Technical Disclosure Commons

Defensive Publications Series

October 2019

Intelligent Signal Collection for Detection of Automated Interactive Session

Anonymous

Follow this and additional works at: https://www.tdcommons.org/dpubs_series

Recommended Citation
Anonymous, "Intelligent Signal Collection for Detection of Automated Interactive Session", Technical Disclosure Commons, (October 18, 2019)
https://www.tdcommons.org/dpubs_series/2585

This work is licensed under a Creative Commons Attribution 4.0 License.
This Article is brought to you for free and open access by Technical Disclosure Commons. It has been accepted for inclusion in Defensive Publications Series by an authorized administrator of Technical Disclosure Commons.

Intelligent Signal Collection for Detection of Automated Interactive Session

ABSTRACT

When user interactions with an online platform are spoofed, e.g., by the use of automated interactive agents or bots that mimic user behavior, such platform is negatively affected, e.g., may lose ad revenue. This disclosure describes techniques to selectively collect signals from interactive sessions and use the collected signals to determine whether an interactive session is a genuine user session of a human user, or an automated interactive session. The collected signals can include static and/or dynamic signals and are matched to a session identifier. The signals are inspected to assign quality scores and the session is determined as a genuine session based on the quality scores of signals associated with it and the values of those signals. The signal collection techniques described herein can also be utilized for other purposes.

KEYWORDS

- Signal collection
- Signal validation
- Bot detection
- Fraudulent session
- Ad fraud
- Click fraud
- Automated agent

BACKGROUND

Online providers such as video hosting services, game providers, social networking services, etc. benefit from genuine user interaction with their platforms. For example, such providers can display advertising on their platforms and generate revenue when users view

advertisements, click on advertisements, etc. In another example, game providers can sell in-game items to generate revenue.

When user interactions are spoofed, e.g., by the use of automated interactive agents or bots that mimic user behavior, such platforms are negatively affected. For example, fraudulent clicks on ads can result in the platform not being able to charge revenue for such ads. In another example, automated gameplay can result in genuine users being kept from leaderboards or other recognition that promotes user engagement with a game. Therefore, online providers benefit from being able to recognize automated interactive sessions.

DESCRIPTION

This disclosure describes techniques to selectively collect signals from interactive sessions and use the collected signals to determine whether an interactive session is a genuine user session of a human user, or an automated interactive session.

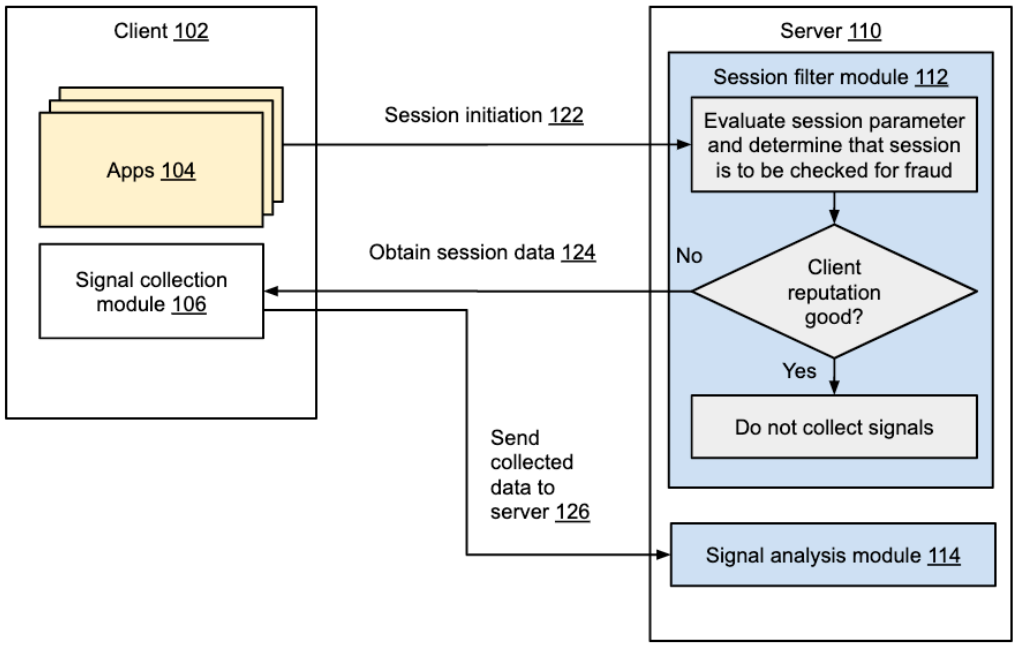

Fig. 1: Intelligent signal collection for detection of automated interactive session

Fig. 1 illustrates an example of intelligent signal collection to detect automated interactive sessions. A client (102), e.g., smartphone, tablet, PC, or other computing device, has software applications (104) such as games, social networking applications, messaging applications, etc. The client connects to a server (110) to engage in an interactive session with the server, e.g., to send and receive data for the application.

Signal collection module

Per techniques described herein, a signal collection module (106) is provided on the client and is utilized to collect signals associated with particular interactive sessions that the client participates in. In operation, when an app session is launched, the signal collection module on the client is activated to obtain the configuration on signals to be collected.

The signal collection module can be provided as a code library that can be accessed and utilized by any of the apps. Collection of signals can include obtaining information about various static or dynamic signals at the client. For example, static signals can include, e.g., device operating system, app version, etc. Dynamic signals can include, e.g., device battery level, touch signals, etc. Touch signals are client signals that are related to user touch action on a touch screen device, e.g., touch coordinates, touch pressure, etc. Signals can include, e.g., network fingerprints; device-specific parameters (e.g., battery level, mobile carrier, etc.); app names / versions; user-activity (keyboard, mouse, touch, sensor values such as gyroscope, etc.); session tokens; and so on.

A signal can include information regarding the time at which the signal value was obtained, the source of the information, the value itself (or an error that indicates the value could not be collected). The signal can be collected as a time series of values or errors. Signals

collected on the client are active signals. The values of these signals are untrusted signals, since these can be tampered with, when the client is a fraudulent agent.

The signal collection module includes code that implements collection of dynamic signals at regular intervals and the signal collection logic for different kinds of signals. Optionally, the signal collection module can be provided as code that is downloaded and executed on the device during an interactive session, but that does not persist on the client.

Signals are collected and stored in a buffer on the client (e.g., a circular buffer bounded by time and/or size), such that storing signals does not take up substantial memory. A sliding time window can be used for signal retention, e.g., 1 minute, 5 minutes, etc. Dynamic signals are collected initially and at regular intervals during the interactive session. Static signals are collected at the time of the event of interest, e.g., display of an ad, ad activation via clicking, etc. Raw signal values can be stored. Further, certain signal values are transformed to ensure that the signal does not include a user's private information, e.g., device name such as "Josh's iPhone" may be transformed to a transformed characteristic that does not include the name, e.g., using a one-way hash function.

Obfuscation is used to prevent detection of the signal collection module. For example, parameters such as local storage name for storing the signals, cookie name, etc. can be given obfuscated names to prevent detection. Further, the signal collection code can be placed together with other functional code such that user experience or functionality is broken if the signal collection code is not loaded/executed.

Session filter module

The server includes a session filter module (112) that determines whether a particular session is to be subjected to data collection. When a client initiates a session (122), the server determines whether the session is to be checked for fraud. For example, if the session includes an advertisement that is to be displayed on the client, the session is identified as a session to be checked.

The session filter module accesses a client reputation database, e.g., that identifies whether a client is likely to be fraudulent or genuine. If the client reputation is good, e.g., meets predetermined criteria, the server determines that no signals are to be collected. Different tiers of reputation can be utilized with corresponding determination of whether to collect signals and if so, which signals to collect and how often. If the client reputation does not meet the criteria, a request is sent to the client (124) to obtain data associated with the session.

In response, the data in the buffer, collected by the signal collection module, is sent to the server. Signal values at the critical event (advertisement) as collected by the signal collection module are included in the data. For example, the collected signals can include data for a certain time period, e.g., five minutes before an ad-click event, and static data from the time of the event. The data is obfuscated and/or encrypted at the client prior to sending to the server.

Signal analysis module

The server also includes a signal analysis module (114) that analyzes the collected signals received from the client (126) to determine whether a session is an automated interactive session, e.g., a session operated by a bot or automated agent without a human user, or a genuine user session. Further to the signals from the signal collection module on the client, the signal analysis

module can also utilize passive signals (server-side signals) that are collected from client requests that occur during the session being analyzed, e.g., corresponding to an ad click event, an ad impression event, etc. Such passive signals can include, e.g., source IP address, user agent string, etc.

For each signal included in the analysis, a signal name and description is stored in the signal analysis module, along with the kind of signal (static/dynamic) and possible valid values for the signal for the particular type of client configuration, e.g., determined based on the operating system of the client and/or other parameters. Each collected signal is inspected and a quality score for the signal is determined. For example, a battery level value outside of the range 0-100% is associated with a low (or zero) quality score, since it does not correspond to a valid battery level for a device. In another example, if the signal context is that of the use of a camera on a smartphone, a signal that is indicative of a keyboard being active (e.g., includes “key down” events) is associated with a low or zero quality score.

Validation of the session is performed based on the signals that are available for the session and their respective quality scores. Validation can be performed as either hard validation or soft validation.

- Hard validation: Signals that are associated with high quality scores are stored in association with a session identifier. Signals that have a low quality score (unexpected signal values) are discarded and not used for validation. This allows the signal analysis module to only consider reliable signals when determining whether a session is genuine.
- Soft validation: Both high and low quality signals are utilized to determine whether a session is genuine. Soft validation can be performed, e.g., when hard validation fails.

Analysis can be performed to determine whether the signals with low quality scores are erroneously obtained (e.g., due to errors in the signal collection module) or is an actual suspicious value that is to be used to validate the session.

The validation logic and quality score function can be updated over time. The collected data for a session can be re-analyzed after such updates. By storing signals in association with session identifiers, the validation techniques can be improved over time. For example, validation logic can be updated to include additional collected signals that were not considered previously.

Session validation can be performed using rule-based techniques, e.g., a decision-tree model, and/or machine learning (ML) based techniques. Multiple techniques can be used in combination, and different types of validation techniques can be used for different types of sessions. The validation can provide a likelihood of whether the session is a human user or an automated interactive session.

CONCLUSION

This disclosure describes techniques to selectively collect signals from interactive sessions and use the collected signals to determine whether an interactive session is a genuine user session of a human user, or an automated interactive session. The collected signals can include static and/or dynamic signals and are matched to a session identifier. The signals are inspected to assign quality scores and the session is determined as a genuine session based on the quality scores and the values of signals associated with it.