Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2013, Article ID 505313, 2 pages
http://dx.doi.org/10.1155/2013/505313

Hindawi

Editorial

Dependability and Security for Wireless Ad Hoc and Sensor Networks and Their Applications

Dong Seong Kim,[1] Sunho Lim,[2] and Wensheng Zhang[3]

[1] *Department of Computer Science and Software Engineering, University of Canterbury, Private Bag 4800, Christchurch 8140, New Zealand*
[2] *T[2] WISTOR: TTU Wireless Mobile Networking Laboratory, Department of Computer Science, Texas Tech University, Lubbock, TX 79409, USA*
[3] *Wireless Networks and Systems Laboratory, Department of Computer Science, Iowa State University, Ames, IA 50011, USA*

Correspondence should be addressed to Dong Seong Kim; dongseong@gmail.com

Received 7 July 2013; Accepted 7 July 2013

Wireless ad hoc and sensor networks have received considerable attention due to the potential applications in civil, military, and homeland security and will play a major role to provide a ubiquitous communication infrastructure. To realize this vision, wireless ad hoc and sensor networks and their applications should be dependable and should run continuously and reliably without interruption in the presence of hardware/software faults and security attacks. Hence, dependability and security are key challenging issues and should be incorporated in designing and developing wireless ad hoc and sensor networks and their applications. This special issue is focusing on the latest research in the area of dependability and security issues for Wireless Sensor Networks (WSNs), Mobile Ad hoc Networks (MANETs)and their applications. We have accepted a few papers that address the previous key aspects in WSNs, MANETs and Smart Grid.

The paper "*hierarchical node replication attacks detection in wireless sensor networks*" proposes a new hierarchical distributed algorithm for detecting node replication attacks using a Bloom filter mechanism and a cluster head selection. Extensive simulation results show that the proposed idea is really efficient with a really high detection probability of replicated nodes.

The paper "*A counterattack-detection scheme in transmission time-based wormhole detection methods*" proposes a counterattack-detection scheme in transmission time-based wormhole detection method using three phases including detection of wormhole attacks, detection of counterattacks, and threshold update. Simulation results show that the proposed method has high reliability for detecting both wormhole attacks and the attacker's counterattack.

The paper "*anonymous cluster-based MANETs with threshold signature*" proposes a secure security system with anonymity for cluster-based MANETs and a threshold signature scheme without pairing computation to protect the privacy of nodes. It shows that the proposed scheme satisfies most properties for an anonymous security system and effectively copes with dynamic environments with greater efficiency by using secret sharing schemes.

The paper "*perturbation-based schemes with ultra-light-weight computation to protect user privacy in smart grid*" develops three perturbation-based algorithms to protect user privacy without using cryptographic primitives in Smart Grid. The proposed random perturbation, random walk, and distributed-bounded algorithms are extensively analyzed to justify their lower computational overhead and applicability.

The paper "*BRS-based robust secure localization algorithm for wireless sensor networks*" proposes a localization algorithm to reduce the impact of malicious nodes in WSNs. The proposed algorithm consists of trust evaluation based on the beta reputation system and the weighted Taylor-series least-squares method to efficiently detect malicious nodes and coordinate nodes, respectively. Extensive simulation results show the effectiveness of detecting malicious nodes and improving localization accuracy.

The paper "*public verifiability secret sharing scheme with provable security against chosen secret attacks*" defines a new secure model of secret sharing, proposes the use of the Lagrange interpolation and the bilinear cyclic groups to construct an efficient publicly verifiable secret sharing scheme on the basis of this model, and demonstrates that the new design is provably secure against adaptively chosen secret attacks based on the decisional bilinear Diffie-Hellman problem.

Dong Seong Kim
Sunho Lim
Wensheng Zhang