The problem presented by this paper is that wireless 802.11 networks are very vulnerable at the MAC or transmission layer. The paper points network security has focused primarily on network access control rather than network availability. The use of a DoS attack would prevent rightful users access to the network and its resources by using various methods in order to shut down genuine traffic flow.

The paper shows that the current 802.11 protocol is vulnerable mainly because of the unauthenticated management frames of the protocol (e.g., ACK, RTS, CTS). By exploiting this vulnerability the researchers are able to develop two very effective DoS attacks against controlled laboratory networks and actual campus networks at USCD.

First the researchers had to slightly modify the firmware of the attacking NIC to allow them to modify the management packets that are to be injected into the network. Once this modification was complete the researchers experimented with two similar attacks; Deauthentication and Disassociation. Both of these attacks were extremely successful in essentially shutting down the network or any desired node in the network. These attacks were achieved by the attacker spoofing a message sent between a client and an access point which will deauthenticate a client and not allow it to send any data until it reauthenticates. The attacker can simply continue to send out this deauthentication message and completely shut out a client from the network. Researchers have provided a solution to this attack where they suggested implementing a delayed affect in executing any deauthentication for a few seconds to ensure that the client is done sending data. If the client sends data after the AP receives the deauthentication message the deauthentication message is discarded.

A second type of attack that the researchers developed but were not able to implement in a real environment was the Virtual carrier-sense attack. This attack involves the attacker modifying the NAV values across the network by asserting large duration fields in a RTS packet. This attack will prevent well behaved clients from accessing the network because they will believe it to always be busy. The attacker only has to repeat this attack about 30 times a second to shut down the network. There were no absolute solutions to this attack but some “good enough” solutions were presented.

This paper shows some very real vulnerability to the existing 802.11 networks and suggests some relatively simple solutions. My primary concern with the paper lies primarily with the fact that the authors present glorified kludges as defenses, rather than enhancements to the 802.11 standard. They point out that with the installed base of 802.11 networks, enhancing the standard to include authorization capabilities for maintenance is wishful thinking. Meanwhile, 802.11, like any telecommunications standard, is constantly evolving. Witness the introduction of the WPA and WPA2 encryption algorithms to 802.11 over the past few years. The authors pointed out some glaring potential weaknesses in the availability of 802.11 networks, but in terms of presenting real ideas for defending against attacks, they took a quick and easy way out.