Mathematical Biosciences and Engineering

MBE, 16(6): 6683–6695.
DOI: 10.3934/mbe.2019333
Received: 06 January 2019
Accepted: 04 May 2019
Published: 24 July 2019

http://www.aimspress.com/journal/MBE

Research article

ONS resolution prediction based on Rasch model

Huqing Wang [1], Feng Xiang[2], Wenbing Zhao[3] and Zhixin Sun [1,*]

[1] Technology Research and Development Center of Postal Industry of State Post Bureau, Nanjing University of Posts and Telecommunications, Nanjing 210003, China
[2] Yuan Tong Express co. LTD, Shanghai, 201705, China
[3] Cleveland State University, Cleveland; OH, United States

*** Correspondence:** Email: sunzx@njupt.edu.cn.

Abstract: IoT (Internet of Things) involves a wide range of fields, and its application scenarios are complex and diverse. Failure of security defense in any link of IoT may lead to huge information leakage and immeasurable losses. IoT security problem is affecting and restricting its application prospect, and has become one of the hotspots in the field of IoT. ONS (Object Naming Service) is responsible for mapping function from EPC code information to URI (Uniform Resource Identifier). The security mechanism of ONS has been extensively studied by more and more scholars in recent years. The purpose of this paper is to apply Rasch, a famous psychological model, to ONS resolution security technology. Through observing the past resolution result, the ability of ONS resolution and the difficulty of EPC code can be calculated. With the difference between the ability of ONS resolution and the difficulty of EPC code, this model can predict the probability of the ONS future resolution to achieve the purpose of privacy protection in IoT addressing. Through simulation and Ministep software, the feasibility of the model is verified.

Keywords: IoT addressing; ONS; security; Rasch; EPC; IoT security

1. Introduction

The emergence of the concept of IoT has attracted the attention of countries and enterprises all over the world [1–3]. The United States has formulated the Advanced Manufacturing Partnership Program and the President's Innovation Partnership Program successively, encouraging enterprises to cooperate with universities and jointly formulate relevant technical standards for IoT. The European Union adopted the horizon 2020 plan in 2013. Japan launched the "i-Japan" strategic plan for 2015,

aiming at building a people-oriented and dynamic digital society, so that digital information can be integrated into every corner like air and water [4]. The South Korean government has released the ICT research and development plan to develop IoT platform, which is one of the top 10 key technologies [5]. IBM actively conducts research on Intelligent IoT, and proposes the use of intelligent IoT to excavate the potential of cognitive era. Amazon launched the AWS IoT fully hosted cloud platform to support the interaction of billions of devices with cloud applications and devices. Intel makes use of edge computing nodes and cooperates with Jingdong to build Jingdong convenience store. It integrates and analyses the data collected by all IoT devices so that customers and shopkeepers can enjoy the responsive retail experience at the same time and help the retail industry digitalize and intellectualize.

IoT covers the communication between things and things, between things and people. It has a huge system, involves a wide range of fields, and its application scenarios are complex and diverse [6]. Failure of security defense in any link of IoT may lead to huge information leakage and immeasurable losses [7]. At the same time, in the era of steady progress of communication network and computer technology, intrusion attack technology is becoming more and more intense. Therefore, the normal development and promotion of IoT can be guaranteed only by studying the security mechanism of IoT, filling the security loopholes constantly, building the security defense system of IoT and ensuring the security of communications and data in IoT. Many scholars have realized the importance of the safety of IoT, and have made many researches in this field [8].

Aiming at the research of IoT addressing security issues, this paper applies Rasch, a famous psychological model, to ONS resolution security technology. With Rasch model, the ability of ONS resolution and the difficulty of EPC code are calculated. With the difference between the ability of ONS resolution and the difficulty of EPC code, this model can predict the probability of the ONS future resolution to achieve the purpose of privacy protection in IoT addressing. This paper is organized as follows. Section 2 investigates the current ONS security solutions. Section 3 introduces Rasch model. Section 4 applies Rasch model to ONS security. Fully, future trends are forecasted in Section 5.

2. Related work

Because of the intrinsic characteristics of IoT, the security problems in IoT addressing not only need to solve the inherent security threats brought by the extension of the Internet, but also need to deal with the further needs of IoT users for privacy protection. While introducing and improving the existing security solutions of the Internet, we need to study the solutions for the characteristics of IoT [9], such as coding resolution, information discovery mechanism and the security solution of 6LoWPAN in IoT addressing architecture. This paper focuses on the security technology in ONS resolution.

ONS resolution system in IoT basically follows DNS method [10]. DNS was designed on the basis of mutual trust model. It is a completely open collaboration system without proper information protection and authentication mechanism. But the premise of mutual trust model is not established in the environment of IoT. The security threats of ONS lie mainly in the following aspects:

(1) lack of authentication for ONS server

Lack of authentication for ONS server will bring two threats. Firstly, the reliability of the resolution results cannot be verified. The results from ONS server may be some illegal websites such

as spam information. Secondly, the ONS server without authentication has the risk of revealing EPC, and the user privacy information is not protected.

(2) lack of authentication for ONS client

Lack of authentication for ONS client can lead to a more common security problem----DOS (Deny of Services) attack. An attacker uses one or more computers to send a large number of requests to the ONS server in a very short period of time. If the server is unable to process these requests, a denial of service phenomenon will occur.

(3) plaintext transmission

The last step of ONS resolution still relies on the existing DNS methods. But DNS query requests and returned results are plaintext without any security mechanism. Plaintext transmission brings two threats. Firstly, the malicious attackers can arbitrarily tamper with the contents of the returned results and implement resolution deception. Secondly, plaintext transmission makes it easy for attackers to implement real-time monitoring of user access requests, resulting in the leakage of user privacy.

The security of ONS is the foundation of EPC addressing. The design and architecture of ONS is based on DNS and inherited the security flaws of DNS [11]. The main threats of DNS are DDoS [12], malicious redirection, man-in-the-middle, domain name spoofing, cache poisoning, single point failure, etc. Most attacks are caused by the lack of necessary authentication mechanism in DNS. Unauthorized attackers return forged malicious domain name information to clients. Setting up the cache of resource records on the server can directly query the parsed resources in TTL (Time to Live) to reduce the traffic and latency. However, DNS lacks the mechanism of checking additional data. The attacker uses this vulnerability to store malicious resource records with large TTL value into cache and spread them to realize the cache poisoning attack. The structure of DNS server is tree oriented, which can lead to single point failure. DNS resolution is a hierarchical recursive or iterative process. If any node in the resolution path fails, it will lead to the failure of the whole resolution. Specially, if the high-level node fails, the impact of the failure will be greater, and even lead to the paralysis of the whole network.

The main security solutions of DNS are DNSSEC [13] and DNSCurve [14]. Considering the vulnerability of existing DNS, DNSSEC introduces public key encryption and authentication mechanism to achieve end-to-end data authenticity and integrity authentication through signature. DNSSEC has some problems such as low system efficiency, complex key management and difficult deployment. Through large-scale experiments, it is concluded that the adoption of DNSSEC may cause some users to refuse service, and a balance must be made between cost and benefit. DNSSEC use RSA algorithm to realize electronic signature, so as to verify the source of DNS data and the integrity of the transmission process, but without encrypting. DNSCurve uses Curve25519, a faster elliptic curve encryption algorithm, and a random number to protect the confidentiality of DNS data. Encrypting DNS data packets, verifying DNS reply packets and clearing forged DNS data packets, DNSCurve can enhance the confidentiality, integrity and availability of DNS resolution.

Because of the similarity between ONS and DNS, applying these two schemes to ONS can improve the security of ONS to a certain extent, but at the same time, due to the particularity of ONS, it is not necessarily possible to achieve ideal results. Through authentication algorithm, eliminating malicious nodes is a common method in communication security. Wu Zhenqiang et al. proposed a

secure transmission model of the IoT, which realized the secret transmission of goods information. During the transmission process, the remote item information server encrypts the item information nestedly with the public key from the back to the front according to the order of the nodes in the response path. The encrypted data is decrypted one by one layer until the item information is restored to plaintext at the local information server. The session key used in each query is dynamically generated in one-time-pad. At the same time, each node uses the filling mechanism to keep the size of the communication packet unchanged to resist attacks such as traffic analysis [15]. Document [16] proposes a secure ONS query protocol, which consists of two parts. One is to use the second-generation onion routing protocol to resist eavesdropping and traffic attacks, and to prevent the leakage of EPC information by hiding the network topology in the public network. The other is the extended DNS protocol, which can solve the trust link problem in long-distance transmission. A certificateless public key cryptosystem is adopted. Users negotiate session keys across domains by multiple KGC (Key Generation Center) to control the length of anonymous routing links and realize the purpose of anonymous sending query information by local servers. Some scholars have proposed ONS solution based on P2P structure [17]. This solution needs to change the existing network topology structure, which is difficult to deploy.

Most of the above research results are based on cryptography. In order to resist the transmission of plaintext information and enhance the confidentiality of data information, encryption scheme can be adopted. In order to resist the forgery and impersonation of malicious users, identity authentication and digital signature schemes can be adopted. However, these schemes will bring certain computing and communication overhead, not suitable for IoT [18]. In order to reduce the computation and communication overhead, this paper proposes an ONS security resolution scheme based on Rasch model. Through historical resolution behavior, the ability of ONS server and the difficulty value of EPC coding are calculated quantitatively, and the probability of future resolution success can be predicted.

3. Rasch model

Rasch model is a latent trait model proposed by Georg Rasch, a Danish mathematician and statistician, based on item response model [19]. It measures potential variables that cannot be observed directly by the individual's performance on the topic. According to Rasch model principle, the probability of a specific individual responding to a particular topic can be expressed by a simple function of individual ability and difficulty of the topic. Whether an individual answers a question correctly or not depends entirely on the comparison between individual ability and difficulty. Based on the principle of dichotomy, in Rasch model, the relationship between the ability of an individual, the difficulty of a question and the probability of an individual giving the correct answer can be expressed by the formula (1) or (2).

$$P_{ni}(X_{ni} = 1/A_n, D_i) = \exp(A_n - D_i) / [1 + \exp(A_n - D_i) \tag{1}$$

$$\ln [\frac{P_{ni}(x_{ni}=1/A_n, D_i)}{1-P_{ni}(x_{ni}=1/A_n, D_i)}] = A_n - D_i \tag{2}$$

In formula (1) and (2), let A_n be the ability of individual n, D_i be the difficulty of topic i, then the probability of individual n giving the correct answer about topic i can be expressed as following:

$$P_{ni}(x_{ni} = 1/A_n, D_i)$$

And, the probability of individual n giving the wrong answer about topic i can be expressed as following:

$$P_{ni}(x_{ni} = 0/A_n, D_i) = 1 - P_{ni}(x_{ni} = 1/A_n, D_i)$$

$$P_{ni}(x_{ni} = 1/A_n, D_i) \in [0,1], P_{ni}(x_{ni} = 0/A_n, D_i) \in [0,1], A_n - D_i \in (-\infty, +\infty)$$

From the above two formulas, it can be seen that the probability of an individual giving the correct answer to one question is related to the difference between his ability and the difficulty of the question. The greater the difference, the greater the probability of correct answer; conversely, the smaller the difference, the greater the probability of error answering. When the two are equal, that is

$$A_n - D_i = 0,\ P_{ni}(x_{ni} = 1/A_n, D_i) \in [0,1] = 50\% \ .$$

Individual ability and task difficulty are independent of each other in Rasch model. Whether the difficulty coefficient is large or small, the individual's ability is constant, and the task difficulty is constant regardless of the ability to select strong or weak test individuals. Therefore, comparing the potential abilities of different individual m and n , the ratio of success to failure is also constant for different tasks i and j. According to these characteristics, the ability of individual n and the difficulty of task *i* can be deduced as follows:

$$A_n = \ln\left(\frac{p_{n0}}{1 - p_{n0}}\right), \quad D_i = \ln\left(\frac{1 - p_{0i}}{p_{0i}}\right)$$

In traditional measurement methods, people used to use 0 to 100 scores to describe the level of the surveyed person. However, this fraction does not represent the ability of the person being measured. For example, the same gap is 5 points, but the difference between 100 and 95 points and between 45 and 40 points is obviously different. Rasch model, through logarithmic transformation method, that is, Logit method, calibrates individual ability and difficulty to the same single dimension, realizes the equidistant meaning between individuals, between subjects and between individuals and topics, and overcomes the non-objectivity in traditional measurement methods.

4. Application of Rasch model in ONS

4.1. Model description and definition

In this section, Rasch model is applied to ONS resolution security. The individual capability in the original model is defined as the ability and credibility of ONS server to parse EPC code successfully. The difficulty in the original model is defined as the parsing difficulty of EPC code provided by ONS client. In practical applications, this difficulty can be weighted by metrics such as security, credibility, privacy level and so on. The main idea of this model is to transform logarithmically the historical parsing results (i.e. the observed values), and then adjust the parsing difficulty of EPC codes and the capability value of ONS servers through multiple iterations. Finally, the model converges to more stable values of difficulty and capability, and displays them on the measurement structure chart. According to the redefinition of the parameters in the Rasch model mentioned above, this paper presents a prediction model for the analytical success probability of ONS.

$$Pr_{ij}(Aons_i, Depc_j) = \frac{e^{Aons_i - Depc_j}}{1+e^{Aons_i - Depc_j}} \tag{3}$$

The symbols in the above formula are shown in Table 1.

Table 1. The Description of Symbols.

Symbol	Description
$Aons_i$	the ability of ONS *i*
$Depc_j$	the difficulty of EPC *j*
Pr_{ij}	the probability of ONS *i* successfully resolving EPC *j*

The algorithm flowchart is shown below.

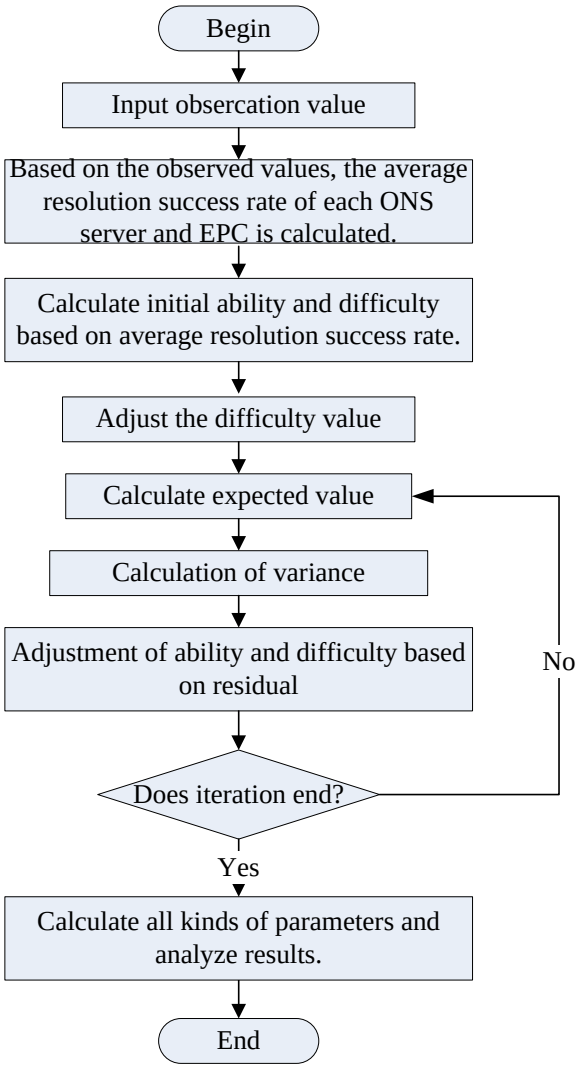

Figure 1. Algorithm Flowchart.

In the above algorithm flow, firstly, according to the actual resolution result, input the observation value, and get the average resolution success rate. According to the average resolution

success rate, the initial difficulty value of each EPC and the initial capability value of each ONS server can be calculated. Then, through several iterations, the capability and difficulty value can be constantly adjusted according to the expected value, variance and other parameters in the literation. Finally, after the iteration, according to the analysis of multiple parameters, the reliability of capability and difficulty value can be evaluated.

4.2. Specific algorithm

In the classical Rasch measurement method, the individual ability or task difficulty is generally estimated and predicted by prior observation. Through simulation experiments, we take *m* ONS servers and *n* EPC codes. The priori observation results are expressed by matrix T:

$$\mathrm{T} = \begin{bmatrix} t_{11}\, t_{12} & \cdots & t_{1n} \\ t_{21}\, t_{22} & \cdots & t_{2n} \\ \vdots & \ddots & \vdots \\ t_{m1}\, t_{m2} & \cdots & t_{mn} \end{bmatrix}$$

T_{ij} indicates the result of ONS *i* parsing EPC *j*, if success, then $t_{ij} = 1$; else $t_{ij} = 0$.

The algorithm steps are as follows:

The average parsing success rate of each ONS and EP is calculated according to the observed values, and the initial capability value and difficulty value are calculated according to the average parsing success rate.

$$S_{ons_i} = \frac{\sum_{k=1}^{n} t_{ik}}{n}, \quad A_{ons_i} = ln\frac{S_{ons_i}}{1 - S_{ons_i}} \quad ,\{i \in [1,2,\cdots m]\}$$

$$S_{epc_i} = \frac{\sum_{k=1}^{m} t_{ik}}{m}, \quad D_{epc_i} = ln\frac{S_{epc_i}}{1 - S_{epc_i}} \quad ,\{i \in [1,2,\cdots n]\}$$

Adjust the difficulty value

$$AD_{epc_i} = D_{epc_i} - \frac{\sum_{k=1}^{n} D_{epc_i}}{n} \quad , \qquad \{i \in [1,2,\cdots n]\}$$

Adjusting the difficulty value is to subtract the average difficulty value from the difficulty of each EPC.

The expected value *E* is calculated to represent the average success probability of a particular ONS server when parsing an EPC code. According to the formula:

$$E = 0 * p(0) + 1 * p(1)$$

That is to calculate each possible success probability by multiplying the corresponding probability. According to the Rasch model, we get:

$$E_{ij} = \frac{e^{Aons_i - Depc_j}}{1 + e^{Aons_i - Depc_j}}$$

Calculate variance *D*. Because the data in Rasch model belong to 0 and 1 two item distributions, variance *D* can be calculated by:

$$D_{ij} = E_{ij} * \left(1 - E_{ij}\right)$$

Continue to adjust the difficulty and ability values.

First, the residual value is calculated based on the difference between the observed value and the expected value.

$$R_{ij} = t_{ij} - E_{ij}$$

The sum SR_E of residual values on the dimension of coding difficulty is adjusted according to the previous EPC difficulty value:

$$AD'_{epc_i} = \frac{AD_{epc_i} - SR_E}{-1 * \sum_{k=1}^{m} D_{ki}} \ , \qquad \{i \in [1,2,\cdots n]\}$$

Similarly, the sum SR_O of the residual value on the ONS server dimension is adjusted according to the previous ONS ability value:

$$AA'_{ons_j} = \frac{A_{ons_j} - SR_o}{-1 * \sum_{k=1}^{n} D_{jk}} \ , \qquad \{j \in [1,2,\cdots m]\}$$

Calculate whether the sum of the squares of the residual is infinitely close to 0 as the basis for judging the end of the iteration.

If the end condition of iteration is not satisfied, then jump to step (3) and continue iteration. Through maximum likelihood method, the value of ONS ability and EPC difficulty are adjusted continuously, and finally the ONS ability value and EPC difficulty value are obtained.

After the iteration, some parameters are set up to analyze the results.

The fitting value *F* is obtained by dividing the square of the residual value by variance.

$$F = \frac{R^2}{D}$$

The average value *AF* of the fitted value F is a statistic sensitive to outliers.

$$AF = average(F)$$

The internal fitting value *InF* is obtained from the sum of the residual squared sum divided by variance sum.

$$InF = \frac{\sum R^2}{\sum D}$$

4.3. Simulation results and analysis

Through simulation, we obtain the resolution result expressed in the form of 10 × 10 matrix as follows:

1									
0									
1									
0									
1									
0									
1									
1									
0									
0									

After 3 iterations of the Rasch model algorithm, the ONS ability value and the difficulty value of EPC are shown in Table 2.

Table 2. ONS ability value and EPC difficulty value.

EPC ONS	1	2	3	4	5	6	7	8	9	10	New ability value
1	0.43	−0.9	0.55	0.32	−0.5	−0.3	0.43	−0.2	0.67	−0.6	0.02
2	−0.2	0.43	−0.2	−0.3	0.85	−0.1	−0.2	−0.1	−0.1	−0.2	−1.58
3	0.06	0.02	0.1	0.04	−0.9	0.16	0.07	0.27	0.16	0.07	2.44
4	−0.2	0.43	−0.2	−0.3	0.85	−0.1	−0.2	−0.1	−0.1	−0.2	−1.57
5	0.43	−0.9	−0.5	0.32	0.55	−0.3	0.43	−0.2	−0.3	0.43	0.02
6	−0.5	0.2	−0.3	0.43	−0.3	0.76	−0.5	0.86	−0.2	−0.5	−0.45
7	0.43	0.14	0.55	−0.7	0.55	−0.3	0.43	−0.2	−0.3	−0.6	0.02
8	0.43	0.14	−0.5	0.32	−0.5	−0.3	0.43	−0.2	−0.3	0.43	0.02
9	−0.5	0.2	−0.3	0.43	−0.3	−0.2	−0.5	−0.1	0.76	0.55	−0.45
10	−0.5	0.2	0.66	−0.6	−0.3	0.76	−0.5	−0.1	−0.2	0.55	−0.45
New difficulty value	−0.3	−1.8	0.22	−0.7	0.21	0.75	−0.3	1.42	0.75	−0.3	0.15

The Outfit and Infit values of the ONS servers and EPC are shown in Figure 2 below. The Outfit values of *ONS_1, ONS_5, ONS_6* and *ONS_10* are greater than 1, which show that the ability of these servers is too high or too low relative to the EPC. The Infit values of *ONS_1, ONS_3, ONS_6* and *ONS_10* are greater than 1, which show that the resolution process is interfered by other factors.

The Outfit values of *EPC_2, EPC_5* are greater than 1, which show that the difficulty of these EPC is too high or too low relative to the ONS server. The Infit values of *EPC_2, EPC_5* are greater than 1, which show that these EPC contain many factors beyond testing.

From the bubble Figure 3 of ONS and EPC, it can be seen that most of the ONS servers and EPC codes are located near the axis of mean square 0, but *ONS_8* and *EPC_5* are abnormal.

Through the Ministep software, we can generate the Logit diagram of ONS ability value and EPC difficulty value, as shown in Figure 4. After the conversion of ONS ability value and EPC difficulty value by Logit value, both of them are measured by Logit and displayed on the same scale, which is comparable.

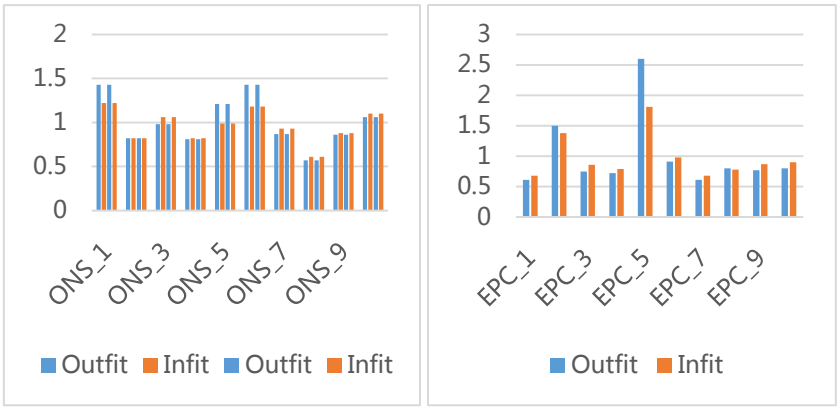

Figure 2. Outfit and Infit Values of ONS Servers and EPC.

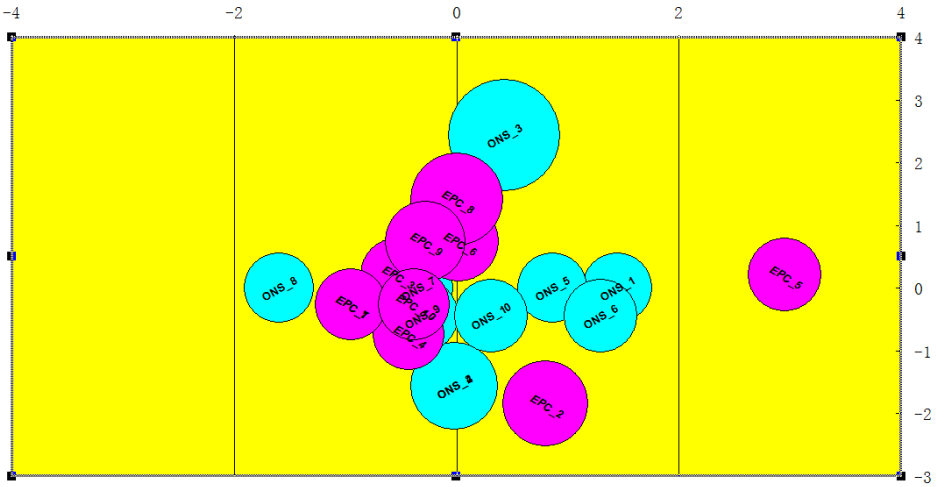

Figure 3. Bubble Figure of ONS and EPC.

The Logit values of ONS ability are on the left and the Logit value of EPC difficulty are on the right. The sorting of EPC difficulty is *EPC_8>EPC_9>EPC_6>EPC_5>EPC_3>EPC_7>EPC_10>EPC_1>EPC_4>EPC_2*. The sorting of ONS ability is *ONS_3>ONS_1>ONS_5>ONS_7>ONS_8>ONS_10>ONS_6>ONS_9>ONS_2>ONS_4*. ONS ability and EPC difficulty values are located in a graph with 8 Logit values intervals and follow normal distribution. For an ONS server near the point where the Logit value is 0, the probability of successful resolution is 50%. For an ONS server above 0, the probability of successful resolution is greater than 50%, and vice versa, less than 50%.

The project reflection probability curve is shown in Figure 5. According to the previous observations, the ONS ability and EPC difficulty are calculated. When the difference between the ONS ability and EPC difficulty is given, the probability of successful resolution can be estimated.

For example, when an ONS server's ability value is one Logit value lower than the difficulty value of an EPC, i.e. −1 point on the abscissa axis in Figure 8 above, it can be seen that the probability of failure resolution is about 75%, and the probability of successful resolution is about 25%.

From the analysis of the above results, it can be seen that Rasch model can calculate the

difficulty value of EPC and the capability value of ONS according to the previous analysis records, and then realize the probability of successful resolution in the future. The experimental results show that Rasch model is effective in the security of the IoT. According to the idea of Rasch model, as long as we find the corresponding relationship between individual ability value and the difficulty value of the topic, it can also be applied to other fields, such as trust mechanism field, education test field and so on.

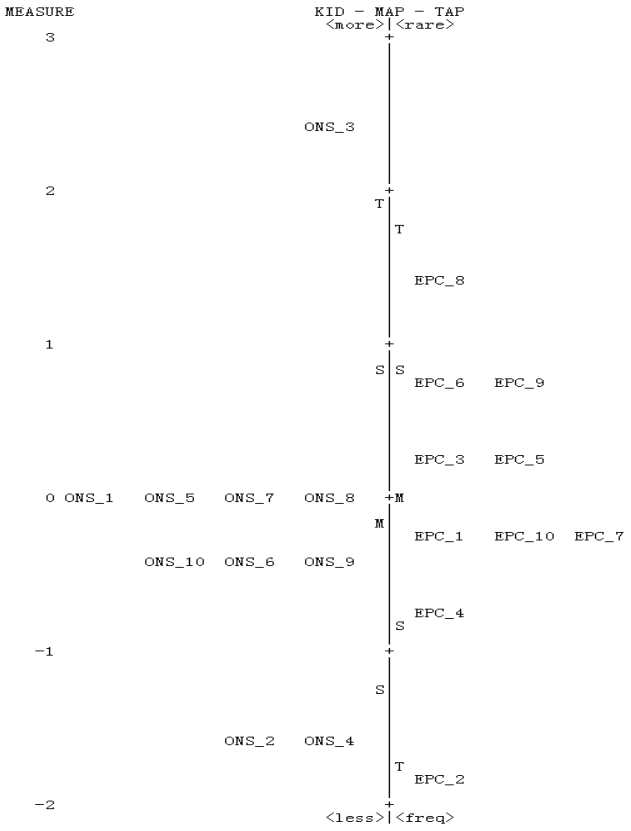

Figure 4. ONS Ability and EPC Difficulty Logit.

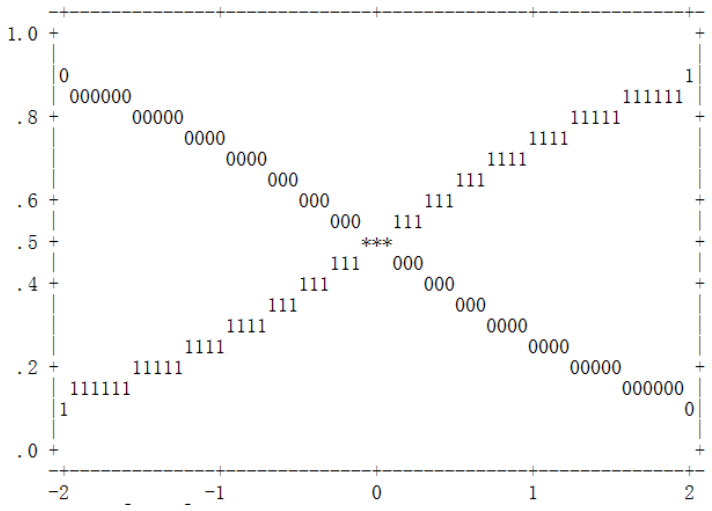

Figure 5. Project Reflection Probability Curve.

5. Conclusion

This paper studies the ONS resolution security technology. It is the first attempt to apply the famous Rasch model in psychology to ONS resolution security technology. According to the past resolution results, the probability of future successful resolution is predicted. The feasibility of the model is verified by simulation. Considering more factors in ONS resolution, establishing the relationship between EPC coding type, length, resolution frequency and difficulty value, and studying the application of multi-faceted Rasch model in IoT addressing security will be our next focus.

Acknowledgments

This research was supported by the National Natural Science Foundation of China under Grant (No. 61672299), the project of Nanjing University of Posts and Telecommunications (No.NY219119), National Engineering Laboratory for Logistics Information Technology, YuanTong Express co. LTD.

Conflict of interest

All authors declare no conflicts of interest in this paper.

References

1. L. Atzori, A. Iera, G. Morabito, The internet of things: A survey, *Comput. Netw.*, **54**(2010), 2787–2805.
2. C. Chang and C. Li, Algebraic secret sharing using privacy homomorphisms for IoT-based healthcare systems, *Math. Biosci. Eng.*, **16**(2019), 3367–3381.
3. C. Stergiou, K. E. Psannis, A. P. Plageras, et al., Algorithms for efficient digital media transmission over IoT and cloud networking, *J. Multi. Inf. Syst.*, **5**(2018), 27–34.
4. F. X. Yu, I-Japan strategy 2015, *Zhong guo Xinxihua*, **13**(2014), 13–23.
5. F. Gao, Z. Y. Zhao, K. X. Zhao, et al., Interpretation of the medium-term and long-term strategy of Korean ICT R&D (2013–2017), *Sci. Tech. Mgt. Res.*, **6**(2015), 30–34.
6. W. Ejaz, M. Naeem, A. Shahid, et al., Efficient energy management for the internet of thins in smart cities, *IEEE Commun. Mag.*, **55**(2017), 84–91.
7. C. M. Medaglia and A. Serbanati, An overview of privacy and security issues in the Internet of Things, Proceedings of the 20th Tyrrhenian Workshop on Digital Communications (Italy), *Springer*, (2010), 389–394.
8. Y. L. Liu, P. Hua and J. Wang, Verifiable diversity ranking search over encrypted outsourced data, *CMC-Comput. Mater. Con.*, **55**(2018), 037–057.
9. J. Wang, C. W. Ju, Y. Gao, et al., A PSO based energy efficient coverage control algorithm for wireless sensor networks, *CMC-Comput. Mater. Con.*, **56**(2018), 433–446.
10. Z. W. Li and Y. Xie, A security query protocol of ONS in EPC system, 2012 International Conference on Anti-Counterfeiting, Security and Identification (Taipei), *IEEE*, (2012), Article number: 6325293.

11. L. J. Zhang and Z. Q. Wu, A controllable trusted and anonymous query mechanism of Internet of Things, *Comput. Technol. Develop.*, **23**(2013), 122–125.
12. C. Fachkha, H. B. Elias and M. Debbabi, Fingerprinting internet DNS amplification DDoS Activities, 2014 6th International Conference on New Technologies, Mobility and Security (Dubai), *OALib J.*, (2014), article number: 6814019.
13. A. Friedlander, A. Mankin, W. D. Maughan, et al., DNSSEC: A protocol toward securing the Internet infrastructure, *Commu. ACM*, **50**(2007), 44–50.
14. M. Dempsky, DNSCurve: Link-Level Security for the Domain Name System, *Int. Draft*, 2004.
15. Z. Wu, Y. Zhou and J. Ma, A security transmission model for Internet of Things, *Chinese J. Comput.*, **34**(2011), 1351–1364.
16. W. Ren, L. Ma and Y. Ren, APP: An Ultralightweight scheme to authenticate ONS and protect epc privacy without cryptography in EPCglobal networks, *Int J. Distrib. Sens. N.*, (2013), Article ID: 784618.
17. P. Danielis, V. Altmann, J. Skodzik, et al., P-DONAS: A P2P-based domain name system in access networks, *ACM T. Int. Techn.*, **15**(2015), 1–11.
18. E. Zhang, X. T. Duan, S. M. Xiu, et al., Server-aided multi-secret sharing scheme for weak computational devices, *CMC-Comput. Mater. Con.*, **56**(2018), 401–414.
19. R. Georg, Probalilistic models for some intelligence and attainment tests, *Copenhagen: Institute of Education Research*, 1960.

AIMS Press