Saudi Journal of Biological Sciences 25 (2018) 237–241

Contents lists available at ScienceDirect

Saudi Journal of Biological Sciences

journal homepage: www.sciencedirect.com

Original article

A security mechanism based on evolutionary game in fog computing

Yan Sun, Fuhong Lin *, Nan Zhang

School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing 100083, PR China

ARTICLE INFO

Article history:
Received 1 August 2017
Revised 25 September 2017
Accepted 27 September 2017
Available online 29 September 2017

Keywords:
Fog computing
Human nervous system
Security mechanism
Evolutionary game

ABSTRACT

Fog computing is a distributed computing paradigm at the edge of the network and requires cooperation of users and sharing of resources. When users in fog computing open their resources, their devices are easily intercepted and attacked because they are accessed through wireless network and present an extensive geographical distribution. In this study, a credible third party was introduced to supervise the behavior of users and protect the security of user cooperation. A fog computing security mechanism based on human nervous system is proposed, and the strategy for a stable system evolution is calculated. The MATLAB simulation results show that the proposed mechanism can reduce the number of attack behaviors effectively and stimulate users to cooperate in application tasks positively.

1. Introduction

Fog computing is a computing paradigm between the terminal device and the cloud data center without the involvement of a third party (Bonomi et al., 2012; Yaacof et al., 2017). This paradigm executes storage and processing tasks through cooperation of users and sharing of resources among considerable scattered heterogeneous devices. Fog computing highly depends on the cooperation of users. Notably, the stability and security of cooperation are difficult to protect owing to the subjectivity of users.

Cloud computing contains many solutions to the problem of network safety. However, these solutions may be unsuitable to fog computing. Compared with cloud computing, fog computing is closer to users and more distributed because of the fog devices working at the edge of the network. The work environment of fog devices faces threats that are non-existent in a well-managed cloud (Stojmenovic and Wen, 2014; Maz et al., 2017).

When users in the fog computing open their resources, nodes in the network are easily attacked and captured as interior malicious nodes; consequently, attacks to the network are launched, such as man-in-the-middle attack and denial of service attack (Cai et al., 2014; Xuana et al., 2017). Attacks from interior malicious nodes are more difficult to prevent than those from external nodes because a few traditional secret key mechanisms become invalid during such events. Hence, the attack behavior of interior malicious nodes affects the network performance seriously and cause paralysis of the entire network. Therefore, the way to effectively protect the security and trust of cooperative users and prevent the attack behavior of interior malicious nodes must be determined (Vaquero and Rodero-Merino, 2014). The performance and security of the fog computing network must also be enhanced.

Fog computing requires mutual trust and resource sharing of different devices. However, the open resource environment provides malicious node opportunities of attack behavior. Based on current fog computing mode, in 2014, Stojmenovic et al. (Stojmenovic and Wen, 2014) further disclosed the problems of security and privacy. They studied a typical attack behavior, namely, man-in-the-middle attack, to discuss the security problem of fog computing. They also investigated the invisible features of such attack behavior by examining the CPU and memory consumption on fog devices. Nevertheless, the authors only proved the imperceptibility of man-in-the-middle attack and did not propose a specific solution to such attack. In 2015, Dong et al. (Dong et al., 2015; Zhenga et al., 2017) proposed a redundancy fog loop program to protect the privacy of local resources, optimize energy utilization, and maximize the security and service life of network. Each fog establishes multiple pseudo-data packages to the source node and provides privacy to the local resources. Through dynamics establishment and cancellation of fog enhanced security, this program increases more than five times of energy efficiency and improves network security to the maximum extent while maintaining the same service life of wireless network. In 2014, Dsouza et al. (Dsouza et al., 2014) proposed the security mechanism of

* Corresponding author.
E-mail addresses: com2017sy@163.com (Y. Sun), td2016lfh@sina.com (F. Lin).

Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

https://doi.org/10.1016/j.sjbs.2017.09.010
1319-562X/

fog computing based on a strategy and expanded the existing fog computing platform to support safe coordination and interoperability among resources upon the requests of different users. However, this mechanism cannot detect policy conflicts and corresponding solutions. Zhang et al. (Zhang et al., 2010) inserted malicious codes into the system and found that man-in-the-middle attack only consumes few resources of fog devices. Considering the existence of abundant fog nodes, the router in fog must be protected. A few scholars have conducted open studies on solutions to the special safety problems of fog computing. On the basis of a comprehensive conclusion of the advantages of fog computing and comparing its special features to cloud computing, in 2015, Wang et al. (Wang et al., 2015) in College of Information Science & Engineering Ritsumeikan University Kusatsu-shi, Shiga, Japan proposed and discussed new problems and challenges of fog security and fog evidence collection. Their research results have encouraged and promoted extensive studies in this field. Lee et al. (Lee et al., 2015; Xu, 2017) believed that the fog itself introduces special security threats. They discussed the concept of Internet of Things (IOT) of fog and existing security measures and established a safe fog computing environment by analyzing correlated security technology. However, they did not formulate specific safety strategies to reduce these attacks and threats.

The idea of evolutionary game in economics can be used to study the security mechanism of fog computing. In 2009, Niyato D et al. (Niyato and Hossain, 2009) in School of Computer Engineering, Nanyang Technological University, Singapore discussed the network selection problem of heterogeneous wireless network by evolutionary game and concluded from evolution dynamics that the evolutionary equilibrium point is the optimal network selection program. In 2010, Ternbine et al. (Bonomi, 2011) studied multiple signal pathways and energy control problems using evolutionary game.

To address the special security problem under the fog environment, a security mechanism based on evolutionary game was designed in this study. A credible third party dynamic penalty strategy was introduced to make the attack cost of malicious users higher than the profits, thereby forcing them to stop their attack behavior.

The main contributions of the study are summarized as follows:

(1) A fog computing security mechanism is established on the basis of the characteristics of the human nervous system. A credible third party is introduced to adjust the distribution bandwidth of users and constrain the behavior of users.
(2) This security mechanism is analyzed by an evolutionary game model, and the behavioral strategy selection of participants is depicted by a replicator dynamics equation. The convergence direction of dynamics is described by an evolutionary stability strategy, and the effects of different penalty conditions on user behavior are discussed.

The rest of the paper is organized as follows. Section 2 establishes a security mechanism under the fog environment by analyzing the characteristics of the human nervous system. Then this mechanism is introduced thoroughly with an evolutionary game. Section 3 conducts a simulation analysis on the validity of this mechanism. Our conclusions are presented, and future research directions are proposed in Section 4.

2. Material and methods

2.1. Security mechanism in fog computing

Fog computing requires mutual trust and resource sharing of different devices. The open resource environment provides malicious nodes with the opportunity to attack. Such open and integrated computing mode increases the concern of users on the security of their devices and arouses the security consciousness of users continuously. However, users cannot understand the device security of other users because of the information asymmetry among different users. A credible third party is thus necessary to supervise and record the behavior of the user.

Preventing the attack behavior of malicious nodes is difficult because of the mobility and extensive geological distribution of fog nodes (Bonomi, 2011). On the basis of the future IOT structure similar to the human nervous system (Ning and Wang, 2011), a distributed credible third party is introduced in the present study for supervising and punishing the user. A security mechanism under the fog environment is established as shown in Fig. 1.

In the human body, spinal cord is an important component of the nervous system and its activity is controlled by the brain. Various feelings and impulsions from the arms and legs and the body pass through the ascending fiber bundle of the spinal cord. These conduction pathways transmit these feelings and impulsions to the brain for advanced comprehensive analysis. Brain activities pass through the descending fiber bundle of the spinal cord to adjust the activities of spinal cord neurons. If all activities must be processed by the brain, the brain will be exhausted. Numerous low-level reflex centers notably exist in the gray substance of the spinal cord, and they can accomplish a few basic reflex activities.

The designed security mechanism for fog computing comprises a cloud data center, a fog computing data center, and distributed intelligent devices. The cloud data center corresponds to the brain nerve center in the nervous system, which adjusts the deployment of the entire security mechanism. The fog data center can be used as the credible third party and is equivalent to the nerve center of spinal nerves. The fog data center can supervise the behavior of the user in real time and provide certain bandwidth penalty to malicious users. Moreover, the fog data center contains information about the credibility of the user and can accept verification requests from the user end and feed back the credibility of desired devices. Similar to the activity of the spinal cord controlled by the

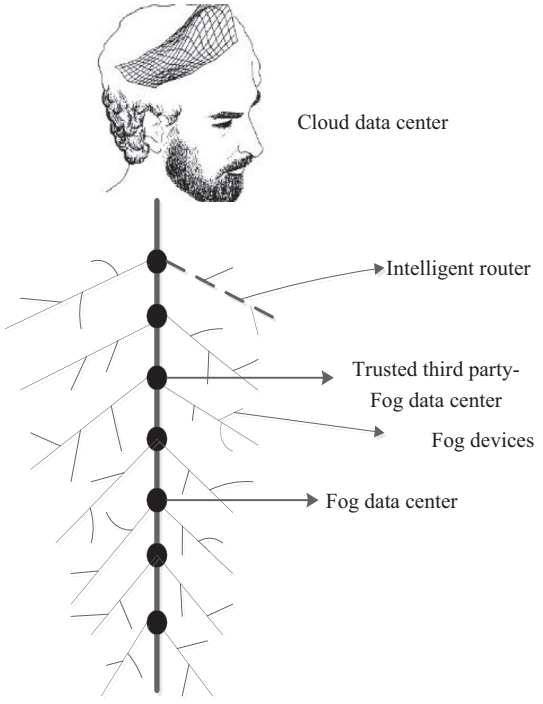

Fig. 1. Security mechanism in fog computing.

brain, the fog data center is also controlled by the cloud data center. The extensive distribution of various fog devices is similar to the two-way excitation conduction of nerve fibers. These devices request services from the data center and other users. In the present study, the fog devices include terminal user devices, access points, an edge router, and an exchanger.

If all verification requests must be processed by the brain, then the brain will be exhausted. Notably, a few unconditioned reflexes, such as knee-jerk reflex, are processed by the spinal cord. In the proposed security mechanism, the fog computing center will process certain simple and time-sensitive security problems and share the pressure of the cloud data center; such arrangement avoids delayed feedback of device credibility and poor cooperation security caused by large security data size in the cloud end.

The spinal cord is the pathway between the peripheral nerves and the brain. The fog data center, that is, the credible third party, similarly serves as the bridge between the user end and the cloud data center.

2.2. Evolutionary game model description

2.2.1. System modeling

A security mechanism for fog computing based on the characteristics of the human nervous system was established. In the following part, a mathematical analysis of the security mechanism is conducted by an evolutionary game. The necessary basic knowledge of the evolutionary game theory is introduced first.

Under the premise of the limited rationality of the assumed game subject, the evolutionary game investigated the system equilibrium by the analytical method and predicted group behavior of players using the evolutionary stability equilibrium.

Theorem 1 Evolutionary Stable Strategy (ESS). *The evolutionary stability strategy means that no mutation strategy will attack the group under the effect of natural selection if all members in the group adopt this strategy* (Weibull, 1997; Smith, 1974).

If $\forall y \in S$, $y \neq x$ has a $\bar{\varepsilon}_y \in (0,1)$ that makes the inequality $u[x, sy + (1-s)x] > u[y, sy + (1-s)x]$ true to any $\varepsilon \in (0, \bar{\varepsilon}_y)$, then $x \in A$ is an evolutionary stability strategy.where S is the strategy set of individual games in the group; y is the mutation strategy; $\bar{\varepsilon}_y$ is a constant related with y; $sy + (1-s)x$ is the mixed system composed of the group choosing evolutionary stability strategy and the group choosing mutation strategy.

Theorem 2 Replicator Dynamics. *Replicator dynamics is a certainty and non-linearity evolutionary game model based on selection mechanism. The basic principle of replicator dynamics is that, in a group of players with limited rationality, the strategies better than the average level will be preferred by most players gradually and a few players who use different strategies will change accordingly* (Mejia et al., 2011; Smith and Price, 1973).

The numbers of players who choose the strategy s and s′ at t according to certain programming are denoted as n_t and n'_t, respectively. The total number of players is N_t, $u_t(s)$ is its profit function, and S is the strategy set:

$$\dot{n}_t(s) = n_t u_t(s) \tag{1}$$

Let $x_t(s)$ be the proportion of n_t in N_t:

$$x_t(s) = \frac{n_t}{N_t} \tag{2}$$

The expected payoff of players who plan to choose the strategy s is:

$$u_t(s) = x_t(s)u_t(s,s) + x_t(s')u_t(s,s') \tag{3}$$

In this way, the average payoff of all players is:

$$\bar{u}_t(s) = x_t(s)u_t(s) + x_t(s')u_t(s') \tag{4}$$

Substituting Eqs. (2), (4) into Eq. (1) yields:

$$\frac{dx_i}{dt} = F(x_i) = [u(s_i, x) - \bar{u}(x, x)]x_i \tag{5}$$

where $u(s_i, x)$ is the expected profits of the individuals choosing the pure strategy s_i during random anonymous games and $\bar{u}(x,x) = \sum_i^x u(s_i, x)$ is the average expected profits of the group. Then the security model based on the evolutionary game was established.

In this study, users with fog device in the network are viewed as a population and all user individuals in the fog are individuals of this population. Users are mutually independent and equal. They make different behavioral decisions on the basis of information exchange and practical situations. In this population, different proportions of groups select specific actions and users who choose different actions are abstracted to different "types" of players. "Types" change with the strategy of players. Individuals selecting specific actions create random pairs and form participant combinations, that is, matching of different strategies. The definitions involved in this model are introduced as follows.

Definition 1 Players. In fog computing, players are divided into two populations: the population composed of normal nodes and the population composed of malicious nodes. The behavior of normal nodes does not threaten the network, but the behavior of malicious nodes will threaten the network security significantly. Both populations are unfamiliar with acceptances and responses of the system, which presents limited rationality.

Definition 2 Strategy. The population composed of normal nodes is supposed to have two strategies: cooperation and noncooperation. The strategy space is recorded as $S_A = (C, N)$. The proportions of groups choosing different strategies are x and $1 - x$, respectively. The population composed of malicious nodes is supposed to have two strategies: non-attack and attack. The strategy space is denoted as $S_B = (U, A)$. The proportions of groups choosing different strategies are y and $1 - y$.

Definition 3 Consumption cost of normal nodes. θ is the consumption cost under the cooperation of normal nodes, and β is the consumption cost under the attack behavior of normal nodes.

Definition 4 Profits from the attack behavior of malicious users. η is the profit from the attack to the cooperation users and υ is the profit from the attack to the non-cooperation users.

In the network, bandwidth is important to users. For example, multimedia online service and the application services of MapReduce will produce tremendous data communication, which requires large bandwidths to the core layer, convergence layer, and access layer in the entire data center network. Therefore, the fog data center will provide users who contribute resources positively with certain rewards of bandwidth but punish malicious nodes with limited or closed bandwidth. Users with large bandwidth possess high information transmission capacity and can use application services conveniently, thereby gaining certain time cost profits. On the contrary, users with limited bandwidth will have delayed access to services, thereby increasing time cost and leading to certain time loss. Therefore, the following hypothesis was made:

Suppose1 bandwidth profits

R is the time incremental profits of normal nodes which are attributed to rewarded bandwidth, and Q is the time cost of malicious nodes which is caused by the punishment of limited bandwidth when the fog data center discovers attack behavior. p is the probability that the attack behavior of malicious node will be discovered by the credible third party.

Based on the definitions and hypothesis mentioned above, the payoff matrixes of normal and malicious nodes with the existence of a credible third party are shown in Table 1.

The profits of the cooperation normal nodes are:

$$u_1 = y(R-\theta) + (1-y)(R-\theta-\beta) = R-\theta-\beta+y\beta \tag{6}$$

Users who refuse to cooperate and open their resources will be neither rewarded nor attacked, and they will not incur cooperation loss. Therefore, the profits of non-cooperation normal nodes are:

$$u_2 = 0 \tag{7}$$

The average profits of the normal node population are:

$$\bar{U}_j = x(R-\theta-\beta+y\beta) \tag{8}$$

The replicator dynamics equation of the population is:

$$\frac{dx}{dt} = x(u_1-\bar{u}_j) = x(1-x)(R-\theta-\beta+y\beta) \tag{9}$$

The profits of the non-attacking malicious nodes are:

$$u_3 = 0 \tag{10}$$

The attack nodes encounter difficulty in gaining profits when users refuse to cooperate. Hence, the profits of attacking malicious nodes are:

$$u_4 = x[(1-p)\eta - pQ] + (1-x)(-pQ) = x(1-p)\eta - pQ \tag{11}$$

The average profits of the malicious node population are:

$$\bar{u_k} = (1-y)[x(1-p)\eta - pQ] \tag{12}$$

The replicator dynamics equation of the population is:

$$\frac{dy}{dt} = y(u_3-\overline{u_k}) = y(y-1)[x(1-p)\eta - pQ] \tag{13}$$

If Eq. (9) = 0, then $x = 0$ or 1. However, two players cannot find an evolutionary stability strategy quickly because $R-\theta-\beta+y\ \beta$ is uncertain. Thus, the value ranges of different parameters must be analyzed to determine the final evolutionary stability strategy. Similarly, if Eq. (13) = 0, then $y = 0$ or 1. Given that $x(1-p)\eta - pQ$ is also uncertain, the value ranges of different parameters must be analyzed to determine the final evolutionary stability strategy.

2.2.2. Stability analysis

The best situation for the overall network system is that malicious nodes adopt the "non-attack" strategy while normal nodes use the "cooperation" strategy. In other words, the system will converge to the state (1, 1) to save energy and storage space and increase the system security effectively, thereby maximizing the system profits.

The best situation for users is to cooperate to open their resources; however, the attackers must stop their attack behavior, that is, $x = 1 y = 1$.

Table 1
Payoff matrix of players.

Normal node|malicious node	Non-attack	Attack
Cooperation	$R-\theta$, 0	$R-\theta-\beta$, $(1-p)\eta - pQ$
Non-cooperation	0, 0	0, $(1-p)v - pQ$

According to Eqs. (9) and (13), the corresponding Jacobian matrix is concluded as:

$$J = \begin{bmatrix} (1-2x)(R-\theta-\beta+y\beta) & x(1-x)\beta \\ y(y-1)(1-p)\eta & (2y-1)[x(1-p)\eta - pQ] \end{bmatrix} \tag{14}$$

Bringing $x = 1 y = 1$ to the matrix yields:

$$J = \begin{bmatrix} -(R-\theta) & 0 \\ 0 & [(1-p)\eta - pQ] \end{bmatrix} \tag{15}$$

The path of the matrix is $trJ = -(R-\theta) + [(1-p)\eta - pQ]$ and the value of the Jacobian determinant is $detJ = -(R-\theta) * [(1-p)\eta - pQ]$.

If $x = 1 y = 1$ is locally stable, then the equilibrium point is the evolutionary stability strategy of the system. Thereafter, it needs:

$$\begin{cases} trJ < 0 \\ detJ > 0 \end{cases} \tag{16}$$

Therefore,

$$R > \theta Q > \eta\left(\frac{1}{p} - 1\right) \tag{17}$$

3. Results and discussion

In this study, a MATLAB simulation test was carried out. Considering the different measurement standards of the parameters, all research parameters were normalized by Eq. (18).

$$m_{standardization} = \frac{m_i - m_{min}}{m_{max} - m_{min}} \tag{18}$$

First, whether the existence of a credible third party can reduce the number of the attack behavior effectively was verified. If $R = 0.6$, $\theta = 0.4$,$p = 0.8$, $\eta = 0.3$, then $Q > 0.075$. If $Q = 0.1$, then $x = 0.5$, $y = 0.3$.

As shown in Fig. 2, when the penalty strategy of the credible third party satisfies Eq. (17), normal nodes will choose to cooperate to gain bandwidth rewards. Although malicious nodes choose the attack strategy, they will stop the attack behavior to maximize their own benefits when they receive evolutionary learning for a certain time. They will also recognize bandwidth limits from the fog data center for their attack behavior. Finally, the network will converge to the state of (cooperation, non-attack).

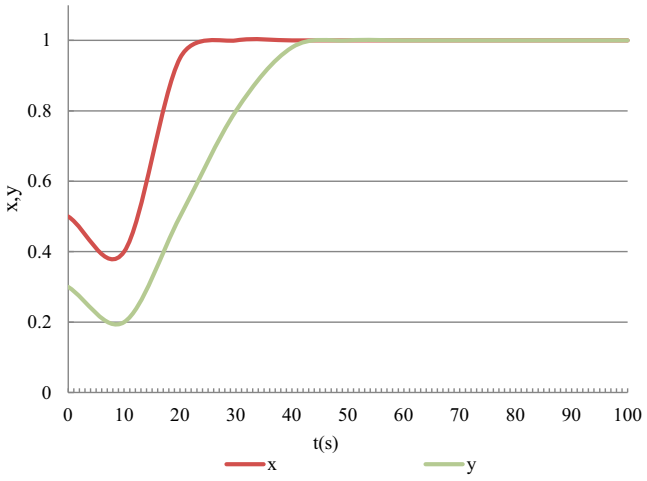

Fig. 2. ESS analysis of the system under supervision of a credible third party.

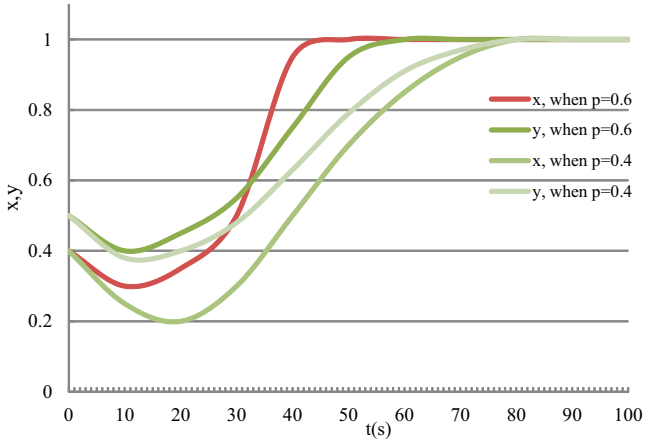

Fig. 3. ESS analysis of the system under different values of p.

A simulation analysis was conducted to verify the influences of p ($p = 0.4$ and $p = 0.6$) on the speed for the system to reach ESS. The results in Fig. 3 shows that p can influence the speed for the system to reach ESS. High p results in short time to reach ESS. This result conforms to practical environment and is due to that, given high p, malicious nodes concern mostly on time cost caused by bandwidth limitation and malicious nodes will choose to stop their attack behavior. Normal nodes are less likely to be attacked owing to the security guarantee of the credible third party, and many users will choose to cooperate to gain bandwidth rewards. This phenomenon shortens the time for the system to reach ESS.

4. Conclusions

The rapid development of fog computing has increased the attention to security problems caused by cooperation of users and sharing of resources among devices. In this study, a cooperation security mechanism based on the reflex activities of the human nervous system was proposed for fog computing by introducing a credible third party. Mathematical modeling and analysis were performed using evolutionary game theory. Meanwhile, an MATLAB simulation test of the effect of the dynamics game evolution and parameters on the final stability state of the game was conducted. The results demonstrate that the proposed security mechanism can reduce the number of the attack behavior effectively, increase the profits of users, and enhance the overall security of the system. The future study will focus on developing a specific technological method to discover the malicious behavior of users based on the credible third party.

References

Bonomi, F., Milito, R., Zhu, J., Addepalli, S., 2012. Fog computing and its role in the internet of things. In: Proceedings of the First Edition of the MCC Workshop on Mobile cloud Computing, pp. 13–16.
Bonomi, F., 2011. Connected vehicles, the internet of things, and fog computing. In: The Eighth ACM International Workshop on Vehicular Inter-Networking (VANET). Las Vegas, USA, pp. 13–15.
Cai, M., Wu, Z., Zhang, J., 2014. Research and prevention of rogue ap based mitm in wireless network. In: P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2014 Ninth International Conference, pp. 538–542.
Dong, M., Ota, K., Liu, A., 2015. Preserving source-location privacy through redundant fog loop for wireless sensor networks. In: Computer and Information Technology; Ubiquitous Computing and Communications.
Dsouza, C., Ahn, G.J., Taguinod, M., 2014. Policy-driven security management for fog computing: preliminary framework and a case study. In Information Reuse and Integration (IRI), 2014 IEEE 15th International Conference, pp. 16–23.
Lee, K., Kim, D., Ha, D., Rajput, U., Oh, H., 2015. On security and privacy issues of fog computing supported Internet of Things environment. In: Network of the Future (NOF), 2015 6th International Conference, pp. 1–3.
Maz, M.R.R., Khairi, A.W., Abustan, I., Rahim, S.S., Khan, M.N.N., Nasehir Khan, E.M., Yahaya, 2017. A study on the selection of suitable sites for integrated smart trapper system installation (InSmarts). Galeri Warisan Kejuruteraan 1 (1), 06–10.
Mejia, M., Peña, N., Muñoz, J.L., Esparza, O., Alzate, M.A., 2011. A game theoretic trust model for on-line distributed evolution of cooperation inMANETs. J. Network Comput. Appl. 34 (1), 39–51.
Ning, H., Wang, Z., 2011. Future internet of things architecture: like mankind neural system or social organization framework? IEEE Commun. Lett. 15 (4), 461–463.
Niyato, D., Hossain, E., 2009. Dynamics of network selection in heterogeneous wireless networks: an evolutionary game approach. IEEE Transact. Vehicular Technol. 58 (4), 2008–2017.
Smith, J.M., 1974. The theory of games and the evolution of animal conflicts. J. Theoret. Biol. 47 (1), 209–221.
Smith, J.M., Price, G.R., 1973. Lhe logic of animal conflict. Nature 246, 15.
Stojmenovic, I., Wen, S., 2014. The fog computing paradigm: scenarios and security issues. In: Computer Science and Information Systems (FedCSIS). Federated Conference, Warsaw, Poland, pp. 1–8.
Vaquero, L.M., Rodero-Merino, L., 2014. Finding your way in the fog: towards a comprehensive definition of fog computing. ACM SIGCOMM Comput. Commun. Rev. 44 (5), 27–32.
Wang, Y., Uehara, T., Sasaki, R., 2015. Fog computing: issues and challenges in security and forensics. In: Computer Software and Applications Conference (COMPSAC), 2015 IEEE 39th Annual, vol. 3, pp. 53–59.
Weibull, J.W., 1997. Evolutionary game theory. MIT Press.
Xu, L., 2017. Research on anti-overturning performance of multi-span curved girder bridge with small radius. Acta Mechanica Malaysia 1 (1), 11–15.
Xuana, G., Zhenga, H., Xiaoyua, S., Jua, L., Bin-Sheng, W., 2017. A Two-dimensional lattice Boltzmann method for compressible flows. Acta Mechanica Malaysia 1 (1), 04–07.
Yaacof, N., Qamaruzzaman, N., Yusup, Y., 2017. Comparison method of odour impact evaluation using calpuff dispersion modelling and on-site odour monitoring. Galeri Warisan Kejuruteraan 1 (1), 01–05.
Zhang, L., Jia, W., Wen, S., Yao, D., 2010. A man-in-the-middle attack on 3g-wlan interworking. In: Communications and Mobile Computing (CMC), 2010 International Conference, vol. 1, pp. 121–125.
Zhenga, H., Xuana, G., Xiaoyua, S., Jua, L., Bin-Sheng, W., 2017. An efficient pseudo-potential multiphase lattice Boltzmann simulation model for three-dimensional multiphase flows. Acta Mechanica Malaysia 1 (1), 08–10.