A Study of Stealthy Denial-of-Service Attacks in Wi-Fi Direct Device-to-Device Networks

Ari Hadiks[1], Yu Chen[1], Feng Li[2], Bingwei Liu[1]
[1]*Department of Electrical and Computer Engineering, Binghamton University, SUNY, Binghamton, NY 13902*
[2]*Purdue School of Engineering and Technology, IUPUI, Indianapolis, IN 46202*

***Abstract*—Wi-Fi Direct technology enriches local services that enables social interactions off the grid. Allowing purely local connections among mobile devices, Device-to-Device (D2D) networks support more versatile proximity-based applications and reduce dependence on central entity. While the D2D paradigm allows more convenient information exchanging or resource sharing, it also brought new challenges. Information assurance and system security are top concerns users have. In this paper, we studied the impacts of Denial-of-Service (DoS) attacks in a D2D underlaying network. Our experimental results show that malicious users can effectively force the victim mobile device drop off its Wi-Fi connection to the access point (AP) without being detected by the AP or the cellular network. We expect this preliminary results can inspire more research in this raising area.**

***Keywords*-Wi-Fi Direct Connection, Denial-of-Service (DoS) Attacks, Device-to-Device (D2D) Networks.**

I. Introduction and Background

The past decade has witnessed the prosperity of online social networks and pervasive computing. The market of mobile devices, including smartphones and other portable wireless devices, has also been growing rapidly. More and more new social networking applications are developed for mobile platform and exploit proximity-based interaction [2]. These proximity-based applications enable users to find nearby friends, services, or other attractions. Presently, "check-in" is still the most common approach for these proximity-based applications. A user has to register and log-in at a centralized server and the location information is required. The application running on the server tracks where the user is and where her friends are.

There are several obvious disadvantages with the centralized service model. On one hand, it risks user's privacy and some users are reluctant to provide their location information to the server. On the other hand, the central server can be the point-of-failure or performance bottleneck. If the server is out of service or overloaded, users cannot get the results even if their friends are actually in vicinity. In fact, most of the location-based services only need local information and the help from a powerful central server is unnecessary if direct user-to-user communication is available.

Wi-Fi CERTIFIED Wi-Fi Direct provided by Wi-Fi alliance allows Wi-Fi devices connect to each other directly in a new convenient way without the need of a wireless access point (AP) [1]. In traditional wireless networks, all wireless devices connect to the AP or wireless router to communicate with multiple peers. In contrast, devices with Wi-Fi Direct capability can form a flexible and secure temporary network to communicate without an AP. Figure 1 shows two typical scenarios of Wi-Fi direct networks. In Scenario 1, Wi-Fi Direct enabled devices form a flexible and secure temporary network to communicate without an AP. Another useful paradigm is to share the cellular connection of a mobile phone like Scenario 2. Among all its attracting features, we believe that the enhanced support of Wi-Fi Protected Setup (WPS) [3] and flexible group formation could the main reasons that consumers will choose this new technology.

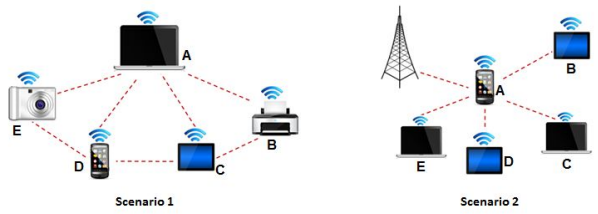

Figure 1. Typical Scenarios of Wi-Fi Direct Enabled D2D Networks.

Wi-Fi Direct devices have the capability of forming a more stable and secure device-to-device (D2D) underlaying network than traditional Ad Hoc networks. While such a D2D network enables users enjoy the convenience brought by the new technology, lack of thorough understanding in vulnerabilities and protection schemes makes security the top concern. Denial of Service (DoS) attacks are simple but effective weapon to disrupt legitimate activities and serve for the attackers goals. There is still not an ultimate defense method against DoS attacks because of well-known reasons: cheap cost for attackers and difficulties in distinguishing normal traffic from attacking traffic.

This paper reports our exploration on characteristics of DoS attacks on Android devices in D2D underlaying network environment. Our experimental study has shown that malicious devices can stealthily impair or even totally block the connection of legitimate devices in the underlaying network. And such an attack is very challenging to be detected by the AP or cellular network.

II. Experimental Results

A. Experimental Setup

Our experiment was conducted using five devices, which are organized like the Scenario 2 in Fig. 1. Device A is a

Samsung Galaxy Nexus smartphone, a Wi-Fi Direct enabled device with cellular radio connection; Device B and C are Google Nexus 7 tablets, Wi-Fi Direct enabled devices without independent data connections; Devices D and E were other two Samsung Galaxy Nexus smartphones without cellular radio connection. These devices form an Ad-Hoc Wi-Fi Direct Network with WPS and WPA2 security. The cellular data connection is a GSM/CDMA 3G/4G connection. A desktop computer worked as the Internet server that mobile devices would access.

Device A acts as an AP for Devices B through E to the server on the Internet. Download/Upload speed depends on the signal quality that Device A has to the Cell Tower. For all Internet communications, Device A acts like a normal router. For example, if Device B wishes to communicate to a server on the Internet, the server communicates with and only sees the IP of Device A. The server cannot communicate with or target any other device on a Wi-Fi Direct Network unless that device is the AP, here it is Device A.

B. Denial-of-Service Attack

Two DoS attack scenarios have been considered, where Device B is the attacker, with 250-threads, 512KB packet size, launching a PHP-based attack.

Scenario A: Device B launched an attack against the server on the Internet. Typically the Server had no trouble withstanding the attack. Because the Wi-Fi Direct underlaying network operated at a much higher bandwidth than Device A's data connection, this attack did not have much impact on communication between devices on the network. However, it consumed all of the remaining upload bandwidth on Device A's data connection, when Device A prioritized its own network communication at a higher level than the other devices' requests. The result was that Devices C, D, and E was not able to properly utilize Device A's internet connection. Device A also experienced a severe slowdown of its data speeds when it did not prioritize itself over its peers. The Server viewed that the DoS attack was launched by Device A and it can block requests from Device A.

Scenario B: Device B launched an attack against a victim, Device D, which was a Samsung Galaxy Nexus CDMA, (Rooted) hosting PHP webserver via Wi-Fi Direct Legacy. Because there was no router or moderator for the network, Device B effectively acted as a signal jammer for the network because its DoS attack against Device D has been received by all devices connected to the network, although only one device will actually respond to the attack. As this attack was within the underlaying network, it did not affect Device A's connection to the Internet. More specifically, we have observed the following results:

1) Attacking device was forced to quit the attack script because the processor was overloaded. Victim experienced roughly 20 seconds of varying performance loss.
2) Webserver on victim device was forced to restart, dropped all active connections, including non-malicious ones.
3) Webserver on victim was not forced to restart, however, Wi-Fi adapter dropped connection. This was uncommon and happened only few times.
4) Victim device's CPU kept at 100% load, being overheat, device was forced to restart. This happened rarely.

C. Distributed Denial-of-Service Attacks

Attacker 1 was Device B, a Google Nexus 7 tablet, with 100-threads, 512KB packet size, PHP-based attack. Attacker 2 was Device D, a Samsung Galaxy Nexus GSM, with 100-threads, 256KB packet size, PHP-based attack. The victim was Device E, a Samsung Galaxy Nexus CDMA, (Rooted) hosting PHP webserver via Wi-Fi Direct Legacy. By distributing the attack across two devices, it lessened the load on the attackers, allowing them to continue their attack until the victim device had to drop its own connection, restart the server, or forcibly restart the entire device due to overheating. If the victim device did not have a safeguard to force-restart after the CPU became overheated, it is highly likely that the device would have been damaged irreparably. More specifically, we have observed the following results:

1) Webserver on victim device was forced to restart dropped all active connections, including non-malicious ones.
2) Webserver on victim device was not forced to restart, however, its Wi-Fi adapter dropped connection.
3) Victim device's CPU kept at 100% load, being overheat, device was force to restart. This happened rarely.

III. CONCLUSIONS

In this paper, we've explored potential security problems in Wi-Fi Direct underlaying network, focusing on Denial-of-Service attacks. Our experimental results verified that malicious users can deprive innocent users' capability to enjoy the convenience given by the D2D network. Every attack test, excepting tests that resulted in the attacking device force-quitting the attack script, resulted in the victim dropping/loosing connection. Currently we are testing speed impact and developing detection/countermeasure schemes. As the D2D underlaying networks become more and more popular, a thorough understanding of attack surface and defense schemes is imperative. We hope this initial work can inspire deeper study and more efforts in this area.

REFERENCES

[1] D. Camps-Mur, A. Garcia-Saavedra, and P. Serrano, "Device to device communications with wifi direct: overview and experimentation," *IEEE Wireless Communications Magazine*, 2012.

[2] R. H. Kravets, "Enabling social interactions off the grid," *Pervasive Computing, IEEE*, vol. 11, no. 2, pp. 8–11, 2012.

[3] S. Viehböck, "Brute forcing wi-fi protected setup," *Wi-Fi Protected Setup. Retrieved March*, 2012.