Mitigating Malware Attacks via Secure Routing in Intelligent Device-to-Device Communications

Hadeer Elsemary(✉)

Faculty of Mathematics and Computer Science,
Georg-August-University, Göttingen, Germany
hadeer.el-semary@informatik.uni-goettingen.de

Abstract. Device-to-Device (D2D) communications have received significant attention nowadays due to the excess number of applications and services. D2D communication promises a higher data rate, lower communication delays, and better power efficiency. Therefore, D2D is expected to be a vital technical component in Internet of Things (IoT) and play an important role with the next generation 5G. Moreover, the rapid growth in mobile capabilities opens the door to the cyber criminals that explore new avenues for malware attacks. Although the literature is proposed security schemes for malware attacks. However, the research field is still immature and unexplored in depth due to the fast evolution of malware at a rate far exceeding the evolution of security techniques. In this paper, the problem of detecting malware attacks is considered in D2D network and a secure energy-efficient routing protocol is proposed. The protocol aims at detecting malware attached to message before it infects the targeted device through optimal secure energy-efficient routes. Moreover, the protocol takes into account the attacker's behavior, computation of players' strategies including different attack cases and consideration of the dynamic scheme in terms of calculating malware detection capabilities and malware types due to the fast evolution of the malware. Through simulations, the proposed routing protocol is evaluated in terms of the detecting rate of the malicious messages and overall expected payoff of the defender compared with other non-strategic routing protocols. Results show that the game achieves Nash equilibrium, and leads to an optimal defense strategy for the network.

Keywords: Device-to-Device communication · Game theory · Malware · Security · Energy efficient routing

1 Introduction

Due to the recent rapid growth in demand of the mobile communication network, new technologies are proposed to improve throughput, communication delay and

A.E. Hassanien et al. (eds.), *Proceedings of the International Conference on Advanced Intelligent Systems and Informatics 2016*, Advances in Intelligent Systems and Computing 533, DOI 10.1007/978-3-319-48308-5_20

computational offloading. Due to this fact, Device-to-Device (D2D) communications are recognized as promising technologies for communications nowadays and in the near future [1]. D2D communication are proposed as a means of gathering the proximity, hop gains and reuse [2]. In addition, D2D enables the device to communicate directly without the involvement of Base Station (BS) or any central entity such that the communication occurs on either licensed or unlicensed spectrum [3].

Due to the recent market demand for new services such as context-aware, proximity services, the industry is exploiting new use cases and new business models based on D2D communication e.g., pervasive health-care monitoring, social networking, public safety and rescue and location based services. Therefore, D2D is expected to be a vital technical component in Internet of Things (IoT) and play an important role with the next generation 5G.

1.1 Problem Definition and Related Work

Due to impressive demand and benefits of D2D communication in different and large areas, new severe security threats are expected on D2D network. Furthermore, the direct connections between devices via short range technologies (i.e., WiFi, Bluetooth) are more vulnerable to security threats. The authors in [9] identify the important security requirements in D2D communication as well as survey and evaluate the existed security schemes. However, the academia and industry have not yet investigated the security issues of the D2D communication seriously.

Due to these capabilities, mobile devices are considered an attractive launching pad for malware attacks. However, this research field is still immature and unexplored in depth [5]. As a result, the mobile malware threats are considered as a hot topic in the next future.

In this paper, we review briefly some of the proposed secure routing protocols based on game theory that optimizing the intrusion detection in mobile wireless network (i.e., multi-hop D2D fashion) [13,14]. Apart from the secure routing protocols, another set of work based on game theory aims at optimizing the intrusion detection [7,8]. The presented stochastic routing protocol in [13] aims at mitigating the eavesdropping from the insider attacker and improving the fault tolerance. They select randomly among paths to forward the packets. In [10–12], the secure routing and packet forwarding game is proposed and they used game theory to study the interaction between the good nodes and malicious nodes under noise and imperfect monitoring. They derived the optimal defense strategies with extensive evaluation of the effectiveness of these strategies. The aforementioned work considered only the insider attackers. In [14], the authors proposed a zero-sum complete information game between network and attacker. They derived the defense strategy for network to detect malicious attacks based on complete information taking into consideration the energy consumption and the quality of service.

The proposed static Bayesian game [6] is one-shot game, where the defender does not take into consideration the evolution of the game. Thus, the defender maximizes his payoffs based on fixed prior beliefs about the types of his opponent.

1.2 Summary of Contributions

Due to the fact that this aforementioned research field is not fully developed, with this paper, a game theoretic routing protocol for D2D communications is proposed to the malware detection problem. It is worth mentioning that the game theory provides an extensive set of mathematical tools to plan for the real life security problems. In particular, adversaries are attempting to infect targeted devices residing in the D2D network through the compromised gateway. On the worst case, we assume that the adversaries exploit the vulnerabilities of the gateways to inject messages attached with malware as well as exploit the operating system vulnerabilities of the smart devices to mount sophisticated malware attacks. Thus, the adversaries need to be considered as rational players and their expected behaviors need to be taken into consideration. Our protocol RMSR models the malware detection problem as two players non-cooperative zero-sum repeated game between D2D network and the adversaries. The main objective of this paper is to propose an optimal secure and energy-efficient routing protocol taking into account the attacker strategies and actions as well as the fast evolution of the malware. We formulate the zero-sum repeated game case where the defender routes the traffic such that the value of the game is maximized. On other words, the defender selects the most secure routes that have the maximum capability of malware detection and enough residual energy for routing process. On the other hand, the attacker tries to be unpredictable to the defender by enriching his actions with different malware types.

This paper extended the work in [6] and the main contribution of this paper summarized as the following: first, presentation of realistic pervasive health monitoring scenario in case of outsider attacker as a case study. Second, consideration of a D2D network contains heterogeneous devices in terms of operating systems. Third, investigation of the repeated game for malware detection problem taking into account the attacker's behavior, computation of players' strategies including different attack cases and consideration of the dynamic scheme in terms of calculating malware detection probabilities and malware types due to the fast evolution of the malware. Finally, conduction of simulations using Omnet++ where the optimality of the defender strategies is verified. The rest of the paper is organized as follows: In Sect. 2, we present the system model describing the environment, the attack model and network setup. In Sect. 3, we introduce the mathematical notations used and formulate the game theoretic framework. In Sect. 4, we describe in details the RMSR routing protocol. In Sect. 5, we conduct simulation and compare RMSR with other protocols. Finally, Sect. 6 contains conclusion and remarks as well as an outlook on further extensions of the paper.

2 System Model

2.1 Environment

As a motivating example, a real world pervasive health monitoring scenario is considered as depicted in Fig. 1. In fact, real world mobile cloud-based health monitoring faces excessive networking latency and longer response time. As a result, there is a growing demand to improve human health and well-being in health care systems [15]. As shown in Fig. 1, smart gateway is exploited to offer several higher-level and low latency local services such as local storage and local data processing. In order to benefit from network-controlled D2D communications [2], the mobile devices in the immediate physical proximity are connected to other devices and form a local D2D network. The mobile devices communicate with one another in D2D multi-hop fashion by using short-range wireless connections such as WiFi in ad-hoc mode. The smart gateway act as a hub between mobile devices in the local D2D network and the remote health data center. The smart gateway provides the management of health records for the patients by storing, updating and retrieving all the medical information about the patients.

We denote any source device by S, which acts as a coordinator which manages the queries of patient health care record locally or remote data center in the Internet if necessary. Since the wireless channel is open and accessible to both legitimate network users and malicious attackers, adversaries can build their malicious access points known as Evil Twin attack which provides deceptive SSID and replace a legitimate gateway. As a result, the adversary is able to eavesdrop on network traffic, inject the infectious message and infect any device residing in a given local D2D network.

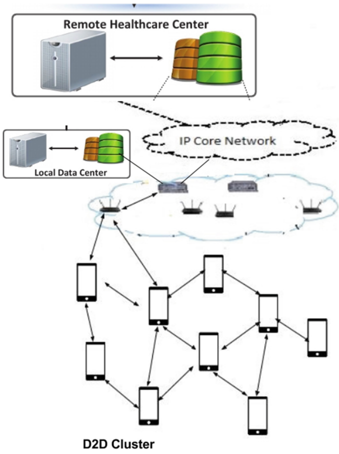

Fig. 1. Example of pervasive healthcare monitoring mobile network

2.2 Network Set-Up

In this paper, Consider a local D2D network of $\mathcal{N}$ heterogeneous mobile devices denoted by $[\mathcal{N}]$ such that the mobile devices are heterogeneous in terms of operating systems. For each message, there is a set of all routes $[R]$ from the S to targeted device. The S selects $r_j \in [R]$ to deliver message, where $[N_j]$ is the set of devices along the route r_j. We assume software-based malware detection systems with sophisticated detection capabilities to be deployed on each device. Every device is running anti-malware control and it can also carry out the real time network traffic monitoring. We have $\varOmega$ different mobile operating systems [6], expressed by the finite set $[\varOmega]$. We denote by $[\mathcal{M}_\omega]$ the set of $\mathcal{M}_\omega$ as a different malware available to the attacker to infect devices that run the mobile operating system ω. For each $\omega \in [\varOmega]$, we assume $\mathcal{C}_\omega$ anti-malware software (i.e., Resources) expressed by the finite set $[\mathcal{C}_\omega]$. Anti-malware detection software is residing on each mobile device n_i and each anti-malware software has its detection rate to detect successfully certain malware type. Since the routing is a cooperative process where the messages are relayed among devices. Any device along the route detects the intrusion with strong evidence of anomalies, it is responsible on responding quickly to the intrusion. as a result every device is responsible on inspecting the received message using its detection capability.

We denote by $D(c_k^i, \mathcal{M}_m)$ is the disability of the device n_i to detect the malware $\mathcal{M}_m$ (i.e., False negative [17]). As a result, for the fixed route r_j, the disability of r_j to detect $\mathcal{M}_m \in [\mathcal{M}_\omega]$ is given by:

$$D(r_j, \mathcal{M}_m) := \prod_{n_i \in N_j} D(c_k^i, \mathcal{M}_m) \tag{1}$$

then the route detection capability of r_j to successfully detect the $\mathcal{M}_m \in [\mathcal{M}_\omega]$ before it reaches the targeted device that runs ω (i.e., True Positive [17]) is given by:

$$\psi(r_j, \mathcal{M}_m) := 1 - D(r_j, \mathcal{M}_m) \tag{2}$$

In addition, the multi-hop D2D communication and malware detection process will necessitate cooperation between devices. Some devices may not collaborate to relay other device's traffic because of their limited available energy. Therefore, our protocol ensures the route availability during the routing process and considers the battery-level of the devices in the routing decision. It chooses the routes with highest energy devices on the basis of residual energy of the device. Formally the battery-level of device n_i, $n_i \in [\mathcal{N}]$ is given by: $\mathcal{E}(n_i) = \frac{\mathcal{E}_r}{\mathcal{E}_{max}}$, such that $\mathcal{E}_r$ is the remaining energy and $\mathcal{E}_{max}$ is the maximum energy available for the device. Therefore the route battery-level on r_j is derived by multiplying the battery-level of all the devices along the route as follows:

$$\mathcal{E}(r_j) := \prod_{n_i \in N_j} \mathcal{E}(n_i) \tag{3}$$

3 Repeated Malware-Defense Secure Routing Games (RMSR)

To investigate the interactions between the defender and the adversary, a non-cooperative two-players game is considered that played by the D2D devices (defender) and the adversary (attacker) in order to derive the optimal defense strategic decisions for the defender. We assume that the attacker exploits zero-day vulnerability of the mobile operating system. Therefore, he selects the malware that targets the vulnerability of certain platform running on the targeted device. On the other hand, the defender has the statistics about different existing malware types for each mobile platform ω. Furthermore, the mobile devices learns more about the attacker actions from the IDS during the subsequent repeated game. Continuing with the notations mentioned in [6]:

- **Strategy Set**: The strategy set of a player refers to all available moves the player is able to take. We consider that the defender's pure strategies is a set of all possible routes $r_j \in [R]$ from the S to the targeted device. The attacker's pure strategy is a set of different malware types $\mathcal{M}_m \in [\mathcal{M}_\omega]$ from which the attacker selects to send to the targeted device aiming its infection.
- **Payoff**: we define the $\mathcal{U}_\Theta$ as the payoff of the defender. The payoff of the defender depends on the route detection capability and the route availability. We define $\mathcal{U}_\Psi$ as the payoff of the attacker of type $\omega \in \Omega$, where the attacker's payoff is opposite to defender's payoff (i.e. zero sum game).

We consider the defender is the row player in the payoff matrix and the attacker are the column player. For a given pure strategy profile $(r_j, \mathcal{M}_m)$, $r_j \in [R]$, $\mathcal{M}_m \in [M_\omega]$ where $\omega \in \Omega$, the payoff of the defender is given by

$$U_\Theta(r_j, \mathcal{M}_m; \omega) = [\psi(r_j, \mathcal{M}_m)\mathcal{V} + \mathcal{E}(r_j)] \tag{4}$$

We assume the $\mathcal{V}$ is the defender's security gain value (monetary), where $\mathcal{V} > 0$. The defender's payoff is the expected gain of detecting the malware before infecting the targeted device depends on the route detection rate in Eq. (1) summed up the route energy level in Eq. (2).

The defender's mixed strategy X $= [x_1, x_2, \ldots, x_\xi]$ is the probability distribution over different routes in $[R]$ (i.e. Pure strategies) from the source device S to the targeted device. Where x_j is probability that the defender will choose its j-th route to send the message.

For each $\omega \in \Omega$, the attacker's mixed strategies $Y^\omega = [y_1^\omega, y_2^\omega, \ldots, y_\eta^\omega]$ is the probability distribution over different malware (i.e. Pure strategies) against targeted devices that run ω. Where y_l^ω is probability that the attacker will choose its l-th malware to infect device that runs ω. In two players zero-sum game with finite number of actions for both players, there is at least a Nash equilibrium in mixed strategy [16]. The RMSR game consists of mixed strategy profile (X, Y^ω), therefore the expected payoff of the defender is denoted by:

$$\mathcal{U}_\Theta \equiv U_\Theta(X, Y^\omega) = \sum_{x=1}^{\xi}\sum_{l=1}^{\eta} x_j y_l^\omega U_\Theta(r_j, \mathcal{M}_m; \omega) \tag{5}$$

For zero sum game, $\mathcal{U}_{\Psi} = -\mathcal{U}_{\Theta}$, This means that the defender's gain is considered the attacker's loss.

4 Repeated Malware-Defense Secure Routing Protocol

Our proposed protocol RMSR stages as follows:

Route Discovery Stage: First the S node broadcasts a Route Request message, the devices that receive this message should broadcast it to their neighbors. If the receiving device is the targeted device, it sends back the Route Reply message containing the full reverse source route. We have appended two new fields in the Route Reply message (route detection capability, route battery-level). Each intermediate device on receiving the Route Reply, updates the route detection rate field by multiplying its detection capabilities using Eq. (1) and updates the route battery-level field using Eq. (3). When the Route Reply reaches the S, it calculates overall route detection rate using Eq. (2)

Route Selection Stage: After the S node receives several routes, then stores its routing table. It uses its routing table to solve the RMSR game and deriving the optimal defense strategy X^*. The S node selects the best route probabilistically according to X^* to send the message.

5 Performance Evaluation

In this section, we have conducted the simulations to evaluate the effectiveness of the optimal defense strategies of the defender and identify when these strategies can work well. In these simulations, mobile devices are randomly deployed inside a rectangular area of 800×800 m and are conducted in Omnet++ network simulator, INET framework and fixed parameters are shown in Table 1. The simulation time changes (10, 20, 40, 60 min) with total number of 7000 messages and 1000 from total messages is malicious messages. We consider one attacker who sends a sequence of malicious messages to a certain target aiming at infecting the targeted device. We plot the detecting rate of malicious messages for three routing protocols (RMSR, DSR, AODV) in case of 3 different attack cases. We evaluate the performance of the optimal defense strategy for RMSR in terms of the detected rate of the malicious messages comparing with other nonstrategic protocols DSR and AODV. We investigate the properties of the Nash equilibrium in RMSR game through the simulations and conduct the results of our study. In the Fig. 2 shows the results of the detecting rate of the malicious messages, varying the pause times in case of different attack cases. In case of Optimal attack, it can be observed that the detecting rate of the malicious messages are small for AODV and DSR protocols, while the RMSR protocol still keeps the detecting rate high even in a hostile environment. Whilst in the case of Uniform attack, it can be noticed that RMSR protocol outperforms the other two ad-hoc protocols and still has high detecting rate of malicious messages. On the other hand, in case of the worst weighted attack, RMSR protocol still outperforms

Table 1. Simulation parameter values

Parameter	Value
Number of nodes	20
Mobility model	Linear Mobility
Mobility Speed	10 mps
Mobility Update Interval	0.1 s
Packet size	512 bytes
Packet generation rate	2 packets/s

the other two protocols and has highest detecting rate of malicious messages. We can notice the average values of the detecting rate of malicious messages in case of a Uniform attack as non-strategic attack within the range [83 %, 78 %]. Whilst in case of Optimal attack the average values of the detecting rate of the malicious messages within the range [75 %, 71 %] as well as in the worst case of the weighted attack the average values of the detecting rate of the malicious messages are approximately 70 %. Likewise in Fig. 3 shows the results of the expected payoff of the defender in case of different attack cases. It is observed that RMSR protocol outperforms the other non-strategic protocols and achieved the highest expected payoff for the defender in all cases. Therefore, we can notice that the RMSR protocol have steadily the best performance even in the worst case.

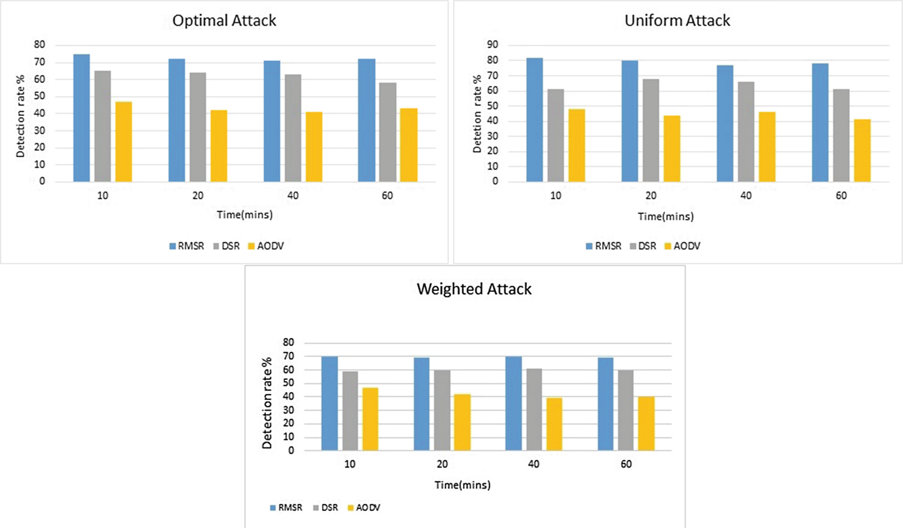

Fig. 2. Detecting rate of malicious packets for 3 different attack cases

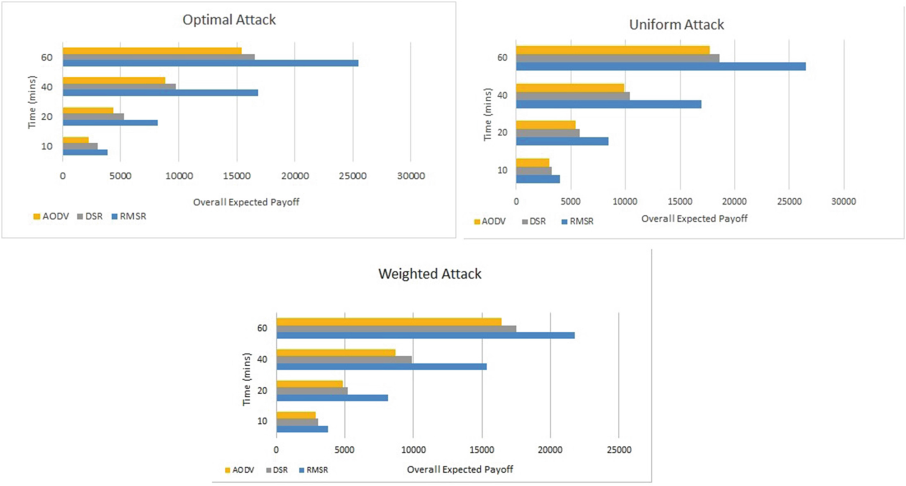

Fig. 3. Expected payoff of the defender for 3 different attack cases

6 Conclusion and Future Work

In this paper, the problem of detecting the malicious messages is considered in the D2D network in a game-theoretic framework in the presence of outsider attacker. A Repeated security game between the D2D network and the attacker is modeled. We show that the game has the Nash equilibrium leading to optimal defense strategy. The defender must design an effective defense scheme to detect malicious messages injected into the network by the attacker. We considered the scenario where the defender has the information about the optimal routes obtained from the RMSR game and can pick the routes to maximize the chances of the detection. Results show that RMSR protocol based on strategic plan outperforms the other non-strategic protocols. Finally, we have estimated the performance of the proposed RMSR protocol on the D2D network. In future work, we plan to consider that the insider attacker case that has control on the IDS, then there is no trust guarantee among the devices and each device will inspect message independently and will try to find the next hop to forward the message.

References

1. Mumtaz, S., Rodriguez, J. (eds.): Smart Device to Smart Device Communication. Springer International Publishing, Switzerland (2014)
2. Fodor, G., Parkvall, S., Sorrentino, S., Wallentin, P., Lu, Q., Brahmi, N.: Device-to-device communications for national security and public safety. IEEE Access **2**, 1510–1520 (2015)
3. Asadi, A., Wang, Q., Mancuso, V.: A survey on device-to-device communication in cellular networks. IEEE Commun. Surv. Tutorials **16**, 1801–1819 (2014)

4. Khouzani, M.H.R., Sarkar, S., Altman, E.: Maximum damage malware attack in mobile wireless networks. IEEE/ACM Trans. Netw. **20**(5), 1347–1360 (2012). Dreese Laboratories, Ohio State University, Columbus, OH, USA
5. Khouzani, M.H.R., Sarkar, S., Altman, E.: Saddle-point strategies in malware attack. IEEE J. Sel. Areas Commun. **30**, 31–43 (2012)
6. Elsemary, H., Hogrefe, D.: Malware-defense secure routing in intelligent device-to-device communications. In: 1st International Conference on Advanced Intelligent System and Informatics (AISI2015), Beni Suef, Egypt. Springer (2015)
7. Wang, W., Chatterjee, M., Kwiat, K.: Coexistence with malicious nodes: a game theoretic approach. In: International Conference on Game Theory for Networks, GameNets 2009, pp. 277–286 (2009)
8. Liu, Y., Comaniciou, C., Man, H.: A Bayesian game approach for intrusion detection in wireless ad hoc networks. In: Proceedings from the 2006 Workshop on Game Theory for Communications and Networks, GameNets 2006, p. 112 (2006)
9. Wang, M., Yan, Z.: Security in D2D communications: a review. In: Trustcom/BigDataSE/ISPA, vol. 1, pp. 1199–1204 (2015)
10. Yu, W., Ji, Z., Liu, K.J.R.: Securing cooperative ad-hoc networks under noise and imperfect monitoring: strategies and game theoretic analysis. IEEE Trans. Inf. Forensics Secur. **2**, 240–253 (2007)
11. Yu, W., Liu, K.J.R.: Game theoretic analysis of cooperation stimulation and security in autonomous mobile ad hoc networks. IEEE Trans. Mob. Comput. **6**, 507–521 (2007)
12. Yu, W., Liu, K.J.R.: Secure cooperation in autonomous mobile ad-hoc networks under noise, imperfect monitoring: a game-theoretic approach. IEEE Trans. Inf. Forensics Secur. **3**, 317–330 (2008). Department of Electrical & Computer Engineering, University of Maryland, College Park, MD, USA
13. Bohacek, S., Hespanha, J.P., Lee, J., Lim, C., Obraczka, K.: Game theoretic stochastic routing for fault tolerance and security in computer networks. IEEE Trans. Parallel Distrib. Syst. **18**, 1227–1240 (2007)
14. Panaousis, E., Alpcan, T., Fereidooni, H., Conti, M.: Secure message delivery games for device-to-device communications. In: Poovendran, R., Saad, W. (eds.) GameSec 2014. LNCS, vol. 8840, pp. 195–215. Springer, Heidelberg (2014). doi:10.1007/978-3-319-12601-2_11
15. Rahmani, A.-M., Kumar, N., Gia, T.N., Granados, J., Negash, B., Liljeberg, P., Tenhunen, H.: Smart e-Health gateway: bringing intelligence to internet-of-things based ubiquitous healthcare systems. In: 12th Annual IEEE Consumer Communications and Networking Conference (CCNC) (2015)
16. Nash, J.F.: Equilibrium points in N-Person games. Proc. Natl. Acad. Sci. **36**, 48–49 (1950)
17. Fawcett, T.: An introduction to ROC analysis. Pattern Recogn. Lett. **27**, 861–874 (2006)