

Submission ID	Title
2	Sybil Attack Detection in a Hierarchical Sensor Network
14	Detecting Bogus BGP Route Information: Going Beyond Prefix Hijacking
16	Securing Personal Network clusters
17	Simple Cross-Site Attack Prevention
18	Mitigating Denial-of-Service Attacks in MANET by Distributed Packet Filtering: A Game-theoretic Approach
28	Securing Pseudo Identities in an Anonymous Peer-to-Peer File-Sharing Network
29	Implications of Radio Fingerprinting on the Security of Sensor Networks
38	Misleading and Defeating Importance-Scanning Malware Propagation
51	SET: Detecting node clones in Sensor Networks
54	A BitTorrent-Driven Distributed Denial-of-Service Attack
64	Anonymity and Security in Delay Tolerant Networks
65	Secure Crash Reporting in Vehicular Ad hoc Networks
71	Simple Authentication for the Web
80	An Assessment of VoIP Covert Channel Threats
82	PWC: A Proactive Worm Containment Solution for Enterprise Networks
85	Deception Framework for Sensor Networks
88	Securing network location awareness with authenticated DHCP
94	Using Reoccurring Costs for Reputation Management in Peer-To-Peer Streaming Systems
96	Breaking EMAP
101	A Layout-Similarity-Based Approach for Detecting Phishing Pages
104	Parameterizing Access Control for Heterogeneous Peer-to-Peer Applications
120	OpenFire: Using Deception to Reduce Network Attacks
123	Detecting Worms via Mining Dynamic Program Execution
15	Intrusion Detection Technology Based on CEGA-SVM
44	Efficient Mechanisms to Provide Convoy Member and Vehicle Sequence Authentication in VANETs
55	Self-Healing Wireless Sensor Networks
58	Enhancing Frequency-based Wormhole Attack Detection with Novel Jitter Waveforms
59	Global Interoperability of National Security and Emergency Preparedness (NS/EP) Telecommunications Services
83	A Feedback Reputation Mechanism to Secure the Optimized Link State Routing Protocol
91	Secure Lightweight Tunnel for Monitoring Transport Containers
93	Modeling and Detection of Complex Attacks