Advanced Science and Technology Letters
Vol.60 (Mobile and Wireless 2014), pp.21-24
http://dx.doi.org/10.14257/astl.2014.60.06

# On Mobile Internet Tethering Detection

Sungcheon Lee and Hyun-chul Kim*

Sangmyung Univ, 300 Anseo-dong, Dong-nam-gu, Cheonan, South Korea 330-720
sc.l@me.com, hyunchulk@gmail.com
*Corresponding author

**Abstract.** With the advent of smartphones, the ever-increasing Internet traffic volume has recently been placing even more heavy loads on cellular network links as well. In particular, now it is being more required to detect traffic from tethered devices, since tethering continues to grow in popularity as it has proven a highly useful option for Internet networking in certain situations, e.g., when traveling, in places where local Wi-Fi hotspots are unavailable or inconvenient, etc. This paper address the problem of detecting tethered traffic of mobile devices, by investigating methods based on OS fingerprinting and traffic packet feature analysis.

**Keywords:** tethering, detection, fingerprinting

## 1 Introduction

With the advent of smartphones, the ever-increasing Internet traffic volume has recently been placing even more heavy loads on cellular network links as well. In particular, now it is being more required to detect traffic from tethered devices, since tethering continues to grow in popularity as it has proven a highly useful option for Internet networking in certain situations, e.g., when traveling, in places where local Wi-Fi hotspots are unavailable or inconvenient, etc. This paper address the problem of detecting tethered traffic of mobile devices, by proposing a method based on OS fingerprinting and traffic packet feature analysis. This paper is structured as follows. Section 2 reviews related work and patents recently proposed for the purpose of detecting tethered traffic and devices. In Section 3, we propose our method for detecting tethered traffic and evaluate it briefly. Section 4 concludes this paper.

## 2 Related Work

In this section, we briefly review recently proposed patents for the purpose of detecting tethered traffic and devices.

ISSN: 2287-1233 ASTL

### 2.1 Patent pending no. 10-2010-0105216 "System and method for controlling tethering in mobile communication network"

Proposed by the telecommunication company SK Telecom in Korea, this (more than) four-years-old patent primarily focuses on the characteristics of applications generating traffic of interests. It first identifies the causing application of target traffic using the deep-packet-inspection (DPI) techniques If the identified application is one of common well-known PC applications, such as P2P file sharing (e.g., BitTorrent), Web-hard, FTP, Microsoft Internet Explorer, PC games, etc., this traffic and the generating device is checked with a higher likelihood score of tethering. Once its likelihood score gets over a pre-specified threshold value, it is classified as of tethered one. Being a (more than) four-years-old proposal, this naïve method does not seem effective any more, as nowadays even mobile systems have become to support many P2P or FTP-like file sharing applications as well as PC games ported to mobile OS. Moreover, the proposed method can be neutralized, by simply changing the "user-agent" value of tethered desktop PC's web browsers to that of mobile web browsers.

### 2.2 Patent no. 10-1361-8230000 "Method for deciding tethering service in communication system and apparatus therefor"

Proposed by the telecommunication company Korea Telecom, this method checks TTL (Time To Live) values in IP packet headers sent by mobile devices. The TTL number is decremented by 1 for every network hop that it goes through a network. The theory behind this method is that, if a mobile device has a TTL of 64 and if there are any other packets coming from the device with a different TTL value, then the user is highly likely to be tethering. This method allows us to detect tethering even if both the tethering and tethered devices use the same Operating System. Yet, users can elude this method as well, by manipulating TTL values of the tethered devices so that their packets contain the same, indistinguishable TTL information.

## 3 Proposed Method and Evaluation

**Table 1**. Devices used for our experiments.

| Manufacturer | Device | OS |
|---|---|---|
| Samsung | Galaxy Nexus | Android 4.3 |
| Samsung | Galaxy S | Android 2.3 |
| Sony Ericson | Xperia Arc | Android 2.3 |
| LG | Optimus G | Android 4.1 |
| Apple | ipad mini | ios 7.0 |
| Apple | Macbook Air | OSX 10.9 |
| Microsoft | PC | Windows 8.1 Embedded |
| Nokia | Lumia 710 | Window Phone 7.8 |

We use the eight devices as depicted in Table 1 for this study of tethering detection. TTL values of mobile device-generated traffic are used to collect the ground truth (of tethering traffic) data, as introduced in the previous section 2.2. We use the Wireshark software [4] to take a look inside the collected packet data.

Fig. 1 shows that TCP window size written in uplink TCP SYN packets from mobile devices can be used to detect tethering. For this experiment, we tether a Windows 8.1 PC to a Samsung Galaxy Nexus(Android 4.3) phone then collect uplink traffic from those two devices. Checking TCP window size values of TCP SYN packets contained in the uplink traffic, we observe that there are two distinct values as shown in Fig. 1: 65,535 (from Windows 8.1 PC) and 14,600 (from Galaxy Nexus Phone). Table 2 summarizes the observed TCP window size values from the used eight devices of ours.

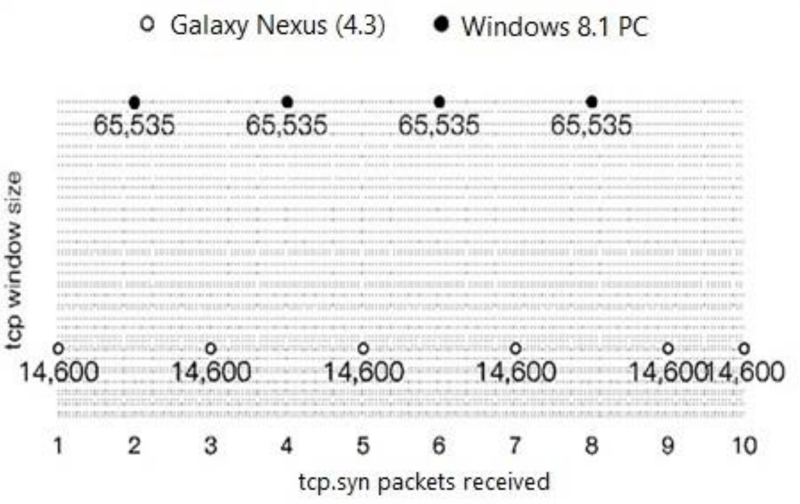

**Fig. 1.** Observed TCP window size values from uplink TCP SYN packets from Galaxy Nexus(Android 4.3) and Windows 8.1 PC.

**Table 2.** Observed TCP Window Size values in TCP SYN packets from different OS.

| OS | tcp.syn packet의 window_size |
|---|---|
| Apple ios 7.0 | 64k |
| Apple OSX 10.9 | 64k |
| Microsoft Windows 8.1 Embedde | 64k |
| Microsoft Window Phone 7.8 | 8k |
| Google Android 2.3 | 5k |
| Goolge Android 4.1 | 12k |
| Goolge Android 4.3 | 12k |

From Table 2, we anticipate that it would be feasible to detect tethering when it is between devices with different OS, e.g., between Android 2.3 and Android 4.1 (or 4.3), Apple OSX 10.9 and Android devices, etc.

## 4 Conclusions

In Section 3, we observe that uplink TCP SYN packets from devices, particularly TCP window size information, can be used to detect tethering. Yet, this information still can be manipulated or modified by the users to neutralize the detection method. To address the limitation, we are currently working towards a combined method where multiple features are used, to make it much harder to evade.

**Acknowledgement.** This research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF), funded by the Ministry of Education (No. 2013-R1A1A2010474).

## References

1. Evans, D.: The internet of things: How the next evolution of the internet is changing everything. CISCO white paper (2011)
2. Cho, B.: System and method for controlling tethering in mobile communication network. Patent, pending no. 10-2010-0105216 (2010)
3. Oh, H: Method for deciding tethering service in communication system and apparatus therefor. Patent no. 10-1361-8230000 (2014)
4. Wireshark, Go Deep. http://www.wireshark.org
5. Czajkowsi, K., Fitzgerald, S., Foster, I., Kesselman, C.: Grid Information Services for Distributed Resource Sharing. In: 10th IEEE International Symposium on High Performance Distributed Computing, pp. 181--184. IEEE Press, New York (2001).