IEEE 2015 Wireless Sensor Network Project List :

1. **A Lightweight Secure Scheme for Detecting Provenance Forgery and Packet Drop Attacks in Wireless Sensor Networks**

2. **Combining Cryptographic Primitives to Prevent Jamming Attacks in Wireless Networks**

The Open Nature of wireless medium leaves an intentional interference attack, typically referred to as jamming. This intentional interference with wireless transmission launch pad for mounting Denial-Of- Service attack on wireless networks. Typically, jamming has been addresses under an external threat model. However, adversaries with internal knowledge of protocol specification and network secrets can launch low-effort jamming attacks that are difficult to detect and counter. In this work we address the problem of jamming attacks and adversary is active for short period of time, selectively targeting the messages of high importance. We show that the selective jamming attacks can be launched by performing real-time packet classification at the physical layer. To mitigate these attacks, we develop three schemes that prevent realtime packet classification by combining cryptographic
primitives with physical-layer attributes. They are Strong Hiding Commitment Schemes (SHCS), Cryptographic Puzzles Hiding Schemes (CPHS), All- Or-Nothing Transformation Hiding Schemes (AONTSHS). Random key distribution methods are done along with three schemes to give more secured packet transmission in wireless networks.

3. **Fault Node Recovery Algorithm for a Wireless Sensor Network**

This paper proposes a fault node recovery algorithm to enhance the lifetime of a wireless sensor network when some of the sensor nodes shut down. The algorithm is based on the grade diffusion algorithm combined with the genetic algorithm. The algorithm can result in fewer replacements of sensor nodes and more reused routing paths. In our simulation, the proposed algorithm increases the number of active nodes up to 8.7 times, reduces the rate of data loss by approximately 98.8%, and reduces the rate of energy consumption by approximately 31.1%.

4. **"Efficient Sensor Node Authentication in Wireless Integrated Sensor Networks Using Virtual Certificate Authority"**

Wireless Sensor Network (WSN) is used for collecting the information from the environment. WSN consists of large number of Sensor Nodes (SN). To implement security during the transmission of data from one node to another node, different security techniques are used. Authentication is an essential requirement in sensor network pursuing security. But the Wireless Sensor Networks are very difficult to secure due to its dynamic and ad-hoc nature. To analyze the security issues that arise try to solve by integrating Wireless Sensor Networks (WSN) with the mobile network and can utilize the combined capabilities of both networks. To address the problem of authentication in WSNs this paper presents propose an efficient and secure framework which provide authentication to a roaming sensor node while allowing a sensor node to move across multiple WSNs. The proposed key management technique to provide authentication is by using Virtual Certificate Authority (VCA) which is designed especially for distributed Adhoc network.

5. **Adaptive and Secure Load-Balancing Routing Protocol for Service-Oriented Wireless Sensor Networks**

Service-oriented architectures for wireless sensor networks (WSNs) have been proposed to provide an integrated platform, where new applications can be rapidly developed through flexible service composition. In WSNs, the existing multipath routing schemes have demonstrated the effectiveness of traffic distribution over multipaths to fulfill the quality of service requirements of applications. However, the failure of links might significantly affect the transmission performance, scalability, reliability, and security of WSNs. Thus, by considering the reliability, congestion control, and security for multipath, it is desirable to design a reliable and service-driven routing scheme to provide efficient and failure-tolerant routing scheme. In this paper, an

evaluation metric, *path vacant ratio*, is proposed to evaluate andthen find a set of link-disjoint paths from all available paths. A congestion control and load-balancing algorithm that can adaptively adjust the load over multipaths is proposed. A threshold sharing algorithm is applied to split the packets into multiple segments that will be delivered via multipaths to the destination depending on the path vacant ratio. Simulations demonstrate the performance of the adaptive and secure load-balance routing scheme.

6. Throughput-Optimal Scheduling in Multihop Wireless Networks Without Per-Flow Information

In this paper, we consider the problem of link scheduling in multihop wireless networks under general interference constraints. Our goal is to design scheduling schemes that do not use per-flow or per-destination information, maintain a single data queue for each link, and exploit only local information, while guaranteeing throughput optimality. Although the celebrated back-pressure algorithm maximizes throughput, it requires per-flow or per-destination information. It is usually difficult to obtain and maintain this type of information, especially in large networks, where there are numerous flows. Also, the back-pressure algorithm maintains a complex data structure at each node, keeps exchanging queue-length information among neighboring nodes, and commonly results in poor delay performance. In this paper, we propose scheduling schemes that can circumvent these drawbacks and guarantee throughput optimality. These schemes use either the readily available hop-count information or only the local information for each link. We rigorously analyze the performance of the proposed schemes using fluid limit techniques via an inductive argument and show that they are throughput-optimal. We also conduct simulations to validate our theoretical results in various settings and show that the proposed schemes can substantially improve the delay performance in most scenarios

7. LDTS: A Lightweight and Dependable Trust System for Clustered Wireless Sensor Networks

The resource efficiency and dependability of a trust system are the most fundamental requirements for any wireless sensor network (WSN). However, existing trust systems developed for WSNs are incapable of satisfying these requirements because of their high overhead and low dependability. In this work, we proposed a lightweight and dependable trust system (LDTS) for WSNs, which employ clustering algorithms. First, a lightweight trust decision-making scheme is proposed based on the nodes' identities (roles) in the clustered WSNs, which is suitable for such WSNs because it facilitates energy-saving. Due to canceling feedback between cluster members (CMs) or between cluster heads (CHs), this approach can significantly improve system efficiency while reducing the effect of malicious nodes. More importantly, considering that CHs take on large amounts of data forwarding and communication tasks, a dependability-enhanced trust evaluating approach is defined for cooperations between CHs. This approach can effectively reduce networking consumption while malicious, selfish, and faulty CHs. Moreover, a self-adaptive weighted method is defined for trust aggregation at CH level. This approach surpasses the limitations of traditional weighting methods for trust factors, in which weights are assigned subjectively. Theory as well as simulation results shows that LDTS demands less memory and communication overhead compared with the current typical trust systems for WSNs.