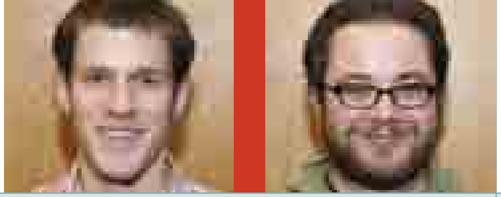


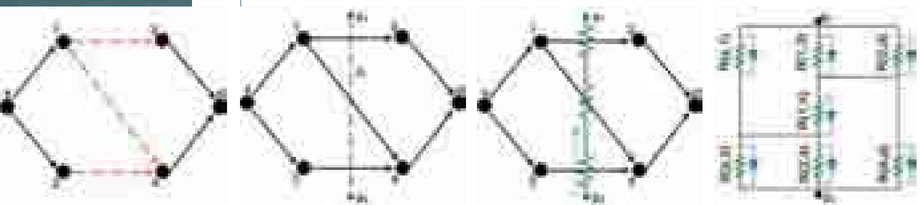
Using Electric Circuits to Evaluate Vulnerability in Wireless Network Routing

DAVID SLATER AND PATRICK TAGUE — Network Security Lab, Graduate Students (EE)

Evaluating security in wireless networks typically involves an independent analysis of the cryptographic security of each network link. However, since a routed message traverses multiple links en route from source to destination, the ability for an adversary to compromise the message (known as the vulnerability of the message) is a function of the network topology, the security provided by each link, and the adversary's ability to compromise network links. This work develops a metric to evaluate message vulnerability by mapping the compromised links in a given network topology to a current flow through an electric circuit.

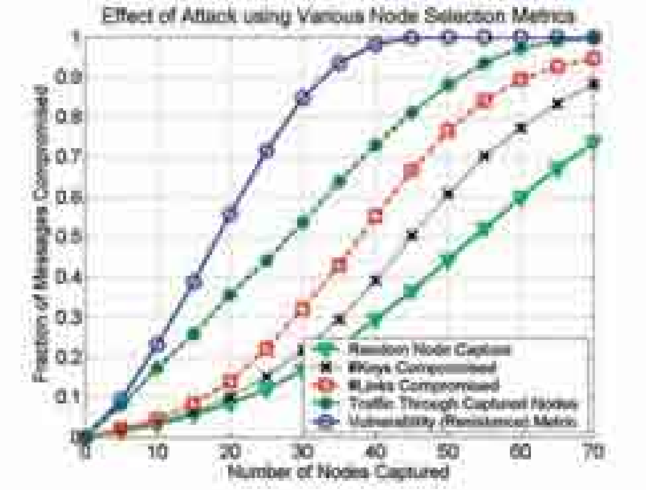
An adversary compromises link security by capturing network nodes and recovering the cryptographic keys stored in memory. The metric is thus developed from the adversary's perspective to optimize the node capture attack, yielding the worst-case message vulnerability from the network perspective.

The metric is developed by focusing on a single source-destination pair in the network and modeling the message routing as a directed flow (figure A). Any message in the source-destination flow is compromised when the adversary compromises an edge cut set of the flow. Each cut set (figure A) corresponds to a possible attack solution for the adversary and is indicated by a possible attack path (figure B). By associating an electrical resistance with each link to be compromised, equal to the number of keys securing the link, the attack path can be mapped to a path of current flow (figure C). By considering all possible attack paths, the directed source-destination flow is mapped to an electric circuit (figure D).



The figure illustrates the mapping from the directed graph representing the route to an electric circuit. In A, a possible edge cut set is indicated by dashed lines. In B, the edge cut is represented as a curve crossing the edges in the cut set. In C, the curve is replaced by a wire, and a resistor is inserted where the curve crosses each edge. In D, the circuit is constructed by combining wires and resistors for all possible edge cuts. The parallel diode for each resistor maintains edge directionality.

By evaluating the equivalent resistance of the circuit constructed from the source-destination flow, the adversary can improve the efficiency of the node capture attack by choosing to capture the node leading to the greatest decrease in equivalent resistance. The impact of such an attack is compared to similar attacks using other node selection metrics.



Five node capture strategies are compared for a network of 500 nodes in which each source sends fragments of each message over multiple paths to the destination. This is conducted in such a way that it forces the adversary to compromise an entire edge cut set of the route to recover the corresponding message.

The proposed metric provides a connection between protocols for message confidentiality and network routing. In the future, this metric will provide insight into the joint design of security and routing protocols that improve message vulnerability. eeKO8

Faculty Advisor: Professor Radha Poovendran
Collaborators: Jason Rogers, Naval Research Laboratory
Research Area: Wireless Network Security
Grant/Funding Source: Army Research Office, Office of Naval Research