A Survey of Trusted Network Trust Evaluation Methods

An-Sheng Yin[1](✉) and Shun-Yi Zhang[2]

[1] Key Lab of Broadband Wireless Communication and Sensor
Network Technology, Nanjing University of Posts and Telecommunications,
Nanjing 210023, China
16629797@qq.com

[2] Department of Internet of Things,
Nanjing University of Posts and Telecommunications, Nanjing 210023, China

Abstract. The proposed trusted network is respond to the increasingly prominent internal network security threats. At present, research on trusted networks focuses on two aspects: pre-network access check and dynamic evaluation after access. The pre-access check considers the integrity of the terminal and uses encryption and authentication methods to achieve it. The dynamic evaluation uses the static and dynamic attributes of the trust to implement trust evaluation.

Keywords: Trusted network · Trust evaluation · Trust model

1 Introduction

With the rapid development of new technologies and services on the Internet, network and information security issues have become increasingly prominent. Most of the current information security threats come from within the network, and the attack methods present trends of intelligence, systematization, and integration. In order to make up the current decentralized, isolated, single defense, and externally attached network security system defects, the trusted network was proposed.

Trusted network studies the security threats within the network. The evaluation and control of internal entities on the network has become an important means for achieving network trust. Trusted network theory has also been widely used in fields such as IoT [1], MANETs [2], Cloud Computing [3], E-commerce [4], and Social Network [5].

The current network powers are racing to study trusted networks. The eID network trusted space construction scheme represented by South Korea and the European Union has been proved to be incomplete. The US government proposed the “trusted network space: Federal Network Space Security R & D Strategic Plan” in 2011 to give a roadmap for the development of trusted network, which requires an integrated approach to ensure the trust of cyberspace. China started earlier in the field of trusted computing. Teams represented by Zhang Huanguo and Feng Dengguo have achieved many successes in security chips, trusted security hosts, trusted computing platforms and applications. Lin Chuang conducted research on the trusted network architectures and prediction of user network behaviors.

J. Li et al. (Eds.): SPNCE 2019, LNICST 284, pp. 87–95, 2019.
https://doi.org/10.1007/978-3-030-21373-2_8

2 Trusted Network Connection

At present, research on trusted networks mainly focuses on two aspects: pre-network access check and dynamic evaluation.

In the stage of network access, the early research realized network trust through encryption and authentication mechanisms, and gradually developed into trusted network architecture based on trusted computing base, trusted chain, and trusted behavior analysis. There are Trusted Network Connect (TNC) architectures of Trusted Computing Group, Microsoft's Network Access Protection (NAP) architecture, and Cisco's Network Admission Control (NAC) architecture.

In terms of products, Huawei launched TSM (Terminal Security Management) solution; TOPSEC launched TNA (Trusted Network Access) access solution; Juniper developed TNC-compliant unified access control product "Juniper Networks Network Connect 8.0". These solutions or products are mainly used to implement system or device authentication, key negotiation, and establishment of trust connections.

The mainstream trusted access technologies that are generally accepted and widely studied at present are the TNC architecture and its basic technology TPM (Trusted Platform Module) module and the mobile terminal's trusted module MTM (Mobile Trusted Module). TNC implements trusted access based on integrity check. It will be one of the basic technologies for high-trusted networks because of its advantages, which will have a significant impact on next-generation information security solutions [6]. The current research on TNC focuses on the improvement of the TNC architecture and protocol, cross-domain authentication, session key agreement, IPSec SA, trusted certificate, two-way non-equivalent evaluation, trust chain transfer and other aspects [7–9].

The main function of the TNC architecture is to determine whether the terminal can access the corresponding network through the pre-access integrity and security check, and there is insufficient attention to the security measures after the access. Therefore, many researchers use the dynamic trust evaluation mechanism after access to achieve the terminal's full trust.

3 Trust Evaluation Model

In the field of dynamic trust evaluation, trusted network research lies in two aspects. One is applied to the Internet of Things, such as WSN, M2M, MANETs, IoV, etc. [1, 2]. The trust evaluation model achieved access control, secure routing, data forwarding, etc. under consideration of the energy consumption of the terminal, the computing capacity, the node mobility, and other issues [11, 12]. The other is used for inter-members interaction in social networks [5], commodities recommendation and consumers decision in e-commerce [4]. Device privacy and user privacy are also the focus of attention. Prasant has been paying attention to user privacy protection methods for reputation collection [13].

3.1 Dynamic Trust Evaluation Model

The dynamic trust evaluation models include behavior analysis model, multi-attribute decision model and reputation model.

The behavior analysis can be divided into equipment behavior analysis and user network behavior analysis. Device behavior analysis is used for identity authentication. Velten used touch screen interactions with smart devices to identify users by analyzing touch behaviors. Wesolowski combined keyboards, mice, and graphical user interfaces to increase the accuracy of authentication [15]. Peng et al. authenticate users more accurately by adding dynamic learning habits and preferences based on devices behavior identification [16].

Lin believes that trusted network should focus on the recording, evaluation, and prediction of online user behavior [17]. Tian proposed behavior-based terminal state analysis and trust decision criteria [18]. Meo combined the semantic analysis methods to determine the relationship between user behaviors and trust in social sharing networks [19]. Behavior analysis models are generally used to identify malicious behaviors [20], behavioral predictions [21], and so on. In the field of e-commerce, consumers recommendation can be made through users purchase behaviors [4].

The multi-attribute decision-making model carries out trust decisions by analyzing the attributes and attribute values that affect the user's trustworthy. The multidimensional trust decision attributes proposed by Li include direct trust, trust risk, feedback trust, incentive function, and entity activity [22]. Jameel et al. proposed a vector-based trust model in a pervasive environment. The model comprehensively considers attributes such as self-trust, historical trust, and time to reflect the dynamics of the trust relationship [23]. Liu selected the optimal trusted path based on the attributes such as interaction degree, interaction times, and self-importance [24]. Xiong selected the optimal trusted network component through multidimensional trusted evaluation index trees such as functional attributes, reliable attributes, security attributes, and aging attributes [25].

Trusted attributes include static attributes and dynamic attributes [26]. The static attribute evaluation mechanism implements the subjective trust evaluation of the trust evaluation subject based on the object's own attributes. The static attributes include the identity trust credentials and the inherent status information of the entity. The dynamic attribute evaluation mechanism implements the subjective trust evaluation of the trust evaluation subject for the object-related interactive behavior, and is related to the behaviors type, the bearer information, the number of successful interactive behaviors, and the subsequent influence.

Reputation model is one of the most widely used trust models. Since the beginning of this century, reputation mechanisms have been used to build trust models, such as TRUMMAR [27], EigenTrust [28], PeerTrust [29], and PowerTrust [30]. Josang often uses reputation models to calculate entity trust [31, 32]. Since the reputation value is derived from the recommendation and evaluation information among individuals, the reputation model is widely applied to P2P networks [28], Ad hoc networks, cloud platforms [33], e-commerce [34], and social networks.

In order to improve the performance of the trust model, the accuracy of reputation values can be improved by accumulating local knowledge [12], analyzing the relevance of the recommended values with Pearson correlation coefficient [33], or evaluating the volatility and consistency of the values [35].

Reputation model mostly uses graph theory to construct computational frameworks [36]. Du divides the model into multiple community structures [5], Yin divides the distributed system into several groups through group partitioning strategy [35]. Theodorakopoulos et al. calculated the shortest trusted path using semi-ring theory [37].

The reputation models study the assessment data collection and computation of network users, and is applied to multi-user interaction scenarios. The reputation model can be regarded as an extension of the behavior analysis model and the multi-attribute decision model. The behavior analysis model is used to analyze user interaction data to generate reputation values [33], and the multi-attribute decision model is used to distinguish multidimensional scenarios and applications and generate corresponding reputation values [34].

3.2 Trust Calculation Method

The trust evaluation model implements trusted network based on trust of the network entity. Trust is a measure of the mutual trust relationship in the network. It is similar to the trust relationship in human society and has the characteristics of timeliness, partial transitivity, ambiguity, and contextual relevance, anti-symmetry, composability, agglomeration, etc. [1, 38]. Referring to these attributes of trust, the algorithms used in the dynamic trust evaluation model include: discrete trust weighting algorithm, probability statistics methods, game theory algorithms, and fuzzy algorithms.

The discrete trust weighting algorithm comes from the composability and partial transitivity of trust, and the weight is divided into decision maker weight and attribute weight. The decision makers weight means that the evaluation subject weights include subjective, objective and combination weighting methods [39]. According to the sources of data, attribute weights are divided into subjective weighting method, objective weighting method and subjective and objective weighting method [40]. Discrete values and colloquial expression values are generally used to calculate discrete trust [41]. The discrete trust weighting algorithm is widely used because it is easy to calculate and understand. Meo uses the context and node depth information to determine the weight of the recommendation value [42]. In the current trust evaluation process, the trust of the user or terminal is calculated using the discrete trust model, dividing the trust level [23], setting the trust threshold [36], determine the trust strategy are become more and more common.

Discrete trust weighting model needs to divide trust grades, which will bring a new problem. If the grading is too broad, it may not get effective control effect. If the grading is too fine, it will cause the efficiency to decline. At the same time, performance distortion may occur at the boundary of the trust grades [43], which leads to the fact that the classification accuracy does not have a uniform distribution.

Because of the ambiguity of trust and the uncertainty of the trust relationship, it is reasonable to calculate the trust value based on probability and statistical methods. There are probability distribution models [44, 45], D-S evidence theory models [46], information entropy models [47, 48], and Bayesian models [31, 32, 49] and so on.

Ganeriwal [44] and Fang [45] build a trust model using beta distributions. Josang established the Bayesian trust model [31] and constructed a trust model using multiple evaluations based on the Dirichlet distribution [32]. Tian et al. proposed a P2P trust model based on recommendation evidence, and predicted node behavior through maximum likelihood estimation [46]. Wang enters the evaluation value of trust into the reverse cloud algorithm, converts the obtained expectation into trust, and reflects the uncertainty of trust through entropy and hyperentropy [47]. Ayday used the Bayesian network model to perform multi-conditional predictions based on the statistics of the previous behavior of the node, and made use of game theory to make decisions on trust results [49].

The game theory algorithm is used for trust decisions, it provides a tool to determine whether the terminal can interact with other terminals [52]. Sankaranarayanan proposed a trust-based game theory framework and algorithm [53]. Fallah used a multi-stage game strategy to solve terminal trust problems in mobile ad hoc networks [54]. Wu uses Stackelberg game to solve user trustworthiness in cognitive radio networks [55]. Yahyaoui uses the game theory model to improve the performance, robustness, and scalability of trusted services [56]. Pawlick proposed a games-of-game framework, which combines the advantages of FlipIt game and Signaling game to calculate the trust of the message [3].

Because of the fuzzy, dynamic, and complex nature of trust, fuzzy algorithms are also widely used in trust computing [46]. Fuzzy trust models rely on defining functions to reflect the degree of trust of nodes [57]. Damiani proposed a global method for calculating trust by summarizing fuzzy trust values [58]. Nepal transformed the user's opinion into fuzzy values and calculated the evaluation sequence accordingly [59].

More and more studies are now using uncertainty-based methods to calculate trust. For example, based on complex network and fuzzy decision analysis [60], cloud model [47], probability theory method [44], gray system theory [61], and group decision [62]. This is because trust is not only ambiguous, but also rough because the boundary of the confidence interval cannot be absolutely clear and causes the trust boundary to be indefinite or has an indiscernible relationship.

3.3 Further Discussion

Above Trust calculation methods always need to summarize trust data globally or locally. Due to the multi-source heterogeneity and mass characteristics of data, it is impossible to achieve real-time or quasi-real-time trust evaluation anyway. Real-time understanding of the state of internal entities is critical to achieving the trust of the network.

In order to achieve real-time or quasi-real-time evaluation of a trusted network, many considerations have been made from the perspective of reducing space complexity [63]. Ayday reduced the computational complexity of the edge function by means of factor graph and the Belief Propagation algorithm [49]. However, considering the continuous increase of data running with the network, this method cannot fundamentally solve the problem.

4 Conclusion

The security threats within the current network are becoming more and more prominent. The proposal of the trusted network is precisely to solve the security risks that appear within the network. Trusted network is achieved by calculating the trust of entities in the network. Behavior analysis model, multi-attribute decision model and reputation model provide a model framework for evaluation. Discrete trust weighting algorithms, probability statistics methods, game theory algorithms and fuzzy algorithms provide an algorithm framework for the calculation of trust.

The method of trust evaluation is quite mature. However, how to evaluate the security threats within the network in a timely and effective manner is an urgent problem to be solved. There is no effective solution at present, so we need to focus on and study.

References

1. Sicari, S., Rizzardi, A., Grieco, L.A., et al.: Security, privacy and trust in Internet of Things. Comput. Netw. Int. J. Comput. Telecommun. Netw. **76**(C), 146–164 (2015)
2. Cho, J.H., Swami, A., Chen, I.R.: A survey on trust management for mobile ad hoc networks. IEEE Commun. Surv. Tutorials **13**(4), 562–583 (2011)
3. Pawlick, J., Zhu, Q.: Strategic trust in cloud-enabled cyber-physical systems with an application to glucose control. IEEE Trans. Inf. Forensics Secur. **12**(12), 2906–2919 (2017)
4. Dan, J.K., Ferrin, D.L., Rao, H.R.: A trust-based consumer decision-making model in electronic commerce: the role of trust, perceived risk, and their antecedents. Decis. Support Syst. **44**(2), 544–564 (2008)
5. Du, J., Jiang, C., Chen, K.C., et al.: Community-structured evolutionary game for privacy protection in social networks. IEEE Trans. Inf. Forensics Secur. **13**(3), 574–589 (2018)
6. Sailer, R., Zhang, X., Jaeger, T., et al.: Design and implementation of a TCG-based integrity measurement architecture. In: Proceedings of the 13th USENIX Security Symposium, San Diego, CA, USA (2004)
7. Ma, J.-F., Li, X.-H., Jiang, Q.: Provable security model for trusted network connect protocol. Chin. J
8. Wei, D., Jia, X.-p., Wang, J., Liu, Y.-s.: New access model and implementation of trusted network based on trusted certificate. J. Jilin Univ. **40**(2), 496–500 (2010)
9. Qin, X., Chang, C.-w., He, R.-y.: Novel trusted network access architecture ETNA. J. Chin. Comput. Syst. **32**(8), 1493–1498 (2011)
10. Govindan, K., Mohapatra, P.: Trust computations and trust dynamics in mobile adhoc networks: a survey. IEEE Commun. Surv. Tutorials **14**(2), 279–298 (2012)
11. Vamsi, P.R., Kant, K.: Performance analysis of trust based geographic routing protocols for Wireless Sensor Networks. In: International Conference on Parallel, Distributed and Grid Computing, pp. 318–323. IEEE (2015)
12. Movahedi, Z., Hosseini, Z.: A green trust-distortion resistant trust management scheme on mobile ad hoc networks. Wireless Pers. Commun. 1–17 (2016)
13. Wang, X.L., Cheng, W., Mohapatra, P., Abdelzaher, T.: Enabling reputation and trust in privacy-preserving mobile sensing. IEEE Trans. Mob. Comput. **13**(12), 2777–2790 (2014)

14. Velten, M., Schneider, P., Wessel, S., Eckert, C.: User identity verification based on touchscreen interaction analysis in web contexts. In: Lopez, J., Wu, Y. (eds.) ISPEC 2015. LNCS, vol. 9065, pp. 268–282. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-17533-1_19
15. Wesolowski, T., Kudlacik, P.: User profiling based on multiple aspects of activity in a computer system. J. Med. Inform. Technol. **11**(6), 121–130 (2014)
16. Peng, J., Gao, N.: Research on identity trusted level evaluation mechanism based on user behavior analysis. Netinfo Secur. **9**, 124–129 (2016)
17. Lin, C., Tian, L., Wang, Y.: Research on user behavior trust in trustworthy network. J. Comput. Res. Dev. **45**(12), 2033–2043 (2008)
18. Tian, J., Liu, Y., Du, R.: Trust evaluation model based node behavior character. Inf. Int. Interdisc. J. **14**(10), 3351–3371 (2011)
19. Meo, P.D., Ferrara, E., Abel, F., et al.: Analyzing user behavior across social sharing environments. ACM Trans. Intell. Syst. Technol. **5**(1), 1–31 (2013)
20. Jung, J.J.: Trustworthy knowledge diffusion model based on risk discovery on peer-to-peer networks. Expert Syst. Appl. **36**(3), 7123–7128 (2009)
21. Liu, C., Fan, M., Wang, G.: Unsupervised behavior evaluation method in trustworthy network. In: 2010 Second International Workshop on Education Technology and Computer Science, vol. 24, no. 3, pp. 78–82 (2010)
22. Li, X.-Y., Gui, X.-L.: Trust quantitative model with multiple decision factors in trusted network. Chin. J. Comput. **32**(3), 405–416 (2009)
23. Jameel, H., Hung, L.X., Kalim, U., et al.: A trust model for ubiquitous systems based on vectors of trust values. In: Proceedings of the 7th IEEE International Symposium on Multimedia, pp. 674–679. IEEE Computer Society, Washington, D.C. (2005)
24. Liu, G., Wang, Y., Orgun, M.A.: Finding the optimal social trust path for the selection of trustworthy service providers in complex social networks. IEEE Trans. Serv. Comput. **6**(2), 152–167 (2013)
25. Xiong, G., Lan, J.-l., Hu, Y.-x., Liu, S.-r.: Evaluation approach for network components performance using trustworthiness measurement. J. Commun. **37**(3), 117–127 (2016)
26. Huang, C.: The study of dynamic trust relationship modeling and managing. National University of Defense Technology, Hunan (2005)
27. Derbas, G., et al.: TRUMMAR: a trust model for mobile agent systems based on reputation. In: IEEE/ACS International Conference, pp. 113–120 (2004)
28. Kamvar, S.D., Schlosser, M.T., Garcia-Molina, H.: The Eigentrust algorithm for reputation management in P2P networks. In: International Conference on World Wide Web, pp. 640–651. ACM (2003)
29. Xiong, L., Liu, L.: PeerTrust: supporting reputation-based trust for peer-to-peer electronic communities. IEEE Trans. Knowl. Data Eng. **16**(7), 843–857 (2004)
30. Zhou, R., Kai, H.: PowerTrust: a robust and scalable reputation system for trusted peer-to-peer computing. IEEE Trans. Parallel Distrib. Syst. **18**(4), 460–473 (2007)
31. Jøsang, A., Quattrociocchi, W.: Advanced features in Bayesian reputation systems. In: Fischer-Hübner, S., Lambrinoudakis, C., Pernul, G. (eds.) TrustBus 2009. LNCS, vol. 5695, pp. 105–114. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-03748-1_11
32. Josang, A., Haller, J.: Dirichlet reputation systems. In: Werner Beds. Proceedings of 2nd International Conference on Availability, Reliability and Security Vienna, Los Vaqueros, pp. 112–119. IEEE Computer Society (2007)
33. Coles, M., Kioussis, D., Veiga, H.: Reputation measurement and malicious feedback rating prevention in web service recommendation systems. IEEE Trans. Serv. Comput. **8**(5), 755–767 (2015)

34. Tadelis, S.: The economics of reputation and feedback systems in e-commerce marketplaces. IEEE Internet Comput. **20**(1), 12–19 (2016)
35. Yin, A., Zhang, S.: A trust model based on volatility and consistency in trusted groups. J. Nanjing Univ. Posts Telecommun. (Nat. Sci.) **34**(3), 101–106 (2014)
36. Jiang, L., Zhang, K., Jian, X., et al.: A new evidential trust model based on graph theory for open computing systems. J. Comput. Res. Dev. **50**(5), 921–931 (2013)
37. Theodorakopoulos, G., Baras, J.S.: Trust evaluation in ad-hoc networks. In: Proceedings of the 3rd ACM Workshop on Wireless Security, pp. 1–10. ACM (2004)
38. Zhang, H.-G., Chen, L., Zhang, L.-Q.: Research on trusted network connection. Chin. J. Comput. **33**(4), 706–717 (2010)
39. Yue, Z.: An extended TOPSIS for determining weights of decision makers with interval numbers. Knowl.-Based Syst. **24**(1), 146–153 (2011)
40. Huang, D., Wu, Z., Zong, Y.: An impersonal multi-attribute weight allocation method based on attribute importance. Syst. Eng.-Theory Methodol. Appl. **13**(3), 201–207 (2004)
41. Carbone, M., Nielsen, M., Sassone, V.: A formal model for trust in dynamic networks. In: Proceedings of the International Conference on Software Engineering and Formal Methods, pp. 54–61. IEEE (2003)
42. Meo, P.D., Nocera, A., Quattrone, G., et al.: Finding reliable users and social networks in a social internetworking system. In: International Database Engineering and Applications Symposium, pp. 173–181 (2009)
43. Guo, Z.-q., Wang, Q., Wan, Y.-d., et al.: A classification prediction mechanism based on comprehensive assessment for wireless link quality. J. Comput. Res. Dev. **50**(6), 1227–1238 (2013)
44. Ganeriwal, S., Balzano, L.K., Srivastava, M.B.: Reputation-based framework for high integrity sensor networks. ACM Trans. Sens. Netw. (TOSN) **4**(3), 66–77 (2008)
45. Fang, W., Zhang, C., Shi, Z., et al.: BTRES: beta-based trust and reputation evaluation system for wireless sensor networks. J. Netw. Comput. Appl. **59**, 88–94 (2016)
46. Tian, C., Yang, B.: A D-S evidence theory based fuzzy trust model in file-sharing P2P networks. Peer-to-Peer Netw. Appl. **7**(4), 332–345 (2014)
47. Wang, S., Zhang, L., Li, H.: Evaluation approach of subjective trust based on cloud model. J. Softw. **21**(6), 1341–1352 (2010)
48. Sun, Y., Yu, W., Han, Z., et al.: Trust modeling and evaluation in ad hoc networks. In: Global Telecommunications Conference, GLOBECOM 2005, vol. 3, pp. 1862–1867. IEEE (2005)
49. Ayday, E., Fekri, F.: Iterative trust and reputation management using belief propagation. IEEE Trans. Dependable Secure Comput. **9**(3), 375–386 (2012)
50. Liang, H.-q., Wu, W.: Research of trust evaluation model based on dynamic Bayesian network. J. Commun. **34**(9), 68–76 (2013)
51. Hu, H., Chen, Y., Su, Z.: Weighted trust evaluation-based malicious node detection for wireless sensor networks. Int. J. Inf. Comput. Secur. **3**(2), 132–149 (2009)
52. Guo, J.-j., Ma, J.-f., Li, Q., Wan, T., Gao, C., Zhang, L.: Game theory based trust management method for mobile ad hoc networks. J. Commun. **35**(11), 50–58 (2014)
53. Sankaranarayanan, V., Chandrasekaran, M., Upadhyaya, S.: Towards modeling trust based decisions: a game theoretic approach. In: Biskup, J., López, J. (eds.) ESORICS 2007. LNCS, vol. 4734, pp. 485–500. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-74835-9_32
54. Fallah, M.S., Mouzarani, M.: A Game-Based Sybil-Resistant Strategy for Reputation Systems in Self-organizing MANETs. Oxford University Press, Oxford (2011)

55. Wu, Y., Liu, K.J.R.: An information secrecy game in cognitive radio networks. IEEE Trans. Inf. Forensics Secur. **6**(3), 831–842 (2011)
56. Yahyaoui, H.: A trust-based game theoretical model for Web services collaboration. Knowl.-Based Syst. **27**(3), 162–169 (2012)
57. Nefti, S., Meziane, F., Kasiran, K.: A fuzzy trust model for e-commerce. In: IEEE International Conference on E-Commerce Technology, pp. 401–404. IEEE (2005)
58. Damiani, E., Vimercati, S.D.C.D., Samarati, P., et al.: A WOWA-based aggregation technique on trust values connected to metadata. Electron. Notes Theor. Comput. Sci. **157** (3), 131–142 (2006)
59. Nepal, S., Sherchan, W., Bouguettaya, A.: A behaviour-based trust model for service web. In: IEEE International Conference on Service-Oriented Computing and Applications, pp. 1–4. IEEE (2010)
60. Ma, J.-y., Zhao, Z.-j., Ye, X.-y.: User behavior assessment in trusted network based on fuzzy decision analysis. Comput. Eng. **37**(13), 125–131 (2011)
61. Zhao, T.-z., Yang, Q.-h., Mei, D.-h.: Trust model for P2P network based on fuzzy set and grey relation. Comput. Eng. **35**(6), 173–175 (2009)
62. Cha, B.R., Sun, P., Kim, J.W.: A fake content remove scheme using binomial distribution characteristics of collective intelligence in peer-to-peer environment. IETE J. Res. **57**(5), 423–429 (2011)
63. Veltri, L., Cirani, S., Busanelli, S., et al.: A novel batch-based group key management protocol applied to the Internet of Things. Ad Hoc Netw. **11**(8), 2724–2737 (2013)