system is to protect the availability, confidentiality (Siqueira and Abdelouahab, 2006) and network information system. Intrusion Detection systems are defined by both the method used to detect attacks and the placement of the IDS on the network. IDS may perform either misuse detection or anomaly detection and may be deployed as either a network-based system or a host-based system. This result in four general groups: misuse-host, misuse-network, anomaly-host and anomaly-network. Misuse detection relies on matching known patterns of hostile activity against databases of past attacks. They are highly effective at identifying known attack and vulnerabilities, but rather poor in identifying new security threats. The performance of the intrusion detection system can be improved by utilizing a hybrid intrusion detection system which combines and misuse analysis. The ongoing Explosion in the use of the Internet has created a scale of the revolution today. However, this explosion is introducing a huge problem of security for both the networks and services. The needs of remote access from customers, users and service provider in a particular environment require that the precautions must take in order to make a balance between the security demands and the access flexibility. The existing security solutions are very complex and costly. What is rapidly needed is a flexible, adaptable and affordable security solution, which provides greater autonomy. Therefore, it is necessary to review the way security system architectures are designed in investigating new technologies that could help make easier and cost-effectiveness new solution.

Corresponding Author: Sasikumar, R., Department of Computer Science and Engineering, R.M.D Engineering College, Anna University, Chennai, Tamil Nadu, India Tel: +91-09941515894

Source of IDS: There are two approaches available for basic Intrusion Detection Systems (IDS), namely host and network based approaches (Eid, 2004). Host based systems collect local data from sources internal to a computer, usually at the OS level. This has the advantage of collecting high quality data directly at the source (e.g., kernel).

Unfortunately, some attacks cannot be detected at a single location. Distributed intrusions may leave innocent marks at each single host and can only be identified when combining data from a number of different machines and even the efficiency of the system found to be increased in a gradual manner.

More over in Network side mostly the encrypted communication alone is randomly used. Network based variants monitor packets on the wire by setting the network interface to promiscuous mode and analyzing network traffic. Therefore they have some possibilities to correlate activities that occur at different hosts, but suffer from scalability problems in case of high network load and have problems when encrypted communication is used.

A new approach is the development of distributed architectures, where sensors (host and network based) collect data, preprocess it and send it to a centralized analyzing station which is able to relate this input. Intrusion Detection has been achieved by following two different strategies of analysis (Barika *et al*., 2009).

Anomaly detection: Relies on models of "normal" behaviors of a computer system. Behavior profiles may be focused on users, applications or networks. Anomaly detection compares the defined profiles against the actual usage patterns to detect "abnormal" activity patterns. These patterns will be considered as intrusions.

Policy Rations: Intrusion Detection System includes many desirable characteristics and also agent system. At least one post.

IDS Rations: Intrusion detection system includes many desirable characteristics and also agent system. At least one past effort has identified desirable characteristics for IDS. Regardless of what mechanisms an IDS is based, it must do the following:

- Run continuously without human supervision
- Be fault tolerant and survivable
- Resist subversion and Impose minimal overhead
- Observe deviations from normal performance
- Be easily adapted to a specific network
- Adapt to changes over time and Find difficult to take in

In this study a similar set of requirements along two themes were developed namely functional and performance requirements.

Efficient rations: The Efficient agents or ratios consist of the following characteristics are as follows in the following ways:

- IDS must continuously monitor and report intrusion and IDS should have a very low false alarm rate
- IDS should provide enough information to repair the system in the case of detection of intrusion. Notice that this characteristic depends on IDS goals. In fact, many IDS solutions focus only on alerting administrators without suggesting any corrective actions
- IDS must detect and react to distribute and coordinated attacks. This detection feature is one of the most difficult because it needs a huge distributed amount of information in addition to the hard task of synchronization between different hosts
- The IDS should be adaptive to network topology and configuration changes

Performance rations:

- Intrusion should be detected in real-time as it should be reported immediately in order to minimize network damage
- The IDS must be scalable in order to handle additional computational and communication loads

Limitations to be followed: The most common IDS shortcomings include the following:

- High number of false positives
- Lack of efficiency: Usually when an IDS is faced with a very large number of events in the network, it slows down a system or drops network packets
- Vulnerability to attacks: Hierarchical structures attackers the opportunity to harm the IDS by cutting off a central branch or even by taking out the root command

Negotiator: Agent is an entity being able to accomplish some work without manual intervention and supervision in certain condition. It is self-adaptable, intelligent and collaborative.

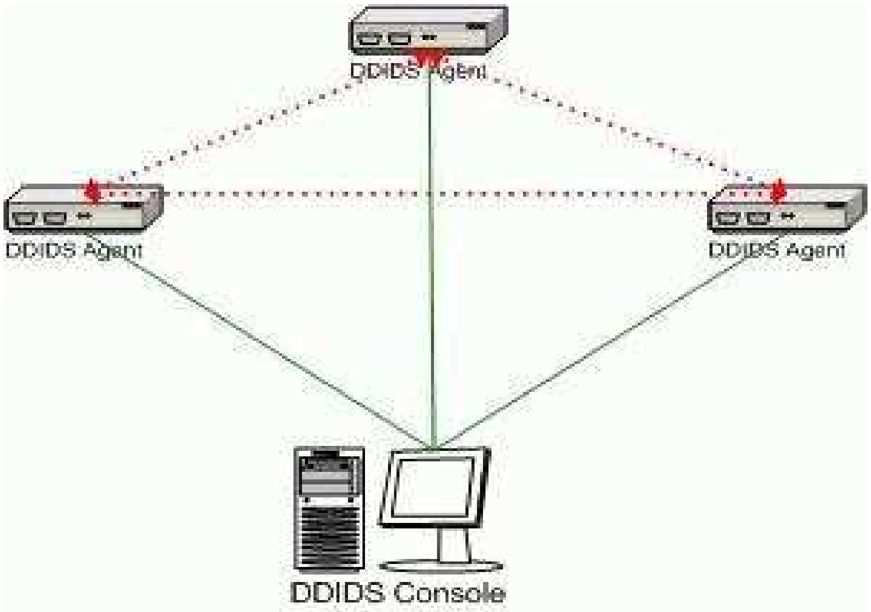

Fig. 1: DDIDS Agent System

Figure 1 shows the basic architecture of dynamic distributed intrusion detection system AGENT SYSTEM. In this system each DDIDS system have a connection with the others for infomratiom sharing between an intrusion and to take a necessary steps to solve a current problem arise in a network. DDIDS console will have a control of every agent in a network and will support for report preparation.

An Agent not only works independently, but also can accomplish some missions with other Agents. Further, an Agent can be controlled to perceive the change of environment and act to the environment back (Dong and Liu, 2007). There are two kinds of agent: static agent and mobile agent (Jun *et al*., 2006).

Static agent is the first proposed (Hou *et al*., 2011) Agent technology which is applied in the area of intrusion detection. Static agent, that is to say, the agent that resides in a fixed position or some fixed platforms.

Mobile agent is an entity capable to move from a node to another over the network. It permits to spread dynamically the server interfaces managed on the different sites. It guarantees a big resistance to network breakdowns; it also permits savings of bandwidth since negotiations between mobile agents and the server consists in local message exchanges that don't pass by the network (Boughaci *et al*., 2006).

Portable negotiator advantages (Mobile): Instead of using static components in an IDS, mobile agent based systems has the advantages of:

- Overcoming Network Latency (faster response)
- Reducing Network Load (less network load)
- Asynchronous Execution and Autonomy (agents can work autonomously)
- Structure and composition (Natural way to structure and design an IDS)
- Operating in heterogeneous environments (Platform Independent)
- Dynamic Adaptation (The system can be reconfigured at run-time)
- Static Adaptation (updating can be added without restarting the whole system)
- Robust and Fault-Tolerant Behavior (The ability to react dynamically in unfavorable situations)
- Scalability (agents can be cloned and distributed) (Fredj *et al*., 2010)

MATERIALS AND METHODS

Projected scheme design: Based on the merit of Agent technology, this study puts forward a distributed intrusion detection system based on agents (Belmekki and Mezrioui, 2005). It is composed of three layers: Layers Consisting of Host Agent and Net Agents, Mobile Agents and decision making and Replication Agents (Zhang *et al*., 2003).

Network connection: Here the term network denotes the connection between the particular systems or machines (i.e.,). A single network consists of many numbers of systems which are found to connect internally. Each and every individual system has its own address. In the proposed DDIDS then number of systems are found to be connected to a single server. Like same ways N number of systems are connected to the single server (Benattou and Tamine, 2005). Whereas if a single is found to be in fault condition doesn't matter it uses to share the information from the neighbor system. Similarly the remaining system also follows the same procedure for sharing the certain information or messages.

Whereas each and every workstation has its own switch and the particular agent system to share the particular message through the router. Here the Network plays an important and major role in order to share the information's between the systems and finally if the fault is found in every system and the message or information cannot transform. In this particular case the dynamic distributed intrusion detected system performed as a major role. By using this DDIDS the efficiency of the system can increased and the information also can transfer very easily (Kannadiga and Zulkernine, 2005).

Host negotiator: The Host Agent's function is protecting the system where it stays. When suspicious activities can't be decided, the Host Agent generates an ID event and transmits it to layer2. Every type of ID event means a kind of possible attack. In Fig. 2 shows the detailed architecture of DDIDS with the workstation and agents .The interlink between the all kinds of DDIDS agent system will share the intrusion data with the support of console window. This console window could be useful for the admin to gather an information about the intrusion happen in a corresponding network.

Algorithm implementation procedure:

```
Step1: Check the connection state of the every node or
       host in a system.
Step2: Have a connection unit switch and IDS for
       verification.
Step3: Make an interlink between all IDS in a network.
Step4: Each IDS in the switch has to check the
       intrusion in the network.
       If ( intrusion)
       Update into two corresponding IDS
       Else
       Repeat step4
Step5: Share the IDS with all network IDS.
Step6: (DDIDS Agent) have to connect with network
       IDS and have a separate console window for
       updates
Step7: Each process has an updating and sharing in the
       network.
```

Net negotiator: The role of the Net Agent is to detect network intrusions. It is installed in the neuralgic places of the network (Syurahbil *et al*., 2009), for example, at the entrance of the network or on the server and so on. The Net Agent supervises the network traffic, records all suspected events in a database and responds intrusions. It also installs mobile agent platform on it. The process that the Net Agent deals with the intrusions is the same as Host Agent.

Agent system: The Agent System consist of Mobile Agents dispatched by the layer 3 for the continuous observation of layer 1 the Host and Net Agents. The Mobile Agent visits all the hosts in the network and collects the related attack data information (Yongle *et al*., 2003). Then it correlates the collected information with the data it has received from the other Host Agent or Net Agent that has generated the same type of ID event. The MA sends out alerts when detects intrusion, on one hand it informs every host it has visited to take the corresponding response measures and show the alerts, on the other hand, it transmits these related information to the layer3 and shows them on the user interface.

Mobile negotiator: MA is responsible for collecting information of an attack from the Host Agents or Net Agents for further analysis in layer3.

Switch network: It consists of a Decision-making Agent (DA), Replication Agent (RA) and Profile Database (PRDB).

Decision-making Agent (DA): Decision-making Agent (DA) is the highest entity of the system and uses MA to control and coordinate with every Host Agent and Net Agent in this system. It orders the agent to execute some functions as updating file-rules dynamically. DA is responsible for the analysis of the information collected by MAs. It has a global view of the system and has knowledge of: (i) Availability of resources in the hosts (memory, disk space). It has a knowledge of who is overloaded and which can receive agents; (ii) Necessity of agents of the network, for example, whether they need more memory. It identifies when an agent is highly/lowly necessary, which implicates that its replication strategy should be observed and possibly altered; (iii) which action of recovery must be executed for each type of detected faults. It can request alteration of the strategy of replication of a group of agents, migration or creation of new agents.

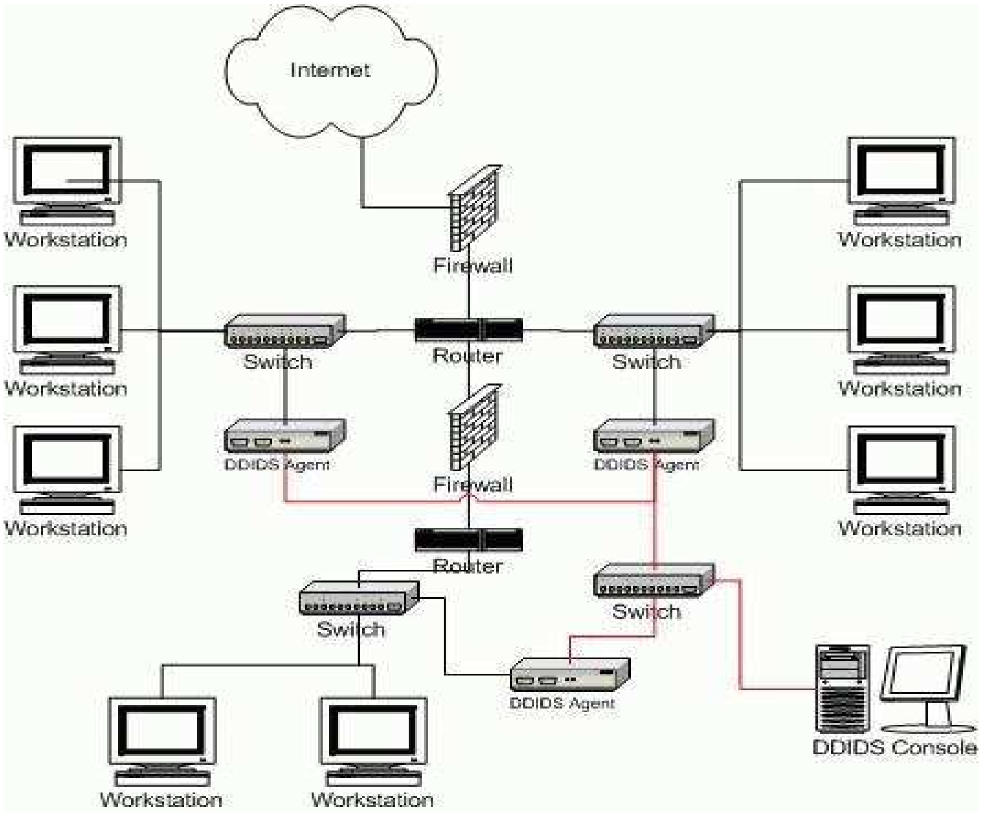

Fig. 2: System architecture of DDIDS

Replication Agent (RA): Replication Agent (RA) is responsible for the replication and recovery management, in other words: for the organization of the group of replicated agents, adding or removing an agent for a group; for the strategies of replication of each group and by which alteration is necessary; for the consistency of the replicas. The replication is transparent to the agents. Only RA knows the groups, the strategies and the number of replicas in each group. RA has knowledge of the localization of the active agents and its replicas.

Profile database (PRDB): Profile Database (PRDB) is the database of profiles. It stores the information related to the standard behavior of each agent on the network. All the authorized actions for each agent of the system should be registered. Besides, the agents that can send solicitations to agents that are registered. DA uses this information in the process of evaluation for the detection of malicious agents.

Fault tolerance: Here the term fault tolerance can be a logical or a physical one. The Decision-making Agent analyses the data collected by MA and passes the control to RA. If it is a logical problem the RA corrects the network. If it is a physical problem it sends an sms to the network administrator.

RESULTS

Experimental design and analysis: To test the validity of the improved system, this study designs an experiment to hold back the stimulated some kinds of attack activities with two different systems. One is the improved intrusion detection system based on Agent and the other is a general Rule-based intrusion detection system. Then, it reaches a conclusion by analyzing and comparing with the test result.

Experiment presentation: Here in this experiment network plays a very important role in order to connect each and every system through a network. Almost all the place the local area network (i.e.,) LAN is used. The experiment is carried out in a LAN with the bandwidth of 100 Mbps. The attack activities are simulated with the target as a host on the LAN. All types of attacks are performed on the proposed Intrusion Detection System (IDS) architecture.

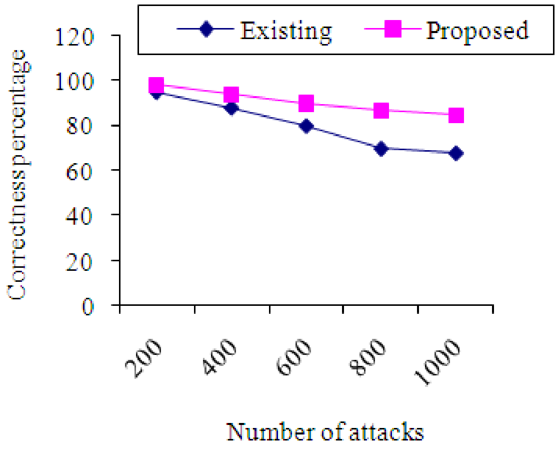

Fig: 3: Fault detection efficiency

Table 1: Comparison with different technique

Technique	Hardware Overhead %	Fault acceptance %
IDS	35	60
DIDS	63	40
DDIDS	70	15

The Table 1 shows the different technique that has been implemented for intrusion detection in a network. If we go with some advance level the hardware requirements gets increased , at the same time the fault accepts level gets decreased. Our proposed method is the best one compare to another technique. Procedure to check an intrusion in network and host by our approach. The percentage of correction increases with the number of attacks. This is shown in Fig. 3:

Step1: In this step, to assign the N number of systems to the particular Network System, then for each individual system going to connect the switch to the particular system.

Step 2: Connecting N number of networks and for every System Switch are also connected in order to exchange the information's or some messages.

Step 3: Sharing information between all IDS in a network connected with the router. The router has to connection with the DDIDS agent with the separate console application for developing the perfect solution for the corresponding errors in a network.

Step 4: Find a fault in any system in network update information to the corresponding IDS agent then share it in the network.

Step 5: Collect the solution from an other IDS agent in a network with support of DDIDS console for the verification in future cases.

DISCUSSION

Performance analysis: The percentage of correction increases with the number of attacks. This system is provided with high detectivity. By the introduction of Mobile Agents, the system is able to analyze and classify real-timely the state of intruding activity, so it can detect the attack correctly. The data about the fault detection by the existing is less compared to our proposed design. Since it has a shared connection for an information sharing between the IDS and can provide a perfect solution by the DDIDS console window. This system is also provided with high flexibility and fault tolerance. In order to prevent letting the whole network undefended, when a part of the IDS fails, agents can work autonomously even if their creators don't operate anymore.

CONCLUSION

Our aim is to provide the Intrusion Detection System is Cooperative and Distributive and also reduce the false positive rate in this mechanism. The main advantage of using this dynamic distributed intrusion detection system many numbers of systems can be included into a single number of servers and also from a single server can dynamically monitor all (i.e.,) the user can monitor each and every individual client system. Intrusion Detection System (IDS) plays an important role in achieving survivability Information system and preserving their safety from attacks. Centralized IDS consumes lot of network resources and is a single point of failure. So Mobile agent platforms are used to overcome deficiencies of centralized IDS, efficiently manage the system and dynamically adapt to network changes and event rules. The mobile agent based IDS shows superior performance in terms of reporting the intrusion instantly. In this study it provides the Intrusion detection system architecture based on Decision-making and Replication Agents with fault tolerance. The study of load balancing is left for future researchers.

REFERENCES

Barika, F.A., N.E. Kadhi and K. Ghedira, 2009. MA_IDS: Mobile agents for intrusion detection system. Proceedings of the IEEE International Advance Computing Conference, Mar. 6-7, IEEE Xplore Press, Patiala, pp: 900-910. DOI: 10.1109/IADCC.2009.4809135

Belmekki, A. and A. Mezrioui, 2005. Using active agent for intrusion detection and management. Proceedings of the International Conference on Computational Intelligence for Modeling, Control and Automation and International Conference on Intelligent Agents, Web Technologies and Internet Commerce, Nov. 28-30, IEEE Xplore Press, Vienna, pp: 989-994. DOI: 10.1109/CIMCA.2005.1631597

Benattou, M. and K. Tamine, 2005. Intelligent agents for distributed intrusion detection system. Proc. World Acad. Sci. Eng. Technol., 6: 190-193.

Boughaci, D., H. Drias, A. Bendib, Y. Bouznit and B. Benhamou, 2006. A distributed Intrusion detection framework based on autonomous and mobile agents. Proceedings of the International Conference on Dependability of Computer Systems, May 25-27, IEEE Computer Socity, pp: 248-255.

Dong, B. and X.L. Liu, 2007. An improved intrusion detection system based on agent. Proceedings of the International Conference on Machine Learning and Cybernetics, Aug. 19-22, IEEE Xplore Press, Hong Kong, pp: 3164-3167. DOI: 10.1109/ICMLC.2007.4370692

Eid, M., 2004. A new mobile agent-based Intrusion detection system using distributed sensors. American University of Beirut.

Fredj, O.B., H. Sallay, A. Ammar, M. Rouached and K. Al-Shalfan *et al*., 2010. On distributed intrusion detection systems design for high speed networks. Proceedings of the 9th WSEAS International Conference on Advances in E-Activities, Information Security and Privacy, (ISPACT' 10), WSEAS, USA., pp: 115-120.

Hou, Z., Z. Yu, W. Zheng and X. Zuo, 2011. Research in intrusion detection system based on mobile agent. Inform. Comput. Appli., 7030: 233-240. DOI: 10.1007/978-3-642-25255-6_30

Jun, W., W. Chong-Jun, X. Jun-Yuan and C. Shi-Fu, 2006. Research on agent-based intrusion detection technique. Comput. Sci.

Kannadiga, P. and M. Zulkernine, 2005. DIDMA: A Distributed intrusion detection system using mobile agents. Proceedings of the 6th IEEE International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, May 23-25, IEEE Xplore Press, pp: 238-245. DOI: 10.1109/SNPD-SAWN.2005.31

Siqueira, L. and Z. Abdelouahab, 2006. A fault tolerance mechanism for Network Intrusion Detection System based on Intelligent Agents (NIDIA). Proceedings of the 4th IEEE Workshop on Software Technologies for Future Embedded and Ubiquitous Systems, Apr. 27-28, IEEE Xplore Press, Gyeongju, pp: 1-6. DOI: 10.1109/SEUS-WCCIA.2006.4

Syurahbil, N.A., M.F. Zolkipli and A.N. Abdalla, 2009. An intrusion preventing system using intrusion detection system decision tree data mining. Am. J. Eng. Applied Sci., 2: 721-725. DOI: 10.3844/ajeassp.2009.721.725

Yongle, D., Q. Jun and S. Meilin, 2003. A cooperative intrusion detection system based on autonomous agents. Proceedings of the Canadian Conference on Electrical and Computer Engineering, May 4-7, IEEE Xplore Press, pp: 861-863. DOI: 10.1109/CCECE.2003.1226031

Zhang, R., D. Qian, H. Chen and W. Wu, 2003. Collaborative intrusion detection based on coordination agent. Proceedings of the 4th International Conference on Parallel and Distributed Computing, Applications and Technologies, Aug. 27-29, IEEE Xplore Press, pp: 175-179. DOI: 10.1109/PDCAT.2003.1236282