CHAPTER 6

CONCLUSION

In a grid environment, a RP provides functional services to consumers. In such a scenario, it is essential that the selection of an RP is not only based on service functionality, but also on the process behavior such as trustworthiness, QoS of the RP and policy-constraints of both the communicating parties. In a broker-based trust management system, intermediaries known as brokers are responsible for ensuring the trustworthiness of the RP and its QoS.

6.1 CONTRIBUTIONS OF THE WORK

Various broker architectures such as Single Broker Architecture, Multi-Broker Architecture and Hierarchical Broker Architecture have been proposed in our work. Selection of RP is based on reputation-based trust, and identity-based trust along with the matched policy constraints when compared to the conventional resource selection process.

Simulation results in Multi-Broker Architecture show that the selection process for a trustworthy RP leads to better performance with less cost-loss for the consumer community. Use of broker’s feedback in addition to the consumer’s feedback, for the computation of trust-index of RP has a positive impact on choosing a ‘trust-worthy’ RP. It is also seen that the waiting time and the maximum queue length decrease as the number of brokers in each domain increases. Thus, the proposed architecture is robust in
terms of selection of suitable RP for a resource request with quicker selection process, reduction in cost-loss and achieving reliability through redundancy.

Simulated results in Multi-Broker Architecture without delegation of requests and with reputation and policy-based resource selection indicate the reduction on the workload of the broker and the number of message exchanges compared to the Multi-Broker Architecture with conventional resource selection method. It is also seen that with the deregistration concept, the broker’s trust-index is almost maintained since the untrustworthy RP are deregistered. The observation is that the proposed filtering and prediction method of malicious feedback in this model is efficient to safeguard the RP’s trust-index and award the RP with its utmost deserving trust-index even when the consumer acts maliciously.

Simulation results in Hierarchical Broker Architecture reveal that the selection process for an RP leads to better performance of the grid with better job-success rate and less cost-loss for the consumer community, compared to the Multi-Broker Architecture. RRAs derive their compensation from registration, renewal, and audit charges paid by the broker community, rather than from individual transactions by the broker as in the prior proposed architecture. Results of the proposed model with integrated reputation and policy-based resource selection methodology point to show further improvement in reduction of cost-loss to the consumers. Filtering of dishonest feedbacks and predicting with a true feedback of RRA for the trust-index computation of RP are implemented and its improved effects are presented. The trust-indices of brokers are also safeguarded with the de-registration concepts in the hierarchical model.

A very important issue in software security, namely the integrity of computation on a remote, un-trusted host in grid environment, is considered.
In this work, some tasks of given jobs are considered as quiz queries instead of separate set of quiz queries in order to avoid the differentiation of jobs from quiz queries at the RP’s site. This proposed improved quizzing scheme in Hierarchical Broker Architecture leads to better resource utilization compared to the existing replication and quiz-based result verification scheme. Trustworthiness of RP is computed based on the quiz-based result verification scheme.

In addition to reputation-based trust, identity-based trust is also considered here to further safeguard the broker architecture by the selection of trustworthy entities (consumers, RP and brokers) with authentication mechanism, DDoS defense and spam filtering mechanisms. The consumers who enter the Hierarchical Broker Architecture with the motive of attacking the system and paralyzing it from functioning are detected by the proposed DDoS Defeat Engine with the help of the Authenticator modules present in it. The Authenticator identifies and rejects the fake requests coming from unauthenticated DDoS consumers and allows only the genuine requests to the RRA for further processing. Thus, resource utilization is improved only for processing genuine requests. Wastage of resources for processing DDoS requests is eliminated by the proposed authenticators with bearable overhead.

Hierarchical Broker Architecture is extended by creating an overlay network of RRA for collaborative spam filtering and DDoS attack defense mechanism. The proposed Anomaly Detection Agent (ADA) that runs the DDoS defense mechanism and the spam filtering thread is placed at the perimeter of each RRA site in the Hierarchical Broker Architecture.

An intuitive three-level hierarchical model has been proposed that consists of registers to capture and analyze the traffic characteristics, a short term memory to perform local attack detection and a long term memory for
global detection and collaboration. The proposed layered spam filtering solution consists of white list, blacklist and Bayesian filtering. These mechanisms are incorporated at the perimeter of the RRA site at the highest tier in the architecture. This firewall-like protection ensures that the smaller entities need not be burdened and also the spam messages as well as attack packets can be filtered before they enter the architecture. The effectiveness of this filtering solution can be seen from the simulated graph which clearly shows that fewer resources are exhausted in a system with the filtering mechanisms in place, as against the system with only trust-based resource selection with less false positives.

The results of the proposed extended model further reinstates the combined effectiveness of DDoS defense mechanism and the spam filtering solution in bringing down the resource wastage, thereby improving the grid resource availability. This simulation uses a static set of attributes to track the frequencies of the attribute-value pairs. This could be made more dynamic to adapt to varying attacks.

6.2 SCOPE FOR FUTURE WORK

This work may be extended in future to include inference engine to define dynamic firewall rules automatically based on the goals defined at the LTM at ADA to counter DDoS attacks more effectively. Also more complete intrusion detection features could be included to further secure the trustworthy Hierarchical Three-tier Broker Architecture. Profile-based complete intrusion detection system may be incorporated at the ADA level to further improve the very important requirement of availability of grid resources. The issues of using trust management in mobile ADHOC grid and its implementation may also be considered in future work.