Assessing the Cooperativeness of Users in Wi-Fi Networks

Szymon Szott, Grzegorz Ptaszek and Lucjan Janowski
AGH University of Science and Technology, 30-059 Krakow, Poland

Keywords: Wi-Fi, Network, Selfish, Cheating, Misbehaviour.

Abstract: Wi-Fi networks are based on the cooperation of users in sharing a common resource – the radio channel. This is a security risk because users may behave selfishly to increase their own throughput but at the same time decrease the overall network performance. Many scientific analyses have focused on this problem, but none have taken into account real user behavior. We present the initial results of a work-in-progress in which we studied a group of users in terms of their online behavior as well as their psychological characteristics. We have found that users behave selfishly in a wireless setting, regardless of their cooperative nature. We provide lessons learned as well as pose open questions for further research in this field.

1 INTRODUCTION

Wi-Fi networks are a popular means of wireless communication: they can be found in homes, offices, and public places. These networks are based on the principle of users sharing a common resource – the radio channel. This need for cooperation leads to certain security issues, which are known in the literature as selfish attacks (the terms cheating and misbehavior are also common). These attacks are specific because they are insider attacks, i.e., they are performed by users which have already gained access to the network. Selfish attacks are becoming a problem because the standard which defines the communication protocol for Wi-Fi networks (IEEE 802.11) contains no incentives for users to cooperate (Szott, 2014). In fact, manufacturers exploit this trait to increase the performance of their devices (Bianchi et al., 2007).

A prominent example of such behavior is a traffic remapping attack (Konorski and Szott, 2014), in which a user takes advantage of the quality of service (QoS) traffic prioritization mechanism of 802.11 (Natkaniec et al., 2013) and assigns high priority identifiers to regular, best effort traffic (Figure 1). This means that regular traffic (e.g., a file transfer) is treated as if it required low delay (as, e.g., a Skype call), thus disturbing the operation of the network. This attack is relatively easy to perform as it requires adding only one rule in the user's firewall software.

Non-cooperative behavior has been well-studied in wireless communications literature, both in terms of the potential benefit to the misbehaving user (Szott et al., 2010) as well as countermeasure methods (Szott et al., 2013a; Szott et al., 2013b). However, despite the multitude of theoretical analyses, practical user behavior has not been studied in real world Wi-Fi deployments. This raises the question: Are users willing to cooperate in a wireless setting? Comparable studies conducted for peer-to-peer networks show that this is not the case (Anagnostakis et al., 2006). Therefore, we propose the following hypothesis: users of Wi-Fi networks will, given the chance, exhibit non-cooperative behavior regardless of their personal character. Towards this end we conducted a study in which we compared the online behavior of users (in a simulated environment) with the outcome of several psychological tests. The initial results are promising and we report several lessons learned. To the best of our knowledge, this work in progress is the first reported study of this kind for Wi-Fi networks.

2 METHODOLOGY

Our study was conducted separately for each participant. It consisted of two parts. First, we assessed their online behavior in a simulated test. Then, we determined their overall willingness to cooperate using psychological surveys.

2.1 Online Behavior Test

The participants were provided with a laptop and asked to test a new application for transferring data

Szott S., Ptaszek G. and Janowski L..
Assessing the Cooperativeness of Users in Wi-Fi Networks.
DOI: 10.5220/0005117300600064
In *Proceedings of the 11th International Conference on Wireless Information Networks and Systems* (WINSYS-2014), pages 60-64
ISBN: 978-989-758-047-5

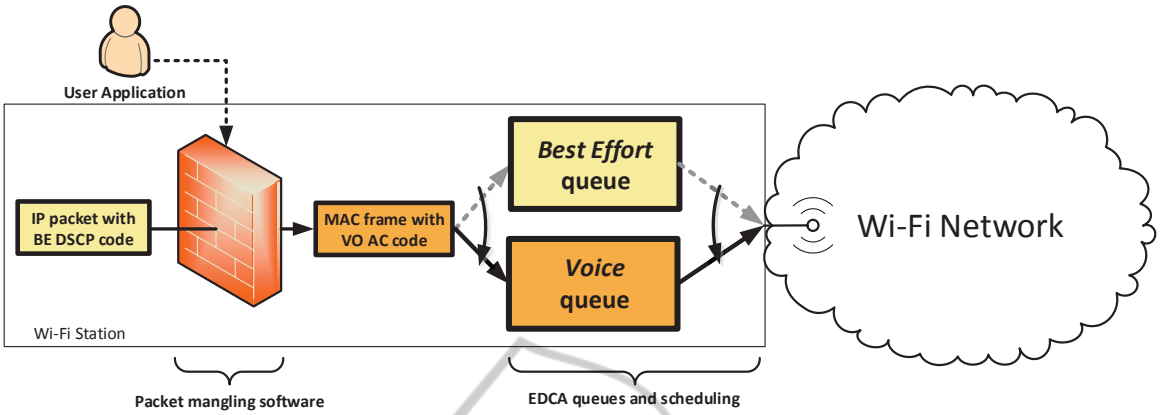
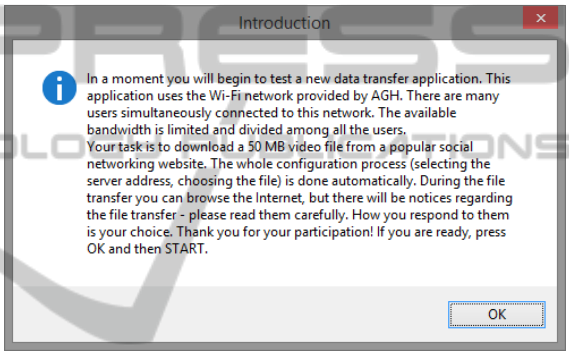
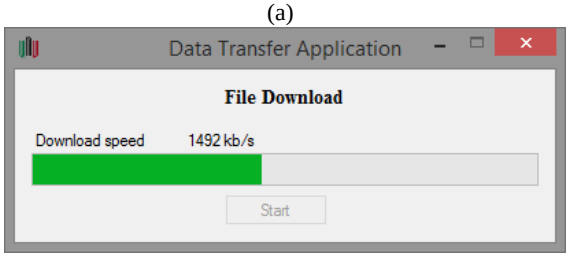


Figure 1: Example of a traffic remapping attack performed by a user of a Wi-Fi station taking advantage of traffic differentiation provided by the enhanced distributed channel access (EDCA) function of IEEE 802.11.

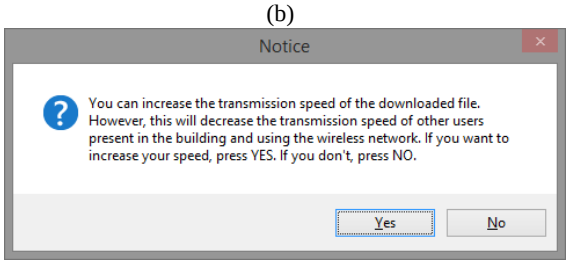
traffic (Figure 2). In reality, the application was only simulated. The participants were informed of the following: they will be using the university's Wi-Fi network, there are currently other users in the building using this network; and the network capacity is limited and shared among all its users. The user's task was to transfer a 50 MB file to a popular social networking site. The application automatically configured all necessary parameters. Since the file transfer took about 5 minutes, users were allowed to browse the Internet in the meantime. During the transfer, at fixed intervals, the testing application created a popup window informing the users that they can increase their transfer rate at the cost of the rate of the other users in the network. They then answered a yes/no question: Do you want to increase your throughput? This question appeared 10 times throughout the file transfer. Based on a user's decision, the application would modify the transfer rate accordingly. The test was repeated in two consecutive trials – for the uplink and downlink directions, respectively. The average throughput values were taken from simulation studies conducted previously for the uplink (Konorski and Szott, 2014) and downlink (Szott et al., 2009) directions. In both cases the selfish attack was a traffic remapping attack. This attack increased the traffic rate approximately two or threefold for the downlink and uplink directions, respectively.



(a)



(b)



(c)

Figure 2: Screenshots of the application used for the online behavior test: (a) introductory screen, (b) application window during normal operation, (c) notice about the possibility of misbehavior. Users were asked to read all instructions carefully.

2.2 Psychological surveys

We applied three different psychological surveys taken from the literature to assess the level of cooperation exhibited by the respondents: the agency and communion scales (Wojciszke and Szlendak, 2010), the belief in life as a zero-sum game scale (Rozycka and Wojciszke, 2000), and the ethic's questionnaire (Wojciszke and Baryla, 2000). All three tests, prepared in the language of the responders (Polish), have

shown to have satisfactory psychometric parameters.

The first scale measures agency (focus on self and own goals) and communion (focus on other people and interpersonal relations) as well as unrestrained agency (excessive focus on self with an ignorance of social relations) and unrestrained communion (excessive focus on others with an ignorance of own agency).

The second scale measures the general belief that life is a zero-sum game – a hidden assumption that one person's profit or success is only possible at the cost of an-other person's loss or failure. People, who believe that life is a zero-sum game delegitimize the social system and believe in injustice in the social world.

The final test measures the degree of faith of the respondent in two ethical codes: the ethics of autonomy and the ethics of collectivism. People with high scores related to the former are distinguished by respect for the welfare, freedom, and rights of an individual, helping others, and loyalty to individuals. People with high scores related to the latter are distinguished by respect for the welfare, interest, and rights of their own group, maintaining group integrity, group loyalty and conformity.

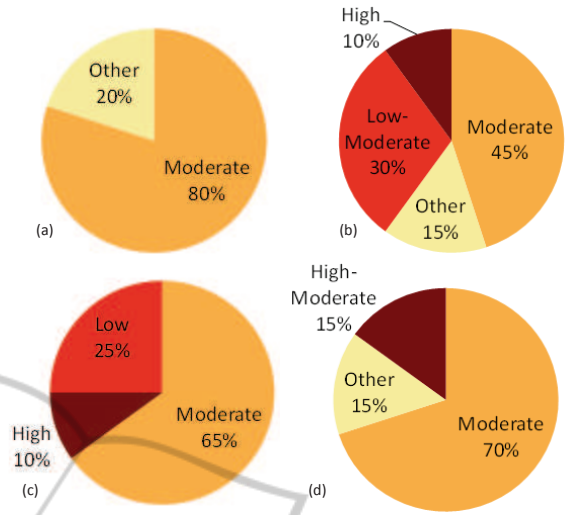


Figure 3: Results of psychological surveys. Participants level of (a) agency and communion, (b) unrestrained agency and unrestrained communion, (c) belief that life is a zero-sum game, (d) faith in ethics of autonomy and ethics of collectivism.

3 RESULTS AND ANALYSIS

The study was conducted on a group of 20 students (13 female) from AGH University. The participants were 21 to 25 years old and familiar with modern technology. This group of users, while small, nevertheless allowed us to draw initial conclusions and prepare subsequent research steps in this work in progress.

The main results of the psychological surveys are presented in Figure 3. The majority of participants exhibited moderate cooperativeness according to all of the scales used for measurement. In fact, 70% of the participants deviated no more than 30% from levels considered moderate. At the same time the majority of them refrained from cooperation in a wireless setting: approximately in 80% of cases users answered yes to the questions posed in the simulated online behavior test. Furthermore, we analyzed these two categories of results (psychological survey and simulated test) using Spearman's rank correlation coefficient and found no significant correlation. These factors confirm our initial hypothesis as stated in the introduction. Further detailed results are described next.

The initial choice of a user describes the first reaction to the dilemma of cooperation in each trial. The obtained results confirm the dominance of non-

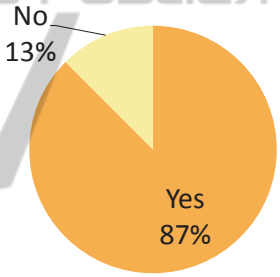


Figure 4: Initial choice of users in each trial.

cooperative behavior (Figure 4). This means that the majority of participants were willing to cheat from the very beginning of the test.

We also analyzed the behavior variation of users, i.e., how often within a given trial each user switched from one behavior to another (Figure 5). In almost half of the trials, users did not change their behavior and continued to cheat. Almost as often, users changed their behavior once or twice. This indicates that they were willing to experiment with the achieved throughput and determine what would happen had they cooperated. Unsatisfied with the lower throughput, users reverted to cheating. Finally, in the remaining 20% of trials users changed their behavior three or more times. This indicates a possible further investigation of choice of behavior on the achieved throughput.

Since each user performed two consecutive trials (uplink and downlink), we measured how often cheating occurred in both of them (Figure 6). No statistical correlation was found, which indicates that the order

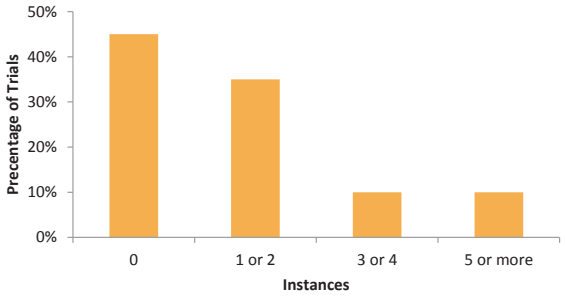


Figure 5: Occurrences of users changing behavior in a trial.

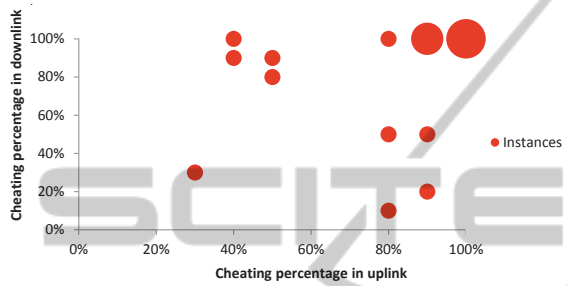


Figure 6: User behavior in uplink and downlink trials. Bubble size denotes number of instances.

of trials was not important. There were some cases, where users learned to cheat in the first trial and continued to do so in the second, whereas other users attempted further experimentation of how their choices made an impact on the throughput values.

4 LESSONS LEARNED

The lessons learned and open questions brought forth through this study include:

- People, even those with moderate or high levels of cooperativeness, tend to not cooperate in a Wi-Fi network. This supports our working hypothesis: users of Wi-Fi networks will, given the chance, exhibit non-cooperative behavior regardless of their personal character. Because the sample population is too low (20 people) to accept the hypothesis unconditionally, we are motivated to study whether the results apply in the general case.
- Similar studies should be performed separately for uncooperative and highly cooperative groups. This would provide further insight on user behavior. However, due to their intrinsic nature, uncooperative groups may be difficult to organize.
- It would be interesting to study a multi-user environment (representative of a hot-spot) to observe the interactions among participants and see how the multi-player prisoner's dilemma plays out.
- Different incentive mechanisms may be studied, e.g., varying the reward for completing the assigned task based on time efficiency. Monetary benefits could be worth considering.
- The framing of the question which the participants are asked in the online behavior test impacts the results. We opted for a neutral approach (Do you want to increase your throughput?) because the use of words such as cheating or misbehaving might influence the participants' perception of the problem, which is also an area of further study.
- Having established that non-cooperative behavior in wireless networks is a problem, the design of countermeasure methods becomes important. What kind of punishment mechanisms could be used and would they be effective in incentivizing cooperation? Can this be done within the framework of 802.11?
- This and subsequent studies may also be useful for service providers, in order to establish their network strategies (which service parameters can be decreased without affecting user experience, how much effort are network users willing to expend to increase their transfer rate) as well as for network managers who want to provide QoS-based resource sharing (Kosek-Szott et al., 2013).

5 SUMMARY

The study of the cooperativeness of Wi-Fi network users, presented in this paper, has provided initial results which satisfy our hypothesis: users of Wi-Fi networks will, given the chance, exhibit non-cooperative behavior regardless of their personal character. This *chance* is not a purely theoretical concept because of the emergence of flexible Wi-Fi platforms such as the Wireless MAC Processor (Szott et al., 2013a). It can be concluded that, on one hand, the scientific research performed in the field of wireless network security and performance analysis is justified, and on the other, that further effort in this work-in-progress is encouraged in order to better understand human online behavior. Our future research agenda will be based on the conclusions presented in Section 4.

ACKNOWLEDGEMENTS

This work was supported by the AGH University of Science and Technology under contracts no.

15.11.230.051 and 11.11.230.018. The authors would like to thank Lukasz Wronski for his support during the tests.

REFERENCES

Anagnostakis, K. G., Charmatzis, F., Ioannidis, S., and Zghaibeh, M. (2006). On the impact of p2p incentive mechanisms on user behavior. In *IN NETECON+IBC*.

Bianchi, G., Di Stefano, A., Giaconia, C., Scalia, L., Terrazzino, G., and Tinnirello, I. (2007). Experimental assessment of the backoff behavior of commercial IEEE 802.11b network cards. In *Proc. of INFOCOM*.

Konorski, J. and Szott, S. (2014). Discouraging traffic remapping attacks in local ad hoc networks. *Wireless Communications, IEEE Transactions on*, DOI 10.1109/TWC.2014.2321577.

Kosek-Szott, K., Natkaniec, M., Szott, S., Krasilov, A., Lyakhov, A., Safonov, A., and Tinnirello, I. (2013). What's new for QoS in IEEE 802.11? *IEEE Network*, 27(6):95–104.

Natkaniec, M., Kosek-Szott, K., Szott, S., and Bianchi, G. (2013). A Survey of Medium Access Mechanisms for Providing QoS in Ad-Hoc Networks. *Communications Surveys Tutorials, IEEE*, 15(2):592–620.

Rozycka, J. and Wojciszke, B. (2000). Skala wiary w gre o sumie zerowej [scale of belief in life as a zero-sum game]. *Studia Psychologiczne*, 48:35–46.

Szott, S. (2014). Selfish Insider Attacks in IEEE 802.11s Wireless Mesh Networks. *IEEE Communications Magazine*, 52(6):227–233.

Szott, S., Gozdecki, J., Kosek-Szott, K., Loziak, K., Natkaniec, M., and Tinnirello, I. (2013a). The risks of WiFi flexibility: Enabling and detecting cheating. In *Proc. of Future Network and Mobile Summit*.

Szott, S., Natkaniec, M., and Banchs, A. (2009). Impact of Misbehaviour on QoS in Wireless Mesh Networks. In *Proc. of IFIP Networking*.

Szott, S., Natkaniec, M., and Pach, A. R. (2010). An IEEE 802.11 EDCA model with support for analysing networks with misbehaving nodes. *EURASIP Journal on Wireless Communications and Networking*, 2010:71.

Szott, S., Natkaniec, M., and Pach, A. R. (2013b). Improving QoS and security in wireless ad hoc networks by mitigating the impact of selfish behaviors: a game-theoretic approach. *Security and Communication Networks*, 6:509–522.

Wojciszke, B. and Baryla, W. (2000). Potoczne rozumienie moralnosci: piec kodow etycznych i narzedzie ich pomiaru [Lay understanding of morality: Five ethical codes and their measurement]. *Przeglad Psychologiczny*, 43:395–421.

Wojciszke, B. and Szlendak, M. (2010). Skale do pomiaru orientacji sprawczej i wspolnotowej [Scales Measuring Agency and Communion]. *Psychologia Spoleczna*, 5:57–70.