CHAPTER 9

CONCLUSION AND

FUTURE SCOPE
CHAPTER-9

CONCLUSION AND FUTURE WORK

9.1 Conclusion

Wireless Sensor Networks in this stage of deployment are prone to attacks that are destructive enough to conquer simple security parameters and disrupt the configuration of system. With the realization of deployment locality, the systems may not be reachable for healing in case of intrusion, route gaps and detection of malicious nodes. The request of reliable network motivated the studies for development of autonomic computing for interacting with the challenges susceptible to sensor networks. Autonomic computing is the deterministic approach in wireless sensor networks which powers the sensor nodes with brainpower to cope with the attacks of undefined structure.

The study of self-computing is carried in four steps. The nodes placed near the destination point consumes high amount of energy compared to the remaining nodes. To maintain the system efficiency the nodes are required to expand least and almost same amount of energy. The self-configuration scheme bifurcate the network based on nodes energy. The node balancing technique classifies the nodes with energy above threshold value in the high modulation index and the nodes with energy below threshold value in the low modulation index. To our surprise, the results for dynamic power constraints were worse than static constraints. The reason is due to the fact that dynamic constraints are more conservative than static ones and therefore more unused energy remains in the nodes after a path is "lost" due to power-outage in one or more nodes.

In wireless sensor networks, the energy limitations of nodes play a crucial role in designing any protocol for implementation. In addition, Quality of Service metrics such as delay, data loss tolerance, and network lifetime expose reliability issues when designing recovery mechanisms for clustering schemes. These important characteristics are often opposed, as one often has a negative impact on the other. PSO has been a popular technique used to solve optimization problems in WSNs due to its simplicity, high quality of solution, fast convergence and insignificant computational burden. However, iterative nature of PSO can prohibit its use for high-speed real-time applications, especially if optimization needs to be
Conclusion and Scope of Future Work

carried out frequently. PSO requires large amounts of memory, which may limit its implementation to resource-rich base stations. Literature has abundant successful WSN applications that exploit advantages of PSO. Data-aggregation needs frequent distributed optimization, and fast solutions: Thus PSO moderately suits it. Static deployment, localization and clustering are the problems solved just once on a base station: Thus PSO highly suits them.

The transmission accuracy of the system is the concerned parameter in many research works. The accuracy can be monitored by various watch mechanisms out of which the Forward error correction codes resulted as the best choice of candidates. The deployment of Reed Solomon Code in wireless sensor network is the novel approach under the category of Forward error correction codes segment. The RS code detects and corrects multiple random symbol errors by adding $t$ check symbols in data. The RS code correct up to $[t-2]$ symbols and can detect up to any combination of $t$ erroneous symbols. In this scheme the performance index degrades with the decrease in SNR value.

Self-Protection of the system against the attacks is an indispensible factor in reliability of the system. Out of all attacks two internal attacks i.e. intrusion detection and Black hole node attack are considered for experimental work. The study of scheme confirmed that the mitigation of these will also cope with the attacks of similar categories with same destructive power. The S-Box architecture scheme is the basic component of symmetric component of symmetric key algorithms for performance of substitution. In block ciphers S-Box obscure the relationship between key and cipher text.

9.2 Future Scope

The future scope of the subject can be found in applications that are feasible and practical enough to satisfy all four parameters of computing to solve various issues in environment of autonomic grid. The future work focuses combining security measures with the work and overall synchronization algorithm for authentication, authorization and process of communication.