VULNERABILITY OF SECURE WIRELESS NETWORKS: A Toolkit for Network Visualization

DAVID SLATER — UNDERGRADUATE (EE), **PATRICK TAGUE** — GRADUATE STUDENT (EE), AND **PHILLIP LEE** — GRADUATE STUDENT (UNIVERSITY OF CALIFORNIA, SAN DIEGO)

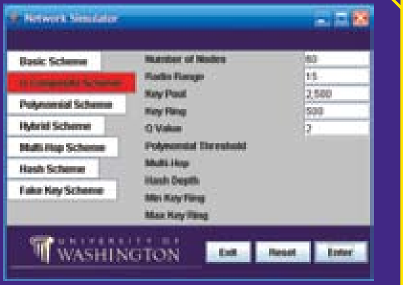
Wireless sensor networks (WSNs) are becoming a critical component for safety monitoring and surveillance systems. For these applications, properties such as integrity, confidentiality and availability of sensed data are crucial and require secure network protocols to establish trust between individual sensor nodes. However, WSNs present unique challenges including resource constraints and scalability requirements. This work analyzes and visualizes the structure and vulnerability of WSNs where symmetric cryptographic keys are assigned to sensor nodes prior to deployment, a solution known as key predistribution.

To establish trust and connectivity in a deployed sensor network, each pair of neighboring nodes must establish a secure communication link with high probability. Due to memory constraints and the randomness of node deployment, links are constructed using symmetric cryptographic keys, which are shared by a potentially large number of sensor nodes. The absence of tamper-proof hardware may allow a malicious adversary to acquire cryptographic keys by compromising sensor nodes. Hence, a secure link between two nodes may be compromised independently of either node.

In prior work, researchers analyzed the security of key predistribution schemes in homogeneous WSNs by computing the average fraction of links that remain secure after a given number of node compromises. This work models node compromise attacks which heuristically achieve a similar worst-case quantity with respect to various metrics. Furthermore, the model is generalized to include heterogeneous wireless networks.

A simulation toolkit has been developed to visualize the structure of WSNs using key predistribution. It implements a variety of key predistribution schemes, and allows for significant variation in network and security parameters. Many attack heuristics can be utilized, and the effects can be qualitatively visualized and quantitatively measured on that network.

The implications of this work are two-fold. The adversarial model provides a deeper understanding of the key predistribution security protocols in a realistic setting. The simulation toolkit also serves as a visual aid and educational tool for understanding the structure and vulnerability of wireless sensor networks.EE

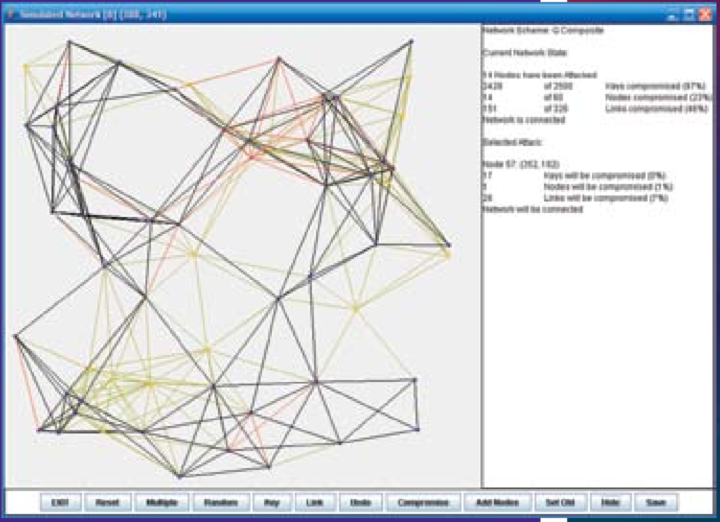


Network Simulator

Basic Scheme
Q-Composite Scheme
Polynomial Scheme
Hybrid Scheme
Multi-Hop Scheme
Hash Scheme
Fake Key Scheme

Number of Nodes: 60
Radio Range: 15
Key Pool: 2,500
Key Ring: 500
Q Value: 2
Polynomial Threshold
Multi-Hop
Hash Depth
Min Key Ring
Max Key Ring

THIS INTERFACE ALLOWS THE USER TO SELECT BETWEEN KEY PREDISTRIBUTION SCHEMES, AND GENERATE RANDOM NETWORKS BASED ON THE CORRESPONDING USER-SELECTED PARAMETERS.



Simulated Network [8] (188, 241)

Network Scheme: Q-Composite

Current Network State:

14 Nodes have been Attacked
2428 of 2500 Keys compromised (97%)
14 of 60 Nodes compromised (23%)
151 of 326 Links compromised (46%)
Network is connected

Selected Attack:

Node 57: (352, 182)
17 Keys will be compromised (0%)
1 Nodes will be compromised (1%)
26 Links will be compromised (7%)
Network will be connected

THIS INTERFACE DISPLAYS THE RANDOMLY GENERATED NETWORK AND ALLOWS THE USER TO SELECT NODES TO COMPROMISE BASED ON VARIOUS ATTACK HEURISTICS. IT DISPLAYS NETWORK INFORMATION GRAPHICALLY AND TEXTUALLY, SHOWING THE POTENTIAL COMPROMISING EFFECTS OF THE SELECTED ATTACK IN RED AND GIVING THE NUMBER OF COMPROMISES IN THE TEXTBOX.

FACULTY ADVISOR: ***Professor Radha Poovendran*** **RESEARCH AREA:** ***Wireless Sensor Network Security***
GRANT/FUNDING SOURCE: ***National Science Foundation CAREER, Army Research Office PECASE***