This is the final draft of the following article:
Denis Kotkov, Gaurav Pandey, and Alexander Semenov. Gaming Bot Detection: A Systematic Literature Review. International Conference on Computational Social Networks. Springer, Cham, 2018. doi: 10.1007/978-3-030-04648-4_21

Gaming Bot Detection: A Systematic Literature Review

Denis Kotkov, Gaurav Pandey, and Alexander Semenov

University of Jyvaskyla, Finland
kotkov.denis.ig@gmail.com, gaurav.g.pandey@jyu.fi,
alexander.v.semenov@jyu.fi

Abstract. In online games, some players employ programs (bots) that allow them to bypass game routines and effortlessly gain virtual resources. This practice leads to negative effects, such as reduced revenue for the game development companies and unfair treatment for ordinary players. Bot detection methods act as a counter measure for such players. This paper presents a systematic literature review of bot detection in online games. We mainly focus on games that allow resource accumulation for players between game sessions. For this, we summarize the existing literature, list categories of games ignored by the scientific community, review publicly available datasets, present the taxonomy of detection methods and provide future directions on this topic. The main goal of this paper is to summarize the existing literature and indicate gaps in the body of knowledge.

Keywords: Online Games · Bot Detection · Machine Learning.

1 Introduction

Online games have millions of players and bring billions of dollars of revenue to game development companies [3]. In this paper, the term *player* refers to the individual, who plays the game [22]. Games can fall into one of the two categories: games that allow players to accumulate game resources between game sessions, such as MMORPGs (massively multiplayer online role-playing games) and games, where players gather game resources in every session from scratch, such as FPS (first-person shooter) games [25]. In this paper, we focus on online games that allow players to save gained resources between game sessions.

Players of these games spend days and sometimes even years building up their characters to compete or collaborate with other players and acquire access to new game content [4]. In this paper, the term *character* refers to an avatar controlled by the player in the virtual world of the game [22]. Game development companies benefit from players by selling to them game items or special abilities that players would spend a lot of effort to acquire.

Players can buy these products not only from game development companies, but also from other players [2]. Markets, where players buy and sell characters and game products are very popular among players, as they offer prices lower

than that of game development companies and allow players to purchase products that game development companies do not sell. For example, more than half of total money exchange in the famous MMORPG game Aion is associated with real money transactions [12]. Many of these markets can be identified in search engines; for instance, market "G2G" [1] offers hundreds of thousands items for sale for World of Warcraft. China, up to 100,000 players are hired to build up their characters for selling [22]. Some player can even make a living just by building up their characters and selling them later [1].

Many players use bots for repetitive actions needed to gain resources or build up their characters. Bots appear in games for different purposes:

- A bot can be integrated in a game to play with human players. Usually, it is clear which character is a bot and these bots are not needed to be detected.
- A player can use a bot to access game content, which was unavailable earlier. For example, a player can implement a bot in the Sikuli[2] platform to access content in the puzzle game Bejeweled[3].
- A player can use a bot to gain social influence in a game. For example, a Counter Strike player can use a bot to win or gain an advantage over other players. Examples of such software are enablers of automatic cross-hair. In this case, the player does not receive any profit, but social influence.
- A player can use a bot to gain real life resources, such as real money or goods. For example, an Aion player can use a bot to bypass game routines and earn game resources. This player can sell the gained resources for real money later.

In this paper, we mainly focus on the detection of bots that appear in games to generate profit for their owners, as these kinds of bots harm both game development companies and players. Game development companies receive less revenue, as instead of buying products from the companies, players earn these products using bots. Ordinary players also suffer because of bots. This is because bots can play without break, build up their characters faster and cause inflation of the game currency by mining it with a much higher speed than ordinary players [22].

Bots are not the only way to cheat in games. Users can also use additional programs that simplify their gaming tasks. For example, a Counter Strike player can use a program that makes walls transparent, which allows this player to track characters of other players and gain an advantage in the game [20]. However, in this paper, we only focus on bots, which are computer programs that control a player's character and play the game unattended [22].

There are multiple bots available for different games; many of them claim that they are feature-rich very easy to use[4], and there are tens of thousands users

[1] https://www.g2g.com/wow-us/Item-2299-19260
[2] http://www.sikuli.org/
[3] https://www.ea.com/games/bejeweled/bejeweled-blitz?setLocale=en-us
[4] https://www.raccoonbot.com/

discussing bot usage at the forums[5]. Typically bots aimed at mobile games require Android OS emulator to be installed, and the bot software works inside the emulator. Some bots are free software, however, some require license fee[6]. Many bot manufacturers claim, that their software has "*advanced artificial intelligence that closely mimics a humans behavior*"[7]; thus, detection of the bots might be not a trivial task.

On the other hand, a lot of research is focused on creation of efficient AI for playing different games, such as poker [9]; and many other games [23]. Also, behavior of online game players was studied as a model for real-life people interaction [6].

The main goal of this paper is to summarize the existing literature on gaming bot detection and indicate gaps in the body of knowledge. The main contributions of this paper are summarized as follows.

- It reviews existing body of knowledge.
- It presents a taxonomy of bot detection methods.
- It provides future directions of the topic based on the literature review.

1.1 Methods and Logistics

This paper provides a literature review on bot detection in online games. We conducted a systematic literature review [21], which included screening (or gathering) related literature, processing (or analyzing) collected literature and communicating the results of the review. The key points followed in our review process are:

- **Literature Search.** We first looked for literature based on the following search queries: "game bot detection", "game bot security" and "game bot cheating detection". We analyzed the top twenty articles from results returned by Google Scholar[8] in response to each search query. We retrieved the search results twice: articles published overall and articles published starting from 2017 (to receive the most recent articles). Overall, we found 35 distinct articles.
- **Screening of Literature.** Our selection criteria for the literature was based on the JUFO ratings[9] of the articles. These ratings created by the Finnish scientific community, classify the publication channels into four levels: 0, 1, 2 and 3. The higher the level the higher the quality of the publication channel. We took into account only articles published in the publication channels of at least level 1. After filtering out articles that do not meet our requirements, we selected 12 key articles (See Table 1).

[5] https://mybot.run/forums/
[6] https://wrobot.eu/store/category/2-wrobot/
[7] https://wrobot.eu/
[8] https://scholar.google.com/
[9] https://www.tsv.fi/julkaisufoorumi/haku.php?lang=en

1.2 Research Questions

In this paper, our literature review focuses on answering the following research questions:

RQ1: *What game categories have received low attention from the scientific community for bot detection?*
Our goal is to detect categories of games that are targeted by bots, but skipped by the scientific community, as these categories bring new challenges and need to be considered.

RQ2: *What are the publicly available datasets for bot detection?*
We aim to collect a list a datasets available for experiments.

RQ3: *How can we detect bots in online games?*
The purpose of this RQ is to review the state-of-the-art bot detection methods.

RQ4: *What are the future directions of bot detection?*
We aim to provide future directions of this topic.

The rest of the paper is organized as follows. We first discuss game categories in Section 2. We then list the publicly available datasets in Section 3 and review bot detection methods in Section 4. We also present future directions of the topic in Section 5. Finally we provide conclusion and future work in Section 6.

2 Studied Game Categories

In this section, we describe existing game categories and categories studied by the scientific community. Finally, we will answer RQ1 by indicating game categories disregarded by the selected studies.

Although games vary significantly, they can generally be classified in several categories. However, these categories are relative and a game can belong to several categories at the same time. We extended the categorization presented in [10] as follows:

- **Role playing games.** A player controls their character and explores the virtual world of the game. These games usually involve earning resources, such as items or game currency and the enhancing character's abilities. A subcategory of these games is massively multiplayer online role-playing games (MMORPGs), e.g. World of Warcraft[10].
- **Action games.** A player navigates their character in the game world by avoiding or destroying obstacles on its way. The emphasis of these games is on the player's hand-eye coordination. A typical example of an action game is Super Mario Bros[11].

[10] https://worldofwarcraft.com/en-us/
[11] https://www.joy.land/super-mario-bros.html

- **Adventure games.** A player navigates their character in the game and solves puzzle like problems on their way. The abilities of the character usually stay fixed. The focus of this category of games is on the story line. An example from this category is Syberia[12].
- **Strategy games.** It is common that in games of this category, a player controls a population of characters and makes decision for them. The focus of this category is on tactic and strategy. A famous example from this category is StarCraft [13].
- **Music games.** A player needs to imitate playing a musical instrument or dance to earn game points. The focus of this category is on the consistency of music and player's movements. An example from this category is Guitar Hero[14].
- **Shooting games.** Normally, a player controls a character armed with a weapon, which is often a gun to destroy other characters. A famous example from this category is the first person shooting (FPS) game Quake[15].
- **Fighting games.** A player controls a character in a combat against one or more other characters. A famous fighting game is Mortal Kombat[16].
- **Puzzle games.** In this category, a player does not normally control any characters. The focus of this category is on puzzle solving. A famous example from this category is Tetris[17].
- **Gambling games.** These games always include consideration, chance and prize. A player bets something of value, such as money on a random event and wins the prize according to the consideration depending on the result of the event. One of the most common example of the game from this category is Roulette[18].

According to our literature review (Table 1), most research on bot detection focuses on MMORPG and FPS. Studies target MMORPG, because in the games of this category, bots are used by certain players for gaining profit. This discourages other ordinary players to play the game and financially hurts the game development companies. Studies also target FPS games, as the case study that can be generalized to other kinds of games [11]. The rest of categories received low attention from the scientific community, while games belonging to these categories also suffer from bots in the same way as MMORPG. For example, the famous strategy mobile game Clash Royale[19] has more than 27 million players[20]

[12] http://www.syberia.microids.com/EN/
[13] https://starcraft.com/en-us/
[14] https://www.guitarhero.com/
[15] https://quake.bethesda.net/en
[16] http://www.mortalkombat.com/
[17] https://tetris.com/
[18] https://www.casinotop10.net/free-roulette
[19] https://supercell.com/en/games/clashroyale/
[20] https://toucharcade.com/2017/08/29/clash-royale-saw-27-million-players-enter-its-crown-championship-fall-season/

and some of these players use bots[21] to improve their characters and sell them later.

3 Datasets for Bot Detection

In this section, we answer RQ2 by listing publicly available datasets based on our literature review. We also discuss the methods to collect datasets, that can be utilized for bot detection tasks.

Researchers collect various datasets for bot detection tasks, but most of them remain publicly unavailable (as we can see that most of the datasets in Table 1 are private). Based on our literature review, we have identified the following datasets:

- **Quake 2 Datasets.** Quake 2 allows to record a log of the game, which can later be used to watch and analyze the recorded game [11]. The logs contain character movements and game events, such as picking game items, shootings and destroying a character. Players share their game recordings on the number of websites, such as Planet Quake[22] or Demo Squad[23].
- **Aion Dataset**[24]. The dataset contains action logs performed by 49,739 characters in the famous MMORPG Aion from April 9 till July 5, 2010 [16]. The dataset also contains the list of banned users verified by human labor, which is useful for testing bot detection algorithms.

In situations, when datasets suitable for researchers' needs are publicly unavailable, researchers employ the following data collection methods:

- **Tracking events.** The researchers could track events (such as clicks and keyboard buttons) in the client application of the game. Gianvecchio at el. [14] developed a program that runs concurrently with the game client application and tracks keyboard and mouse events.
- **Developing a game.** The researchers could develop their own games that suit their needs and track events in them. Alayed at el. [7] developed an FPS game and tracked players' actions in this game.
- **Dataset generation.** In order to generate botnet datasetm Shiravi et. al [26] analyzed real packet traces to create profiles for agents generating real traffic. Then they generated malicious traffic by exploring multi-stage attack scenarios. Similar approach can be followed specifically for bot detection.

There are many bot software packages available, and for collection of the dataset it could be possible to run the bot at controlled environment; but in this case it is not possible to collect data from the game without specific reverse-engineering (or packet sniffing), since main game software is closed and located at the servers controlled by game-developer.

[21] http://clashroyalebot.com.br/
[22] http://planetquake.gamespy.com/
[23] http://q2scene.net/ds/
[24] http://ocslab.hksecurity.net/Datasets/game-bot-detection

Table 1. A Summary of Articles

Article	**Category**	**Game**	**Dataset**
Chen et al. [11]	Trajectory	FPS (Quake 2)	Game traces publicly available at five websites dedicated to Quake
Kang et al. [16]	Action frequency & social activity	MMORPG (Aion)	A public Aion dataset
Kang et al. [18]	Action frequency & social activity	MMORPG (Aion)	A private Aion dataset
Mitterhofer et al. [22]	Trajectory	MMORPG (World of Warcraft)	A private dataset collected from World of Warcraft (only trajectories)
Bernardi et al. [8]	Action frequency & social activity	MMORPG (Aion)	A public Aion dataset
Gianvecchio et al. [14]	Action frequency	MMORPG (World of Warcraft)	A private dataset (keyboard and mouse events)
Alayed et al. [7]	Action frequency	FPS (Trojan Battles, developed for this research)	A private dataset (game events)
Kang et al. [17]	Social activity	MMORPG (Aion)	A private dataset (game events and chatting activity)
Kwon et al. [19]	Social activity & network-side	MMORPG (Aion)	A private dataset (trade log)
Thawonmas et al. [28]	Action frequency	MMORPG (Cabal Online)	A private dataset (event log)
Tao et al. [27]	Action frequency	NetEase MMORPG	A private dataset (event log)
Chung et al. [13]	Action frequency	MMORPG (Yulgang Online)	A private dataset (event log)

4 Bot Detection Methods

In this section, we answer RQ3 by classifying methods used for detection of gaming bots.

4.1 Supervised and Unsupervised Learning Methods

Most methods employ machine learning for bot detection. [8, 5, 24, 16]. These methods can employ a supervised learning algorithm or an unsupervised learning algorithm.

In case of supervised machine learning methods (specifically, classification algorithms), the software needs a *ground truth* dataset: with instances labeled as bots or ordinary users. Using such dataset, a bot classifier model can be trained. For an unknown instance, this trained model in turn is used to estimate the probability that the instance is a bot. If the probability is beyond a certain threshold, the instance is classified as a bot.

Unsupervised methods used for bots detection do not require learning a model using a training dataset. A popular unsupervised method is *anomaly detection*; they aim to detect rare or abnormal activity by the bots. Moreover, clustering of players can also be used for bot detection [27]. Here, the human players that are typically the majority of players in the gaming system, would form larger clusters than players suspected to be bots.

4.2 Method Classification based on User Behavior

Fig. 1. Taxonomy

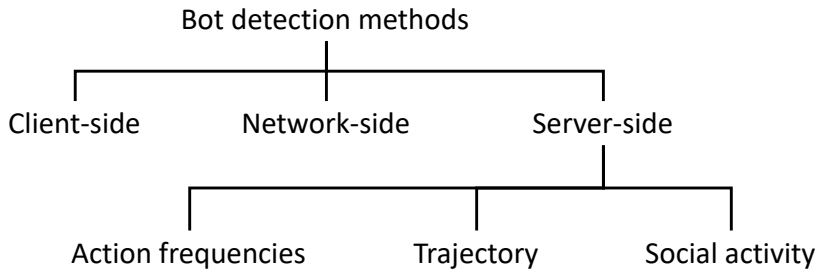

Figure 1 demonstrates the taxonomy of bot detection methods on the basis of user behavior. Bot detection methods can be classified into three categories [16]: client-side, network-side and server-side.

– **Client-side.** Client-side methods function similarly to anti-viruses. Players install these programs to their computers and the programs detect bots by monitoring information regarding processes that are being executed.

- **Network-side.** Network-side methods are based on analysis of the network traffic.
- **Server-side.** Server-side methods are based on behavior of players in the game. Server-side methods usually involve machine learning algorithms and can be classified based on the used features: action frequencies [14], character trajectory [11] and social activity [17].
  - **Action Frequencies.** Action frequency features are based on the number of times a character performed a particular action. For example, an action frequency feature can be a number of times an FPS character hit the target [7].
  - **Trajectory.** Character trajectory features are based on the movements of the character in the game, such as a trace generated by the character in Quake 2 [11].
  - **Social Activity.** Social activity features are based on social interactions between characters. There can be trades between characters [19] or messages sent from one character to another [17].

Table 1 summarizes the reviewed literature in terms of the presented taxonomy and our research questions. The majority of selected studies employ action frequency features, while some use both action frequency and social activity feature spaces. Trajectory features are the least popular according to the selected literature.

The reviewed bot detection methods are based on machine learning, either supervised or unsupervised. Most of the studies employ neural networks [8, 14] common classification algorithms, such as logistic regression [7], support vector machines [7] or naive Bayesian classifier [11].

Studies on bot detection also differ in terms of tasks:

- Detecting bots one by one. The majority of studies develop a method which classifies each character as a bot or a real user. For example, Thawonmas et al. [28] proposed a method to detect if a particular character is a bot.
- Detecting groups of bots. Kwon et al. [19] developed a method of detecting gold farming groups in World of Warcraft. These groups consist of several bots, where each of them plays one of the three roles: a gold farmer, a merchant or a banker. Gold farmers destroy monsters, collect game resources, such as money and items and pass them to merchants. Merchants items from game money and deliver them to bankers. Bankers sell game money for real money to other players.

Note: We notice that game bot detection methods are similar to methods for the detection of fake accounts on the social media sites [15], as fake account detection methods use the same fundamental assumption that the behavior of fake accounts is different from that of real users.

5 Future Directions

In this section, we address RQ4 and identify the following future directions for the detection of gaming bots on the basis of literature review:

- The studies on gaming bot detection mostly focus on MMORPG and disregard other game categories, such as strategy or action. Online games that belong to these genres also allow to accumulate resources between user sessions and suffer from bots. For example, the game Clash of Clans[25] is populated with bots[26]. Games of disregarded categories bring new challenges to the scientific community, as their game mechanics are different from that of MMORPG.
- Another future direction is the expansion of the types of machine learning models used for the detection of bots. For example, Markov Decision Process could be used to develop a model particularly for the detection of bots in online games.
- The majority of the review studies used up to two feature spaces (for example, action frequency and social activity). Meanwhile, employing a wider variety of features spaces has a potential to increase the detection accuracy. However, handling more feature spaces in many cases is more challenging than dealing only with a single feature space.

6 Conclusion and Future Work

Some online players use bots to gain virtual resources, without making efforts in gaming. This often results in negative effects on the revenue for the game development companies as well as dissatisfaction of the ordinary players. In this paper, we conducted a systematic literature review and focused mainly on games that allow accumulation of resources in subsequent session. We answered the following research questions:

- *RQ1. What game categories have received low attention from the scientific community for bot detection?*
  We found that the selected studies mostly target MMORPG and FPS games and disregard other categories of games, such as strategy, action and fighting.
- *RQ2. What are the publicly available datasets for bot detection?*
  We indicated two publicly available datasets: the Quake 2 dataset and the Aion dataset. Both datasets contain data on players' actions in the games, but majority of the datasets are not publicly available
- *RQ3. How can we detect bots in online games?*
  We presented a taxonomy of bot detection methods: client-side, network-side and server-side, which can be based on action frequencies, social activity or character trajectory. To detect bots, the reviewed studies used common classification algorithms and neural networks.
- *RQ4. What are the future directions of bot detection?*
  We indicated three future directions: targeting more game categories, the expansion of methods for detection bots and the combination of different feature spaces.

[25] https://supercell.com/en/games/clashofclans/
[26] https://www.raccoonbot.com/

In our future work, we are planning on extending this literature review with comparison of studies on the topic in terms of methodologies. Our future work also includes design of bot detection methods.

References

1. 7 Ways to Make Money Playing Video Games. https://ivetriedthat.com/7-ways-to-make-money-playing-video-games/, Accessed: 14.09.2018
2. G2G Corporate — Gaming For A Living. https://corp.g2g.com/, Accessed: 14.09.2018
3. Global Games Market Revenues 2018 — Per Region & Segment — Newzoo. https://newzoo.com/insights/articles/global-games-market-reaches-137-9-billion-in-2018-mobile-games-take-half/, Accessed: 14.09.2018
4. I will game: Anatomy of MMO addiction. https://www.cnet.com/news/i-will-game-anatomy-of-mmo-addiction/, Accessed: 14.09.2018
5. Ahmad, M.A., Keegan, B., Srivastava, J., Williams, D., Contractor, N.: Mining for Gold Farmers: Automatic Detection of Deviant Players in MMOGs . In: 2009 International Conference on Computational Science and Engineering. pp. 340–345. IEEE (2009)
6. Ahmad, M.A., Srivastava, J.: Behavioral data mining and network analysis in massive online games. In: Proceedings of the 7th ACM International Conference on Web Search and Data Mining. pp. 673–674. WSDM '14, ACM, New York, NY, USA (2014). https://doi.org/10.1145/2556195.2556196, http://doi.acm.org/10.1145/2556195.2556196
7. Alayed, H., Frangoudes, F., Neuman, C.: Behavioral-Based Cheating Detection in Online First Person Shooters using Machine Learning Techniques. In: Computational Intelligence in Games (CIG), 2013 IEEE Conference on. pp. 1–8. Citeseer (2013)
8. Bernardi, M.L., Cimitile, M., Martinelli, F., Mercaldo, F.: A Time Series Classification Approach to Game Bot Detection. In: Proceedings of the 7th International Conference on Web Intelligence, Mining and Semantics. p. 6. ACM (2017)
9. Brown, N., Sandholm, T.: Superhuman ai for heads-up no-limit poker: Libratus beats top professionals. Science (2017). https://doi.org/10.1126/science.aao1733, http://science.sciencemag.org/content/early/2017/12/15/science.aao1733
10. Chen, C.L., Ku, C.C., Deng, Y.Y., Tsaur, W.J.: Automatic Detection for online Games Bot with APP. In: Fog and Mobile Edge Computing (FMEC), 2018 Third International Conference on. pp. 289–294. IEEE (2018)
11. Chen, K.T., Liao, A., Pao, H.K.K., Chu, H.H.: Game bot detection based on avatar trajectory. In: International Conference on Entertainment Computing. pp. 94–105. Springer (2008)
12. Chun, S., Choi, D., Han, J., Kim, H.K., Kwon, T.: Unveiling a Socio-Economic System in a Virtual World: A Case Study of an MMORPG. In: Proceedings of the 2018 World Wide Web Conference on World Wide Web. pp. 1929–1938. International World Wide Web Conferences Steering Committee (2018)
13. Chung, Y., Park, C.y., Kim, N.r., Cho, H., Yoon, T., Lee, H., Lee, J.H.: Game bot detection approach based on behavior analysis and consideration of various play styles. ETRI Journal **35**(6), 1058–1067 (2013)
14. Gianvecchio, S., Wu, Z., Xie, M., Wang, H.: Battle of Botcraft: Fighting Bots in Online Games with Human Observational Proofs. In: Proceedings of the 16th ACM conference on Computer and communications security. pp. 256–268. ACM (2009)

15. Gurajala, S., White, J.S., Hudson, B., Matthews, J.N.: Fake Twitter Accounts: Profile Characteristics Obtained using an Activity-based Pattern Retection Approach. In: Proceedings of the 2015 International Conference on Social Media & Society. p. 9. ACM (2015)
16. Kang, A.R., Jeong, S.H., Mohaisen, A., Kim, H.K.: Multimodal game bot detection using user behavioral characteristics. SpringerPlus **5**(1), 523 (2016)
17. Kang, A.R., Kim, H.K., Woo, J.: Chatting Pattern Based Game BOT Detection: Do They Talk Like Us? KSII Transactions on Internet & Information Systems **6**(11) (2012)
18. Kang, A.R., Woo, J., Park, J., Kim, H.K.: Online game bot detection based on party-play log analysis. Computers & Mathematics with Applications **65**(9), 1384–1395 (2013)
19. Kwon, H., Mohaisen, A., Woo, J., Kim, Y., Lee, E., Kim, H.K.: Crime Scene Reconstruction: Online Gold Farming Network Analysis. IEEE Trans. Information Forensics and Security **12**(3), 544–556 (2017)
20. Laurens, P., Paige, R.F., Brooke, P.J., Chivers, H.: A Novel Approach to the Detection of Cheating in Multiplayer Online Games. IEEE (2007)
21. Levy, Y., Ellis, T.J.: A Systems Approach to Conduct an Effective Literature Review in Support of Information Systems Research . Informing Science **9** (2006)
22. Mitterhofer, S., Krügel, C., Kirda, E., Platzer, C.: Server-Side Bot Detection in Massively Multiplayer Online Games. IEEE Security & Privacy **7** (2009)
23. Ontañón, S., Synnaeve, G., Uriarte, A., Richoux, F., Churchill, D., Preuss, M.: A survey of real-time strategy game ai research and competition in starcraft. IEEE Transactions on Computational Intelligence and AI in Games **5**(4), 293–311 (Dec 2013). https://doi.org/10.1109/TCIAIG.2013.2286295
24. Prasetya, K., Wu, Z.d.: Artificial neural network for bot detection system in MMOGs. In: Proceedings of the 9th Annual Workshop on Network and Systems Support for Games. p. 16. IEEE Press (2010)
25. Rocha, J.B., Mascarenhas, S., Prada, R.: Game Mechanics for Cooperative Games. ZON Digital Games 2008 pp. 72–80 (2008)
26. Shiravi, A., Shiravi, H., Tavallaee, M., Ghorbani, A.A.: Toward developing a systematic approach to generate benchmark datasets for intrusion detection. computers & security **31**(3), 357–374 (2012)
27. Tao, J., Xu, J., Gong, L., Li, Y., Fan, C., Zhao, Z.: NGUARD: A Game Bot Detection Framework for NetEase MMORPGs (2018)
28. Thawonmas, R., Kashifuji, Y., Chen, K.T.: Detection of MMORPG Bots Based on Behavior Analysis. In: Proceedings of the 2008 International Conference on Advances in Computer Entertainment Technology. pp. 91–94. ACM (2008)