PsychNology Journal, 2016
Volume 14, Number 2-3, 87 – 98

Biometric Authentication Methods on Smartphones: A Survey

Riccardo Spolaor*[1], QianQian Li[1], Merylin Monaro[1], Mauro Conti[2], Luciano Gamberini[3] and Giuseppe Sartori[3]

[1] University of Padua (Italy)

[2] Dept. of Mathematics University of Padua (Italy)

[3] Dept. of General Psychology University of Padua (Italy)

ABSTRACT

Nowadays, users are starting to develop a symbiotic bound with their smartphones. Users continuously carry these devices and use them for daily communication activities and social network interactions. On the other hand, a smartphone is equipped with sensors that can infer not only information about the context (e.g., location), but also about its owner. Since smartphones handle a huge amount of private information, recent techniques rely on those sensing capabilities to authenticate the user, measuring her biometric features. In this paper, we survey the most relevant biometric authentication methods on smartphones proposed in the literature. We categorize such methods by the nature of biometrics used, by their temporal features and by the sensing capabilities they rely on. Moreover, we draw some future directions in this promising research topic.

Keywords: *Physiological authentication, behavioral authentication, smartphones, human-computer interaction.*

Paper received 15/06/2016; received in revised form 31/10/2016; accepted 7/11/2016.

1. Introduction

In recent years, lots of researchers put their effort in understanding users' behavior using mobile devices. Smartphones have become daily used personal devices. People use them for both managing personal data and handling private communications. The

Cite as:

Spolaor R., Li Q., Monaro M., Conti M., Gamberini L., & Sartori G.. (2016). Biometric Authentication Methods on Smartphones: A Survey. *PsychNology Journal, 14*(2-3), 87 – 98. Retrieved [month] [day], [year], from www.psychnology.org.

*Corresponding Author:
Riccardo Spolaor
Brain, Mind and Computer Science
University of Padua
63 Via Trieste, Padua, Italy
E-mail: riccardo.spolaor@math.unipd.it

pervasiveness of such devices is generating a symbiotic bound between the user and her smartphone. According to the participants surveyed in a TIME's Mobility Poll (Gibbs, 2012), most of the participants stated that they could not live a single day without their smartphones. In detail, 91% of the participants say that their smartphones are very important and, for 60% of them, even more important than coffee.

Unfortunately, there are many privacy issues related to smartphone usage because of the huge amount of sensible data they can store. For example, an unauthorized user can steal a smartphone and gain the access to photos, contacts and even bank accounts. For this reason, authentication methods are fundamental to prevent the access to unauthorized users. Non transparent methods (e.g., password, PIN) are the most commonly used approaches. However, these methods require an aware interaction by the user and a predefined secret, which can be easily uncover by an attacker. Furthermore, even when in place, these methods often do not prevent a malicious user to get access to the phone, e.g., answering to an incoming call (Conti, Zachia-Zlatea & Crispo, 2011). For this reason, researchers focused their efforts on designing authentication methods more precise, more usable and less prone to attackers. Biometric authentication methods move to this direction. Instead of relying on a secret, biometric authentication methods rely on physiological and behavioral characteristics of the user.

Smartphones manufacturers (e.g., Samsung) have already expressed their interests in biometric authentication (Samsung GRO, 2014). Moreover, some company (e.g., BioCatch, 2008) commercializes software products based on cognitive traits (e.g., typical of eye-hand coordination, behavior patterns, usage preferences, device interaction patterns), physiological factors (e.g., left/right handedness, press size, hand tremor, arm size, muscle usage) and contextual factors (e.g., device location).

The main contribution of this paper is to survey biometric based authentication methods in the literature. In particular, we first elicit these methods into categories and then we summarize the most important features of each one of them. Finally, we discuss some possible future research directions in the field of biometrics authentication methods on smartphones.

2. Biometric Authentication Methods

Authentication methods protect smartphones from being accessed by unauthorized users. Common authentication methods that are already deployed on smartphones leverage a secret information which should be known only by the authorized user. These methods include passwords, Personal Identification Numbers (PIN) and unlock patterns. In recent years, researchers proposed a lot of authentication methods based on biometric features. We categorize the biometric authentication methods in the literature by the way they perform the user authentication. Firstly, we can classify such methods according to the nature of the biometric features that are measured by smartphone sensors (also schematized in Figure 1):

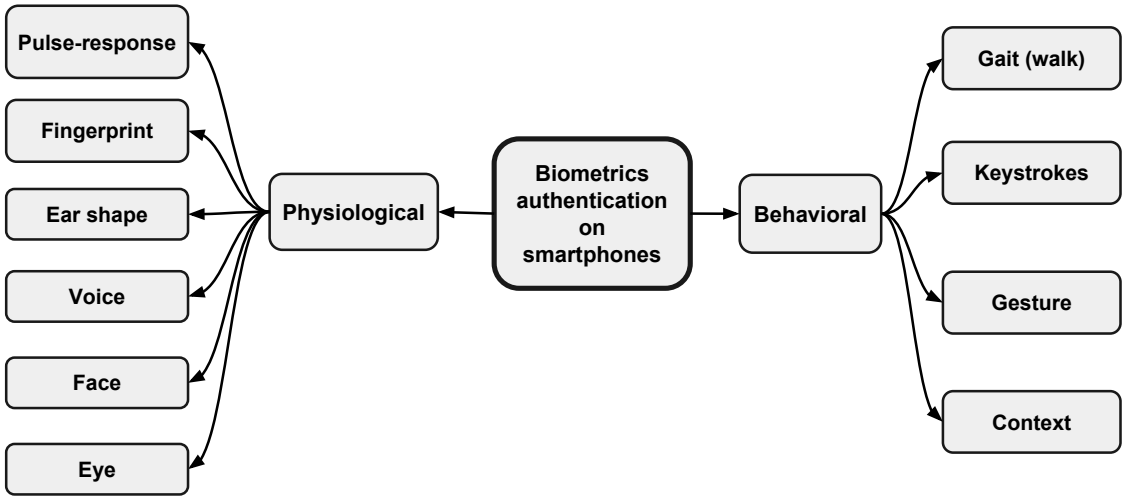

Figure 1. Physiological and behavioral biometrics authentication on smartphones

– Physiological biometrics authentication methods rely on users' body characteristics (e.g., fingerprint, face) to authenticate users.

– Behavioral biometrics authentication methods rely on the way the user behaves with her mobile device (e.g., keystrokes dynamics, gait).

Secondly, biometrics authentication methods can also be divided into two main categories according to time required to collect data from users and authenticate them:

– One-time authentication requires the user to perform a specific task for a limited period of time (e.g., input a PIN). In order to not affect the user experience, a one-time authentication method needs to be as fast as possible, but at the same time it must reach a high accuracy. For the same reason, such authentication is performed only on privacy sensitive phases (e.g., unlock the smartphone, access to bank account).

– Continuous authentication can involve the collection of data from sensors for a long period of time. Practically, a continuous authentication method performs two tasks at the same time: (i) incrementally builds a behavioral profile of the user adding new observations from sensors, (ii) verifies that the current observation matches with the behavioral profile of the user built from the past observations (e.g., gestures, gait).

At the best of our knowledge, all physiological biometric-based authentication methods in the literature belong to one-time authentication category.

Another distinction that could be done is the one between implicit (or transparent) and explicit (or non transparent) authentication methods. On one hand, explicit authentication methods require the user to perform a specific task, so the user is aware of when the authentication method is taking place. On the other hand, implicit ones do not require the user to perform any specific task to be authenticated.

2.1 Physiological Biometrics

Several authentication methods that rely on physiological biometrics are already deployed on smartphones. As a first example of physiological biometric, manufacturers recently started to embed on high-end smartphones a specific biometric sensor for digital fingerprints (Ricknäs, 2015). As another example, authentication systems use the frontal camera in order to recognize the face or the eyes of the owner. The study by Hadid, Heikkila, Silvén and Pietikainen (2007) proposes a face and eye detection and authentication for mobile phones. For the face detection, there are two approaches: color based (fast but prone to illumination and background changes) and Haar-like/AdaBoost based (slow but accurate).

Raja, Raghavendra, Stokkenes and Busch (2014) propose a standalone modular biometric system according to periocular information to authenticate users on smartphones. In the first stage, users have to capture a probe periocular image with rear or front camera and store it into a database for features extraction. The extracted features are compared to the reference templates in the database, in order to obtain a comparison score which decides upon the access to the device.

Fahmi et al. (2012) propose an authentication method that relies on the uniqueness of the shape of human ear. Using the frontal camera, the method is able to authenticate the user by the shape of her ear while she is taking a call.

Despite the prototype was not originally deployed on smartphones but it can be extended also on them, Rasmussen, Roeschlin, Martinovic and Tsudik (2014) propose a pulse-response biometric authentication method. Pulse-response biometric relies on

the property that each human body exhibits a unique response to a signal pulse applied at the palm of one hand, and measured at the palm of the other.

Other researchers rely on a set of physiological biometrics at the same time. Kim, Chung and Hong (2010) propose an enhanced authentication method using multi-modal personal information. The proposed approach collects information from face, teeth and voice from smartphone sensors, and authenticates users using these three traits simultaneously.

2.2 Behavioral Biometrics

In this section, we report the most relevant authentication methods that use behavioral biometrics. Some of them are not strictly designed for smartphones but they can be extended to work also on mobile devices. We first describe one-time authentication methods, then we proceed with continuous time ones.

One-time authentication methods: In the literature, some researchers rely on behavior of the user while she inputs information on touchscreen. Specifically, some authentication methods are based on the analysis of keystroke dynamics when typing on a mobile phone (Clarke & Furnell, 2007; Clarke, Karatzouni & Furnell, 2009; Karatzouni & Clarke, 2007; Nauman & Ali, 2010; Zahid, Shahzad, Khayam & Farooq, 2009). Giuffrida, Majdanik, Conti and Bos (2014) propose a sensor-enhanced keystroke dynamics authentication method. In other words, while users input the password, the system authenticates them using both motion sensors and taps on the touchscreen. The effectiveness of this authentication method is also proved to be secure even against the statistical attacks (Stanciu, Spolaor, Conti & Giuffrida, 2016). The authentication method proposed by Zheng, Bai, Huang and Wang (2014) is similar to the method proposed by Giuffrida et al. (2014), but it combines four features (i.e., acceleration, pressure, size, and time) extracted from smartphone sensors while the user is typing her PIN. Another method proposed by De Luca, Hang, Brudy, Lindner and Hussmann (2012) performs an implicit authentication where users are authenticated by the way they perform the unlock pattern on touchscreen. Zheng et al. (2014) proposed a method where users draw shapes (or perform gestures) on the front and the back of smartphones to enter tap-based passwords. The sequence and the way users draw the shape password is one kind of authentication which is robust against shoulder surfing pan (De Luca et al., 2014) and it is also easy and fast to use. This method also uses the habit they switch sides of the smartphones as authentication; this feature increases the security while authentication speed stays

relatively fast. Another example of authentication with touchscreen is proposed by Saevanee and Bhatarakosol (2008), where the authors use the finger pressure on a touchscreen to authenticate the user.

Other work in this direction uses motion sensors to authenticate implicitly the user when she is answering or placing a phone call (Conti, Zachia-Zlatea & Crispo, 2011), also called phone-to-ear gesture.

Continuous authentication methods: An example of behavioral biometric is the user's gait (i.e., the way she walks). Mantyjarvi, Lindholm, Vildjiounaite, Makela and Ailisto (2005) tested subjects' gait while they wear an accelerometer sensor placed on the belt. Similarly, the method proposed by Derawi, Nickel, Bours and Busch (2010) assumes that the smartphone is placed at the hip of each volunteer to collect gait data.

Regarding the user interaction with the touchscreen, Frank, Biedert, Ma, Martinovic and Song (2013) propose a continuous authentication method based on user interaction with smartphones touch-screen (i.e., up-down and left-right scrolling). Similar to the one-time method (Giuffrida et al., 2014), Gascon, Uellenbeck, Wolf and Rieck (2014) proposed a continuous authentication method that analyzes typing-motion behavior of users on smartphones. The authors asked participants to enter short sentences on touchscreen while all available sensor events were recorded to build a typing-motion behavior profile of the user.

Some other methods consider the context and location in which a mobile device is used. Shi, Niu, Jakobsson and Chow (2010) proposed an implicit continuous authentication method that uses multiple observations related to user behavior. The method considers a rich set of information, such as location, motion, communication, and usage of applications. The authors collected users' behavior data from their smartphones for two weeks in order to prove to the effectiveness of their proposal. Another example of context inferring technique is CRêPE (Conti, Crispo, Fernandes & Zhauniarovich, 2012), a framework for enforcing fine grained context-related policies, which can recognize the context in which a mobile device is used, continuously monitoring the environment via phone sensors. This framework supports both physical contexts (e.g., location, time), which are associated to physical sensors (e.g., GPS, clock, Bluetooth), and logical contexts, which are defined by functions over physical sensors.

3. Future Research Directions

Some possible future directions on continuous authentication methods can rely on cognitive games or other sources of information such as external devices and side-channels.

Cognitive games: A possible future direction in one-time behavioral authentication consists of measuring the behavior of the user while she solves cognitive games. Existing cognitive game easily extendable for this purpose are cognitive CAPTCHAs for touchscreen-enable devices, such as Capy (Capy, 2010) Puzzle and CAPTCHaStar (Conti, Guarisco & Spolaor, 2016).

External devices: Additional sources of information to improve the reliability of existing authentication methods could be external or wearable devices, such as smartwatches, fitness wristbands or Google Glass devices (Chauhan, Asghar, Kaafar & Mahanti, 2016). In fact, such devices are embedded with sensors, thus they could be a source of valuable information to infer behavioral patterns. In this paper, we do not consider biological biometrics such as blood and DNA. This because such biological measurements require specific hardware that are not commercially available at the time of writing, but it is reasonable to consider that such hardware could be embedded into smartphones in a near future.

Side-channel analysis: A side-channel is an observable source of information that is the result of the way the user interacts with a device. Network traffic is an example of side-channel and it could be relied to build a behavioral profile of a user. Indeed, some recent work shows that it is possible to infer from the encrypted network traffic the set of apps installed (Taylor, Spolaor, Conti & Martinovic, 2016) and even the actions the user performs within an app (Conti, Mancini, Spolaor & Verde, 2016). Moreover, since Conti, Nati, Rotundo and Spolaor (2016) proved that it is possible to recognize a user from the energy consumption of her laptop, we can reasonably consider this side-channel on smartphones as a valuable source of information for a user authentication method.

We strongly believe that it is possible to build an authentication method combining multiple behavioral biometrics and evaluating their impact on authentication dynamically, with an approach based on the context of usage. We also believe that, in the future, biometric authentication methods will significantly improve both the security and the usability of smartphones.

4. Conclusion

In this paper, we surveyed the state of the art of authentication methods on smartphones that are based on user biometrics. Firstly, we categorized authentication methods in the literature according to the nature of the biometric features, which are measured by smartphone sensors, into behavioral and physiological biometric categories. Physiological biometrics are related to body characteristics of the user, while behavioral biometrics are related to the way a user interact with her smartphone. Secondly, we divided the behavioral authentication methods into two categories according to time required to collect data from users and authenticate them (i.e., one time and continuous authentication). Finally, we discussed some possible future research directions in the field of biometrics authentication methods on smartphones.

5. Acknowledgements

Mauro Conti is supported by a Marie Curie Fellowship funded by the European Commission (agreement PCIG11-GA-2012-321980). This work is also partially supported by the EU TagItSmart! Project (agreement H2020-ICT30-2015-688061), the EU-India REACH Project (agreement ICI+/2014/342-896), and by the projects “Physical-Layer Security for Wireless Communication”, and “Content Centric Networking: Security and Privacy Issues” funded by the University of Padua.

6. References

Behavioral Authentication - BioCatch. (2008). Retrieved October 25, 2016, from http://www.biocatch.com/behavioral-authentication

Chauhan, J., Asghar, H. J., Mahanti, A., and Kaafar, M. A. (2016, June). Gesture-Based Continuous Authentication for Wearable Devices: The Smart Glasses Use Case. In S. Schneider, M. Manulis and A.-R. Sadeghi (Eds.) *International Conference on Applied Cryptography and Network Security* (pp. 648-665). New York: Springer International Publishing.

Clarke, N. L., and Furnell, S. M. (2007). Authenticating mobile phone users using keystroke analysis. *International Journal of Information Security*, 6(1), 1-14. New York: Springer International Publishing

Clarke, N., Karatzouni, S., and Furnell, S. (2009, May). Flexible and transparent user authentication for mobile devices. In D. Gritzalis, J. Lopez (Eds.) *IFIP International Information Security Conference* (pp. 1-12). Berlin: Springer Berlin Heidelberg.

Conti, M., Crispo, B., Fernandes, E., and Zhauniarovich, Y. (2012). CRêPE: A system for enforcing fine-grained context-related policies on android. *IEEE Transactions on Information Forensics and Security*, 7(5), 1426-1438.

Conti, M., Guarisco, C., and Spolaor, R. (2016, June). CAPTCHaStar! A novel CAPTCHA based on interactive shape discovery. In S. Schneider, M. Manulis and A.-R. Sadeghi (Eds.) *International Conference on Applied Cryptography and Network Security* (pp. 648-665). New York: Springer International Publishing.

Conti, M., Mancini, L. V., Spolaor, R., and Verde, N. V. (2016). Analyzing android encrypted network traffic to identify user actions. *IEEE Transactions on Information Forensics and Security*, 11(1), 114-125. New York: IEEE International Publishing

Conti, M., Nati, M., Rotundo, E., and Spolaor, R. (2016, May). Mind The Plug! Laptop-User Recognition Through Power Consumption. In R. Chow, G. Saldamli (Eds.) *Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security* (pp. 37-44). New York: ACM.

Conti, M., Zachia-Zlatea, I., and Crispo, B. (2011, March). Mind how you answer me!: transparently authenticating the user of a smartphone when answering or placing a call. In B. Cheung, L. C. K. Hui, R. Sandhu and D. S. Wong (Eds.) *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security* (pp. 249-259). New York: ACM.

De Luca, A., Hang, A., Brudy, F., Lindner, C., and Hussmann, H. (2012, May). Touch me once and I know it's you!: implicit authentication based on touch screen patterns. In J. A. Konstan, E. H. Chi and Kristina Höök (Eds.) Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 987-996). New York: ACM.

De Luca, A., Harbach, M., von Zezschwitz, E., Maurer, M. E., Slawik, B. E., Hussmann, H., and Smith, M. (2014, April). Now you see me, now you don't: protecting smartphone authentication from shoulder surfers. In M. Jones and P. Palanque (Eds.) *Proceedings of the 32nd annual ACM conference on Human factors in computing systems* (pp. 2937-2946). New York: ACM.

Derawi, M. O., Nickel, C., Bours, P., and Busch, C. (2010, October). Unobtrusive user-authentication on mobile phones using biometric gait recognition. In D. W. Fellner, X. Niu (Eds.) *Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP)* (pp. 306-311). New York: IEEE.

Fahmi, P. A., Kodirov, E., Choi, D. J., Lee, G. S., Azli, A. M. F., and Sayeed, S. (2012, October). Implicit authentication based on ear shape biometrics using smartphone camera during a call. In S.-W. Lee and D. S. Yeung (Eds.) *2012 IEEE International Conference on Systems, Man, and Cybernetics (SMC)* (pp. 2272-2276). New York: IEEE.

Frank, M., Biedert, R., Ma, E., Martinovic, I., and Song, D. (2013). Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. *IEEE transactions on information forensics and security*, 8(1), 136-148.

Gascon, H., Uellenbeck, S., Wolf, C., and Rieck, K. (2014). Continuous Authentication on Mobile Devices by Analysis of Typing Motion Behavior. *Sicherheit*, 1-12).

Gibbs, N. (2012, August). Your Life Is Fully Mobile. *Time*; The wireless issue. Retrieved October 25, 2016 from http://techland.time.com/2012/08/16/your-life-is-fully-mobile/

Giuffrida, C., Majdanik, K., Conti, M., and Bos, H. (2014, July). I sensed it was you: authenticating mobile users with sensor-enhanced keystroke dynamics. In L. Cavallaro (Eds.) *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment* (pp. 92-111). New York: Springer International Publishing.

Hadid, A., Heikkila, J. Y., Silvén, O., and Pietikainen, M. (2007, September). Face and eye detection for person authentication in mobile phones. In B. Rinner and W. Wolf (Eds.) *First ACM/IEEE International Conference on Distributed Smart Cameras* (pp. 101-108). New York: IEEE.

Karatzouni, S., and Clarke, N. (2007). Keystroke analysis for thumb-based keyboards on mobile devices. In D. Gritzalis and J. Lopez (Eds.) IFIP International Information Security Conference (pp. 253-263). New York: Springer US.

Kim, D. J., Chung, K. W., and Hong, K. S. (2010). Person authentication using face, teeth and voice modalities for mobile device security. *IEEE Transactions on Consumer Electronics*, 56(4), 2678-2685.

Mantyjarvi, J., Lindholm, M., Vildjiounaite, E., Makela, S. M., and Ailisto, H. A. (2005, March). Identifying users of portable devices from gait pattern with accelerometers. In Petropulu (Eds.) Proceedings (ICASSP'05). IEEE International Conference on

Acoustics, Speech, and Signal Processing, 2005. (Vol. 2, pp. ii-973). New York: IEEE.

Nauman, M., and Ali, T. (2010, June). Token: Trustable keystroke-based authentication for web-based applications on smartphones. In Bandyopadhyay S.K., Adi W., Kim T., Xiao Y. (eds) *Proceedings of the International Conference on Information Security and Assurance* (pp. 286-297). Berlin: Springer..

Puzzle Captcha - Capy. (2010). Retrieved October 25, 2016, from https://www.capy.me/products/puzzle_captcha/

Raja, K. B., Raghavendra, R., Stokkenes, M., & Busch, C. (2014, September). Smartphone authentication system using periocular biometrics. In Christoph Busch, Arslan Brömme (Eds.) *Biometrics Special Interest Group (BIOSIG), 2014 International Conference of the* (pp. 1-8). New York: IEEE.

Martinovic, I., Rasmussen, K. B., Roeschlin, M., & Tsudik, G. (2014). Authentication using pulse-response biometrics. In L. Bauer (Ed.) *Proceedings of the 21st Annual Network and Distributed System Security Symposium (NDSS), Washington DC: Internet Society*.

Ricknäs, M. (2015, June) Fingerprint sensors on their way to more smartphones. Retrieved October 25, 2016 from http://www.pcworld.com/article/2938792/fingerprint-sensors-on-their-way-to-more-smartphones.html

Saevanee, H., and Bhatarakosol, P. (2008, December). User authentication using combination of behavioral biometrics over the touchpad acting like touch screen of mobile device. In E. Bollin and P. Plapper (Eds.) *Computer and Electrical Engineering -ICCEE 2008* (pp. 82-86). New York: IEEE.

Samsung Advanced Institute of Technology. (2014). Retrieved October 25, 2016, from http://www.sait.samsung.co.kr/saithome/Main.do?method=main&pageKind=01

Shi, E., Niu, Y., Jakobsson, M., and Chow, R. (2010, October). Implicit authentication through learning user behavior. In S. K. Bandyopadhyay and W.Adi (Eds.) *International Conference on Information Security* (pp. 99-113). Berlin: Springer Berlin Heidelberg.

Stanciu, V. D., Spolaor, R., Conti, M., and Giuffrida, C. (2016, March). On the effectiveness of sensor-enhanced keystroke dynamics against statistical attacks. In C. Busch and A. Brömme (Eds.) *Proceedings of the Sixth ACM Conference on Data and Application Security and Privacy* (pp. 105-112). New York: ACM.

Taylor, V. F., Spolaor, R., Conti, M., and Martinovic, I. (2016, March). Appscanner: Automatic fingerprinting of smartphone apps from encrypted network traffic. In M. Backes (Ed.) *2016 IEEE European Symposium on Security and Privacy* (EuroS&P) (pp. 439-454). New York: IEEE.

Zahid, S., Shahzad, M., Khayam, S. A., and Farooq, M. (2009, September). Keystroke-based user identification on smart phones. In L. Mé (Eds.) *International Workshop on Recent Advances in Intrusion Detection* (pp. 224-243). Berlin: Springer Berlin Heidelberg.

Zheng, N., Bai, K., Huang, H., and Wang, H. (2014, October). You are how you touch: User verification on smartphones via tapping behaviors. In J. Kaur and G. Rouskas (Eds.) *2014 IEEE 22nd International Conference on Network Protocols* (pp. 221-232). New York: IEEE.