Abstract

Wireless Sensor Networks (WSNs) consist of tiny, low cost sensor nodes with limited processing capability and communication bandwidth which are deployed in large number, especially in remote and hostile areas. Typically, sensor nodes are battery powered and replacement or recharge of battery is not feasible in most of the cases. The self-organized sensor nodes form a temporary network without predefined network infrastructure and centralized network administration. The unique features of WSNs make them popular in a variety of application areas such as climatic data gathering, seismic and acoustic underwater monitoring, industrial control and monitoring, intelligent agriculture, surveillance and security, military applications, health care and many more.

Sensor nodes are generally operated in standby mode and then, suddenly become active after detecting event in the surrounding area. The resulting effect is the generation of large and sudden impulses of data which would be delivered to the sink or the base station without disrupting the performances of the sensing operations. When large numbers of sensor nodes are active simultaneously in transmit mode, there is a high chance of packet collisions followed by network congestion. It is one of the major bottleneck in resource constrained WSNs, especially for large networks, where the traffic loads exceed the available capacity of the resources. Congestion causes buffer overflow, packet drops and re-transmission of packets due to the limited buffer size of the sensor node. It reduces precious battery life of the sensor nodes due to the additional computation and communication overhead, which in turn decreases network lifetime, degrades network performance and Quality of Services. Moreover, the special characteristics of WSNs make them vulnerable to various types of security attacks and some security attacks have direct impact on network congestion. For example, HELLO flood attacks, Jamming attacks, Sybil attacks and Node replication attacks aggravate congestion by flooding the network with fake messages, jamming intermittently, re-transmitting same message several times and

creating false node identification respectively. In this way, the congestion created by the faulty malicious nodes plays an important role in the overall congestion of the WSNs.

The researchers throughout the globe have proposed several energy efficient routing algorithms to maximize the network lifetime. But unfortunately, most of the conventional data gathering and routing algorithms do not consider the congestion phenomenon and the impact of the security threats. Some congestion control algorithms for WSNs are reported in the literature, but most of them do not consider the role of the malicious nodes. The traditional cryptographic security solutions are not suitable for resource limited WSNs. Nowadays, the concept of trust is considered as an alternative method, which has been used for getting secured and trustworthy data routing. The integration of trust and congestion control in data routing is the new idea, where the faulty malicious nodes are detected and isolated from the data routing path, causing reduction of network congestion. This is the largely open research domain and very few research efforts have been reported in this direction. To cater this problem, the present research study on trust based congestion control has been undertaken which has a lot of potential to develop in the near future.

In this thesis, the merits of the trust based congestion control over the conventional congestion control algorithms, in terms of network lifetime and throughput, have been argued. In this context, the types of congestion and their effects, basic principle of congestion control and challenges of congestion control in WSNs have been discussed. The concept of trust is discussed in brief and the relation of congestion control with trust management is explained.

In *Chapter 1*, problem overview, objective and the motivation of the present research study is discussed.

Chapter 2 includes literature survey and review of the existing congestion control algorithms. The commonly occurred security attacks in WSNs are discussed in brief and the existing trust evaluation methods are also studied extensively in this chapter.

In *Chapter 3,* two new trust integrated data routing algorithms, ITLSRP and FTSRP are presented by using Link State Routing Protocol as the basic data routing scheme.

In *Chapter 4,* a new congestion control protocol is proposed, where selection of routing path is modeled on the basis of traffic sharing with the help of Genetic Algorithm.

In *Chapter 5,* two new fuzzy algorithms (TFCC and TCEER) for trust based congestion control in Wireless Multimedia Sensor Networks are proposed where multimedia sensor nodes are deployed for multimedia applications.

In *Chapter 6,* a new approach for congestion aware energy efficient data routing algorithm (TC-ACO) is presented by utilizing Ant Colony Optimization technique.

In *Chapter 7,* CET-PS algorithm is discussed, in which three of our previously proposed trust based congestion aware data routing algorithms (TFCC, TCEER and TC-ACO) are integrated into a single protocol suite, where the routing path is selected adaptively on the basis of the congestion status of the sensor node and the parameter called Composite Protocol Efficiency (CPE).

In *Chapter 8,* a new trust based congestion control algorithm (TCR-FC) is proposed, where dedicated state-of-the-art Fuzzy Co-processor (FCP) architecture is designed for fuzzy computation. The proposed model is implemented in Field Programmable Gate Array.

Finally, in *Chapter 9,* the thesis is concluded by summarizing the overall findings. It also includes suggestions for the future direction of research in this domain.

In brief, the main contributions of the thesis are listed as:

- Detailed study of the existing congestion control algorithms and trust based security solutions, explanation of the requirement of trust based congestion control in WSNs.
- Proposal of two new trust integrated data routing algorithms (ITLSRP and FTSRP).
- Proposal of six novel algorithms (GACCTR, TFCC, TCEER, TC-ACO, CET-PS and TCR-FC) for trust based congestion control in WSNs.
- Verification of the merits of the proposed trust based congestion control models over the conventional congestion control algorithms, in terms of network lifetime and throughput of the network, using simulation and performance analysis.