Fault-Tolerant Clustering Topology Evolution Mechanism of Wireless Sensor Networks

Abstract

- Wireless sensor networks (WSNs) are often subject to failures caused by energy depletion, software or hardware fault of nodes, environmental events, hostile attacks, and other reasons. It is critical to ensure a WSN application system is available during some presence of fault or interruption.
- Recent work in topology control has shown that a reasonable topology can improve the robustness of WSN. However, due to the limited resource of sensor nodes, topology control cannot easily tradeoff between fault tolerance and energy saving.
- To address this issue, we present a regular hexagonal-based clustering scheme (RHCS) and a scale-free topology evolution mechanism (SFTEM) for WSNs, that increases network survivability as well as maintains energy balance.

- RHCS uses a regular hexagonal structure for clustering sensor nodes, which satisfies at least 1-coverage fault-tolerance. SFTEM combines the reliability of RHCS with scale-free properties to connect clusters to form a robust WSN, which exploits the synergy between reliable clustering scheme and topology evolution, and can tolerate comprehensive faults including random failure and energy failure. In addition, to evaluate the performance of SFTEM, the simulation experiments were carried out to compare three factors including fault-tolerance, intrusion-tolerance and energy balance with other methods in literature. The simulation results show that, the performance of SFTEM is superior to those of the referenced topology evolution mechanisms of WSNs.

Existing system

- The sensor nodes in WSNs are easy to breakdown caused by energy depletion or natural disaster and deliberate attack [11], [12]. In addition, the failed sensor nodes would reduce the coverage of the network, would split originally connected network, and even lead to an entire global network paralysis.
- Wireless sensor networks (WSNs) are often subject to failures caused by energy depletion, software or hardware fault of nodes, environmental events, hostile attacks, and other reasons. It is critical to ensure a WSN application system is available during some presence of fault or interruption.

Hardware requirement

Processor	Pentium –III
Speed	1.1 Ghz
RAM	256 MB(min)
Hard Disk	20 GB
Floppy Drive	1.44 MB
Key Board	Standard Windows Keyboard
Mouse	Two or Three Button Mouse
Monitor	SVGA

Software requirement

• Operating System	-	Windows 7/8
• Application Server	-	Tomcat 5.0
• Front End	-	JAVA
• IDE	-	NETBEANS 7.1
• Back-End	-	HEIDISQL 3.5

Proposed system

- we present a regular hexagonal-based clustering scheme (RHCS) and a scale-free topology evolution mechanism (SFTEM) for WSNs, that increases network survivability as well as maintains energy balance. RHCS uses a regular hexagonal structure for clustering sensor nodes, which satisfies at least 1-coverage fault-tolerance.
- SFTEM combines the reliability of RHCS with scale-free properties to connect clusters to form a robust WSN, which exploits the synergy between reliable clustering scheme and topology evolution, and can tolerate comprehensive faults including random failure and energy failure.
- In addition, to evaluate the performance of SFTEM, the simulation experiments were carried out to compare three factors including fault-tolerance, intrusion-tolerance and energy balance with other methods in literature.

Conclusion

- WSNs are susceptible to failure due to the vulnerability of sensor nodes and attacks from malicious intruders. Hence, the fault-tolerance is an important issue in WSN applications. In this paper, we construct a regular hexagonal-based clustering scheme (RHCS) of sensor networks and analyze the reliability of RHCS based on Markov model.
- Then, we present a scale-free topology evolution mechanism (SFTEM). We also analyze the dynamic characteristics of SFTEM using mean-field theory. Simulation results show that the node degree distribution of SFTEM follows a power law distribution, and both the fault-tolerance and intrusion-tolerance of RHCS outperform other models.

Reference

- [1] Anand, S., and M. R. K. Keetha. "FPGA implementation of artificial Neural Network for forest fire detection in wireless Sensor Network," *in Proc. 2nd Int. Conf. Comput. Commun. Technol. (ICCCT),* Apr. 2017, pp. 265-270.
- [2] Deepa, S., et al. "Energy conservative data transmission using Z-Mac technique in wireless sensor network for environmental monitoring," *in Proc. Int. Conf. Technol. Innov. Agricul. Rural (TIAR),* July. 2016, pp. 194-199.
- [3] Azzabi, Tarek, H. Farhat, and N. Sahli. "A survey on wireless sensor networks security issues and military specificities," *in Proc. Int. M&N,* Oct. 2013, pp. 68-73.
- [4] Scarpato, G., et al. "A wireless network as support to the monitoring of Campi Flegrei volcano in Italy," *in Proc. Int. Workshop on Measurements and NETWORKING* IEEE, 2013:68-73.