4 SUMMARY AND CONCLUSION

The multi agent systems open a way to the malicious agents who can falsify the service completion by respondent selection. The motivation of an attacker can be either selfish or malicious. Being selfish, an attacker may respond maliciously against a service request. While being malicious, an attacker may respond to service request, though he unable to give service, thus causing chaos and interference for service seeking agents.

Networking technology of computers and communication systems, from closed network have evolved to open network, now accessible publicly. Trust and security issues have become critically important with the fast expansion of multi-agent systems or applications such as the E-business systems, Agent-to-Agent, Grid and Semantic Web which are open, anonymous and dynamic in nature. A multi-agent system is one in which many agents run concurrently, communicating among them and working toward either individual goals or a common objective. Individual components in each system are both autonomous and flexible in their actions and due to this attackers/malicious agents are always seeking to spread malicious content in the multi-agent network. One of the solutions to minimize the threats is to evaluate the trust and reputation of interacting agents. Trust evaluation models use different standards in its opinion and with the existence of fraud and unreliable services, agents face dilemma in identifying and selecting efficient service with increasing choice of chance. With these research problems in mind, this thesis proposed a reputation-based dynamic trust evaluation model.

The divergent properties such as control flow, computed values, and ordering events of distributed computing open doors for several security vulnerabilities. The ongoing research given considerable attention on Trusted and reputation based respondent selection in order to establish secure and reliable service exchange. However, these mechanisms compromised to the specific attacks like Eminence Tainting and Colluded Eminence Boosting, which are easily degrade the effectiveness of trust and reputation based distributed service exchange models. Hence it is obvious that proposal
of novel and robust trust and reputation based secure communication protocol for service exchange practices like B2B, B2C ecommerce models is still a considerable research objective. This thesis proposed a multi-objective model that aimed to identify the reputation of a respondent involved. The factors reputation score, reputation update frequency" and "reputation update diversity" are proposed as multi-objectives to estimate the eminence of the agent. Along the side the proposed model also alert to defend the attacks such as "bad mouthing", "colluding", and “ballot stuffing”.

Here in this thesis the reputation aware agent selection strategy was proposed. The said model is significant and optimal towards multi agent systems. The devised reputation aware agent selection model is decentralized in which each buyer agent separately maintains the reputation of seller agents it has interacted with. Buyer agents exchange seller reputation information with each other when evaluating sellers for purchase decisions. The proposed model addresses subjectivity in buyers’ opinions and the possibility of variations in buyers’ ratings of sellers. The devised reputation aware agent selection model is designed for multi agent systems in an ecommerce environment and provides a method for computing the direct rating of the sellers based on the reputation provided by the buyer’s to a respective seller. The goal of this proposal is to optimize the buyer’s performance by helping it choose a seller who is offering the quality of service. The devised reputation aware agent selection model devised a reputation verification and update models, and is conceptually a protocol, that uses direct experiences and witness information of an individual, considers reputation/trust as a subjective property, considers reputation/trust to be a single context as it is specifically designed for ecommerce market, assumes that agents can cheat, and information exchanged is a continuous measure. The proposed model does not compute a separate value for the reliability of the trust value, but instead incorporates the trustworthiness of the witnesses, the experience of the witness, and the age of the information while computing trust and reputation value. The experiment results indicating that the model devised here is proven to be robust under divergent number of respondents.