Jamming Detection of Smartphones for WiFi Signals

Guolong Liu, Jinliang Liu, Yan Li, Liang Xiao, Yuliang Tang
Dept. of Communication Engineering, Xiamen University, 361000, China
Email: liuglong@foxmail.com

***Abstract*—In this paper, we investigate the impact of jamming attacks on the performance of smartphones regarding their WiFi access and propose a real-time jamming detection method based on the received signal strength indicator and the packet loss rate of WiFi signals, which can be easily implemented on Android smartphones. Experiments are performed to evaluate the proposed jamming detection method, in which universal software radio peripherals are used as jammers to block the WiFi signals between smartphone phones and wireless routers. Experimental results show that the proposed application can detect jamming attacks with small false alarm rate and miss detection rate.**

***Index Terms*—Packet loss rate, Received signal strength indicator, Denial of service, Jamming detection**

I. Introduction

Jammers that aim to block the legitimate transmissions by injecting jamming signals into wireless media can severely degrade network performance. Multiple types of jammers, such as constant jammers, random jammers, reactive jammers and smart jammers, have been found to attack wireless networks and have received extensive research attention [1]–[4]. Most existing anti-jamming techniques assume accurate jamming detection [5]–[8]. For example, a code tree system based on the unique properties of code sequences to detect jamming attacks in spread spectrum communication systems was proposed in [5]. In [6], a new jamming detection approach was presented using the measure of correlation among the error and the correct reception times. A Bayesian based distributed detection scheme was proposed in [7]. Based on signal strength, packet delivery ratio, and pulse width of the received signal, a multimodal scheme models different jamming attacks to detect and classify them in [8].

Jamming detection has become an important issue to improve security in wireless networks [9]–[14]. For example, signal-to-noise ratio has been used to detect jamming in [9]. In [10], an estimation-based jamming detection system was designed for time-critical networks. In addition, the packet delivery ratio, bad packet ratio and energy consumption amount can be used for jamming detection in [11]. Another jamming detection algorithm exploits the number of retransmissions and the packet delivery rate in [12]. In [13], a machine learning technique is applied to select the threshold in the jamming detection. Finally, the chip error rate can be used to detect jamming in direct sequence spread spectrum systems in [14].

The work of L. Xiao was partly supported by NSFC (61271242,61001072). The work of Y. Tang was supported by NSFC (61371081).

Most existing work on jamming detection focus on sensor networks and traditional wireless networks. In this paper, we investigate the jamming detection on smartphones based on the received signal strength indicator (RSSI) and packet loss rate (PLR). A jamming detection application is developed on Android smartphones for IEEE 802.11 systems. Experiments over universal software radio peripherals (USRPs) as jammers are performed to evaluate the impact of jamming attacks on the transmission between a wireless router and a smartphone. Experimental results show that our scheme can detects jamming accurately under various indoor scenarios.

The remainder of the paper is organized as follows. We present a jamming detection application for Android systems in Section II. Experimental results are provided in Section III. Finally, we conclude our work in Section IV.

II. Jamming Detection

In this paper, we consider the WiFi transmission between a smartphone and a wireless access point (AP), both within the coverage of a jammer based on USRP. The packet loss rate of the WiFi signals can be used to detect jamming attacks. More specifically, a high packet loss rate can result from jamming or a large channel fading between the smartphone and AP. Therefore, we present a jamming detection method for smartphone based on the packet loss rate and the received signal strength indicator obtained by the smartphone.

We implement a jamming detection application on an Android system, with the user interface as shown in Fig. 1. The underlying detection criterion is based on the observation that in the absence of jamming, a high signal strength usually corresponds to a low packet loss rate while the case with a low RSSI and a high packet loss usually results from a large radio propagation loss. Otherwise, in the presence of a jammer, both the signal strength and the packet loss rate are high.

As shown in Algorithm 1, the smartphone first obtains the RSSI values of the WiFi signals and then sends a set of packets to the wireless router by command $Ping$ and calculate the packet loss rate. The average packet loss rate and RSSI are denoted by $\bar{\mathrm{H}}$ and $\bar{\gamma}$, respectively. Two thresholds in the jamming detection are set based on the field test results in similar scenarios, including the packet loss rate threshold θ_p and the RSSI threshold θ_r, respectively. The packet delivery ratio and signal strength were applied to detect jamming attacks for wireless sensor network.

978-1-4799-8088-8/15/$31.00 ©2015 IEEE

Algorithm 1. Jamming detection for a smartphone.

Initialization: N, θ_p and θ_r;
Measure H_i and γ_i for the N packets sent by the AP;
$\bar{\mathrm{H}} \leftarrow E_{1 \le i \le N}[H_i]$
$\bar{\gamma} \leftarrow E_{1 \le i \le N}[\gamma_i]$
if $\bar{\gamma} > \theta_p$ and $\bar{\mathrm{H}} > \theta_r$ **then**
  Send jamming alarm
end if

If the jammer continually sends random or meaningless signals to the channel disregarding the MAC protocols but not strong enough to destroy the whole network, the propagation delay is very large. Therefore, if a packet has not been received by Android phone in a long time, assume that the packet has been lost. Based on the above description, we apply the statistics of packet loss rate and RSSI to detect jamming attacks. If high RSSI and high packet loss rate are detected at the same time, the smartphone declares that it has been jammed. Otherwise, the smartphone is not jammed.

Fig. 1. User interface of jamming detection application on Android smartphone.

III. Experimental Results

As shown in Fig. 2, experiments have been conducted to evaluate the jamming detection of smartphones in a $11.8 \times 7.2 \times 3$ m^3 office room, in which the sinusoidal jamming signals with jamming power -18.85 dBm were generated by USRP N210 located at [2.2, 5.6, 1.5] m, and a wireless router located at [11, 5.7, 1.5] m provided WiFi access at 2.412GHz, i.e., Channel 1 in 802.11n systems. In addition, the Android smartphone *XiaoMi* was placed in various locations as shown in Fig. 3 to connect with the router. In the experiment, the smartphone sent 3000 packets each with 1024 bytes to the wireless router in each position.

In the first experiment, a smartphone was placed at position #1 in Fig. 3, about 1.34 m from the jammer with jamming power ranging from -24 dBm to -18.2 dBm. As indicated in Fig. 4, the RSSIs measured by the smartphone are between -39 and -33 dBm, which are much less than the corresponding

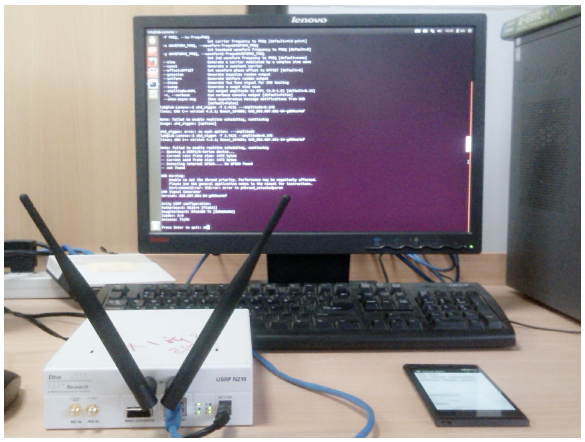

Fig. 2. Experimental settings, consisting of a USRP and an smartphone.

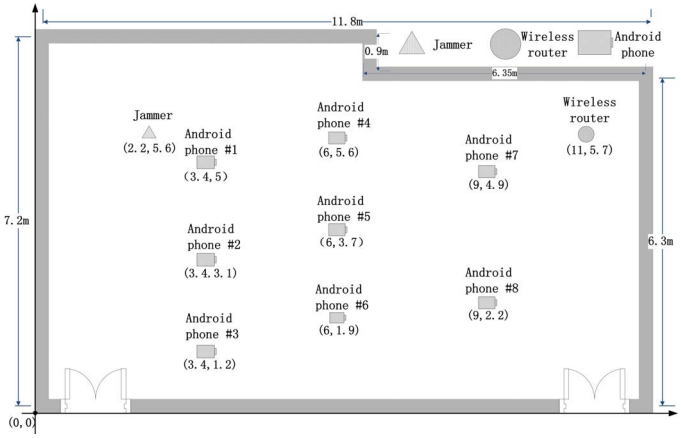

Fig. 3. Experiment topology, with smartphones and a jammer located in a $11.8 \times 7.2 \times 3$ m^3 room, and a USRP and a wireless router located at [2.2, 5.6, 1.5] m, [11, 5.7, 1.5] m, respectively.

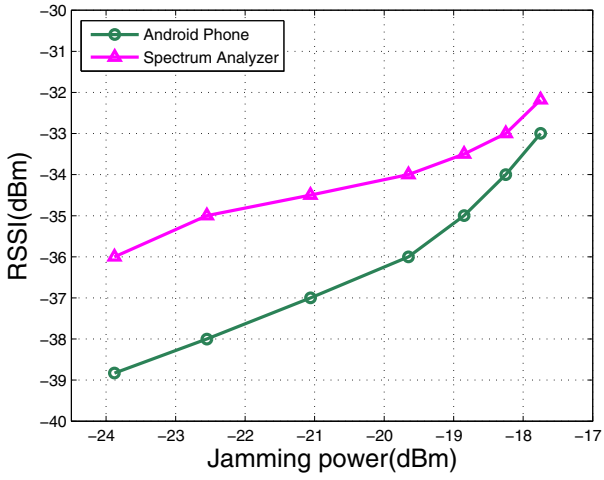

Fig. 4. RSSIs of WiFi beacon signals received by smartphones with jamming power in the range between -24 to -17 dBm.

values measured by a spectrum analyzer located at position #1 as well.

In the second experiment, a USRP was placed at a fixed location while a smartphone was placed in eight positions in Fig. 3. The packet loss rate and received signal strength indicator are shown in Fig. 5, indicating that the (PLR, RSSI) pair can be used to detect jamming. In addition, as shown in Fig. 6, the packet loss rates of the smartphone averaged over eight locations under jamming is much higher than that without jamming with the same RSSI.

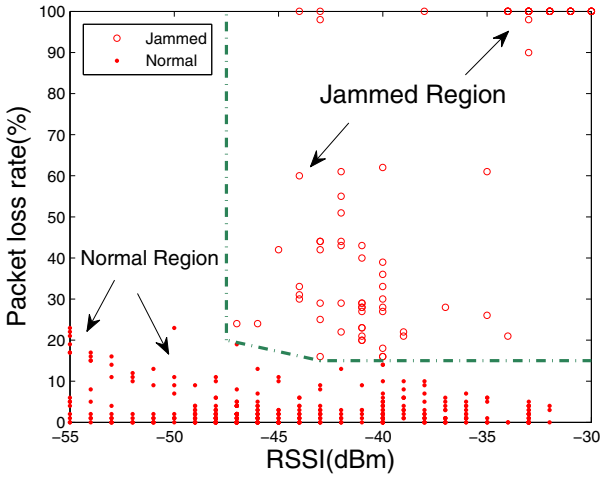

Fig. 5. Threshold determination method for smartphones to detect a jammer with jamming power -18.85 dBm.

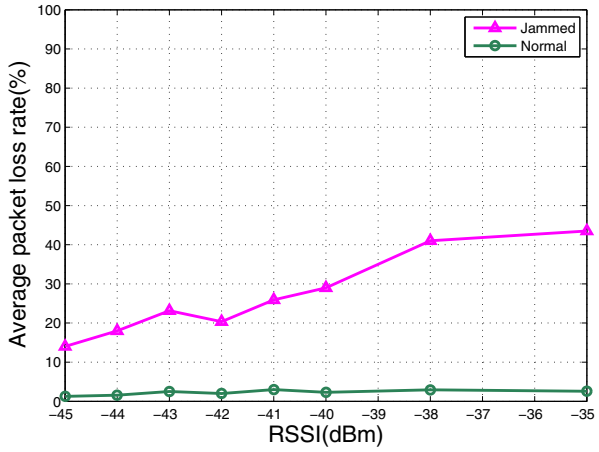

Fig. 6. Average packet loss rate vs. RSSI obtained by smartphones with or without jamming.

Finally, experimental results validate the accuracy of the proposed jamming detection application. For example, the false alarm rate (or miss detection rate) of the proposed application averaged over eight smartphone locations as shown in Fig. 3 is 0.37% (or 2%), if the jamming power is -18.85 dBm.

IV. Conclusions

In this paper, we have investigated the impact of jamming attacks on WiFi signals of smartphones via experiments and developed a jamming detection application on Android smartphones, based on the packet loss rate and RSSI information that can be easily measured by smartphones. Experimental results demonstrate that the proposed jamming detection application can conveniently detect jamming attacks in real time, with both the averaged false alarm rate and miss detection rate of jamming mostly well bellow 2%.

References

[1] L. Xiao, H. Dai, and P. Ning, "Jamming-resistant collaborative broadcast using uncoordinated frequency hopping," *IEEE Trans. Information Forensics and Security*, vol. 7, no. 1, pp. 297–309, 2011.

[2] L. Xiao, H. Dai, and P. Ning, "Mac design of uncoordinated fh-based collaborative broadcast," *IEEE Wireless Commun. Letters*, vol. 1, no. 3, pp. 261–264, 2012.

[3] C. Li, H. Dai, L. Xiao, and P. Ning, "Analysis and optimization on jamming-resistant collaborative broadcast in large-scale networks," in *Proc. Asilomar Conf. Signals, Systems and Computers*, pp. 1859–1863, 2010.

[4] Y. Li, L. Xiao, J. Liu, and Y. Tang, "Power control stackelberg game in cooperative anti-jamming communications," in *Proc. Int'l Conf. Game Theory for Networks*, pp. 93–98, 2014.

[5] J. Chiang and Y. Hu, "Cross-layer jamming detection and mitigation in wireless broadcast networks," *IEEE/ACM Trans. Networking (TON)*, vol. 19, no. 1, pp. 286–298, 2011.

[6] A. Hamieh and J. Ben-Othman, "Detection of jamming attacks in wireless ad hoc networks using error distribution," in *Proc. IEEE Int'l Conf. Commun. (ICC)*, pp. 1–6, 2009.

[7] Y. Lin and M. Li, "Distributed detection of jamming and defense in wireless sensor networks," in *Proc. IEEE Annual Conf. Information Sciences and Systems*, pp. 829–834, 2009.

[8] N. Sufyan, N. Saqib, and M. Zia, "Detection of jamming attacks in 802.11 b wireless networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2013, no. 1, pp. 1–18, 2013.

[9] A. Fragkiadakis, V. Siris, N. Petroulakis, and A. Traganitis, "Anomaly-based intrusion detection of jamming attacks, local versus collaborative detection," *Wireless Commun. and Mobile Computing*, vol. 15, no. 2, p. 276C294, 2013.

[10] Z. Lu, W. Wang, and C. Wang, "From jammer to gambler: Modeling and detection of jamming attacks against time-critical traffic," in *Proc. IEEE Int'l Conf. Computer Commun. (INFOCOM)*, pp. 1871–1879, 2011.

[11] M. Cakiroglu and A. Ozcerit, "Jamming detection mechanisms for wireless sensor networks," in *Proc. ICST Int'l conf. Scalable information systems*, 2008.

[12] A. Marttinen, A. Wyglinski, and R. Jantti, "Statistics-based jamming detection algorithm for jamming attacks against tactical manets," in *Proc. IEEE Military Commun. Conf. (MILCOM)*, pp. 501–506, 2014.

[13] O. Punal, I. Aktas, C. Schnelke, G. Abidin, K. Wehrle, and J. Gross, "Machine learning-based jamming detection for ieee 802.11: Design and experimental evaluation," in *Proc. IEEE Int'l Symp. A World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, pp. 1–10, 2014.

[14] M. Spuhler, D. Giustiniano, V. Lenders, M. Wilhelm, and J. Schmitt, "Detection of reactive jamming in dsss-based wireless communications," *IEEE Trans. Wireless Commun.*, vol. 13, no. 3, pp. 1593–1603, 2014.