Available online www.jocpr.com

Journal of Chemical and Pharmaceutical Research, 2014, 6(5):1521-1528

Research Article

ISSN : 0975-7384
CODEN(USA) : JCPRC5

The evolutionary game study on the privacy and interest of users and websites in the social network environment

Xia Chen, Tingjie Lu, Longfei Guo and Shuyue Lou

School of Economics and Management, Beijing University of Posts and Telecommunications, Beijing, China

ABSTRACT

The previous researches on the relationship between privacy and interests are mostly concentrated in the indifference nodes (user behavior only) an mainly based on competition of interests of the players, This paper innovatively studied the long-term game based on privacy and the interests of the two sides: users and websites. We introduced emergency interference factors into the game for the first time, and constructed the evolutionary game of the interests and privacy of both sides, then simulate the trend of evolution game. Results show that, only the implementation of strong public opinion and supervision mechanism that maintain the interests of the user, can realize the expected results which maximum the utility of users and the whole social.

Key Words: privacy, evolutionary game, social network, factors of emergencies

INTRODUCTION

With the development and popularization of OSN (online social network), the safety of OSN's users' privacy becomes a crucial issue. Especially in social network, people cannot help to disclose their own privacy while releasing their personal information. In December 2011, many network sites such as Renren, Tianya BBS and SinaMicroblog have been involved in the "disclosure event", resulting in the wide concern on "privacy" by users and the industry.

On social networks, the user and the network site are the players of the game. Users tend to consider about privacy disclosure to obtain certain interest, and network sites tend to decide whether to disclose users' privacy or not for interest. Most of the previous studies have been focused on the game of the current interest by players. [1,2]. Scholars at home and abroad have conducted some researches with the application of evolutionary game on interpersonal communication[3],economic[4]and so on. Only a few scholars have already studied on the privacy issue by using the evolutionary game: Charles A. Kamhoua's research provides reference for the construction of our evolutionary game model, but it only focus on the game between the users, without considering the factor of websites [5].

In short, the previous researches on privacy are mostly concentrated in the current interests of the players, but most of the game players would like to take the long-term strategy in face of the interest. In this study, we innovatively studied the long-term game between users and websites, and introduced emergency interference factors for the first time and we constructed a evolutionary game model to study the evolutionary behavior of the problems of network privacy in social networks.

The other part of this paper is as follows: the second part is the building and analysis of the model while introducing emergency as a interference factor. In the third part, the evolution process curve was simulated through MATLAB in order to analyze its evolutionary rule directly and further to analyze what measures should be taken by Website, media and social respectively to achieve maximum benefits under different conditions. The fourth part is the conclusion.

EVOLUTIONARY GAME MODEL CONSTRUCTION OF INTERNET PRIVACY PROBLEM

First, suppose that before negative media exposure happens, build the payoff matrix. Second, suppose that when users are influenced by negative media exposure, and then build another payoff matrix.

2.1 Evolutionary Game Model without regard to Emergencies

Firstly, build the payoff matrix between users and website without regard to emergencies, as shown in table 1.Assumptions for income of users and website without regard to emergencies: (1)users do not know whether the website has leaked their privacy, so there is no loss when they post their private information(privacy);(2)Fixed income when users use the website (I_1);(3)Fixed income when users use the website and extra income acquired by disclosing private information (I_2, $I_2>I_1$);(4)Fixed value of websites (V_1);(5)Extra value of websites by selling users' information (V_2).

Table 1 The payoff matrix between users& website without regard to Emergencies

Websites Users	Leak privacy	Not leak privacy
Provide privacy	I_2，V_1+V_2	I_2，V_1
Not provide	I_1，V_1	I_1，V_1

2.1.1 Deduction of Evolutionary Game Model

In the real environment, it is common that websites and users make choices at a certain probability and achieve the equilibrium of hybrid strategy. For users, suppose that the proportion of choosing to provide private information is x (t) (short for x), and the proportion of not choosing is 1-x; for websites, suppose that the proportion of choosing to disclose users' privacy is y (t) (short for y), and the proportion of not choosing is 1-y. According to the method of fitness solution in the game theory and Table 1, following results can be obtained:

Users' income for providing private informationU_{1o}, Users' income for not providing private information:U_{1n}:

$$U_{1o} = I_2 \quad ; U_{1n} = I_1 \quad (1)$$

Average expected income of user group in a hybrid strategy regardless of providing private information:

$$U_1 = x^*I_2 + (1\text{-}x)^*I_1 \quad (2)$$

According to the theory of evolutionary game, if the proportion of individuals using certain strategy increases in group, the strategy will develop in the group. It is called replication dynamic equation. Therefore, the replication dynamic equation of user group strategy can be obtained based on Equation 1 and 2.

$$\frac{dx}{dt} = x(U_{1o} - U_1) = x * [I_2 - (x * I_2 + (1 - x) * I_1)](3)$$

Similarly, the value of websites for leaking users' information:

$$U_{2l} = x(V_1 + V_2) + (1\text{-}x)V_1 \quad (4)$$

The value of websites for not leaking users' information:

$$U_{2n} = V_1(5)$$

Average expected value of website group in a hybrid strategy regardless of leaking users' information:

$$U_2 = y^*[x^*(V_1 + V_2) + (1\text{-}x)V_1] + \ (1\text{-}y)V_1 \qquad (6)$$

The replication dynamic equation of website group can be obtained based on Equation4 and 6.

$$\frac{dy}{dt} = y[U_{2l}\text{-}U_2] = y^*(1\text{-}y)^*x^*V_2(7)$$

2.1.2 Analysis of Evolutionary Game Model

According to the character of evolutionary stable strategy, a stable state that stays robust against small perturbations will be called evolutionary stable strategy. Mathematically, it is equivalent that when perturbations make x less than x*,$\frac{dx}{dt} = F(x)$must be greater than 0; when x is higher than x*, $\frac{dx}{dt} = F(x)$ must be less than 0. Based on this, suppose that$\frac{dx}{dt} = F(x) = 0$ then x=0 or x=1. When x=0, F'(x) is greater than 0. So it is not the evolutionary stable strategy of this game. Only when x=1, it is the evolutionary stable strategy. Similarly, when y=1, it is the evolutionary stable strategy of websites.

It means, under the circumstance which there is no negative media exposure and other ways to let users know whether their private information has been leaked. Users will finally provide their private information to website, and websites will finally leak and sell users' private information.

2.2 Evolutionary Game Model with regard to Emergencies

(1) Assumption of the Model and Payoff Matrix

Over above analysis, the payoff matrix between users and websites is built considering the emergencies, shown as Table 2.Considering emergencies, make following assumptions for income of users and websites (new variables of C, I_3, R): (1)The cost when users post private information (C);(2)When the users change the privacy setting or install privacy protection software. After they feel safe, safety income (I_3) appear; (3) Websites' leaking users information is exposed, which result in website reputation loss (R).

Table 2 Payoff Matrix between Users & Websites Considering Emergencies

Websites Users	Leak privacy	Not leak privacy
Provide privacy	I_2–C+I， V_1+V_2–R	I_2， V_1
Not provide privacy	I_1， V_1	I_1， V_1

(2) Deduction of Evolutionary Game Model

Under this payoff matrix, users' income for providing private information is

$U_{1o} = y*\left(I_2\text{-}C + I_3\right) + \left(1\text{-}y\right)*I_2$ (8)

Users' income for not providing private information is

$U_{1n} = I_1$(9)

Average expected income of user group in a hybrid strategy regardless of providing private information is：

$U_1 = x * [y * (I_2 - C + I_3) + (1 - y)I_2] + (1 - x) * I_1$(10)

The replication dynamic equation of user group can be obtained based on Equation8 and 10：

$\frac{dx}{dt} = x\left(U_{1o}\text{-}U_1\right) = x*(1\text{-}x)\left[I_2\text{-}I_1\text{-}y* \quad C + y*I_3\right]$(11)

Similarly, the value of websites for leaking users' information:

$U_{2l} = x\left(V_1 + V_2\text{-}R\right) + \left(1\text{-}x\right)V_1$(12)

The value of websites for not leaking users' information:

$U_{2n} = V_1$ (13)

Average expected value of website group in a hybrid strategy regardless of leaking users' information:

$U_2 = y*[x*\left(V_1 + V_2\text{-}R\right) + \left(1\text{-}x\right)V_1] + \left(1\text{-}y\right)V_1$(14)

The replication dynamic equation of website group can be obtained based on Equation11 and 13.

$\frac{dy}{dt} = y\left[U_{2l}\text{-}U_2\right] = x*y*\left(1\text{-}y\right)*(V_2\text{-}R)$ (15)

(3) Analysis of Evolutionary Game Model

Analyze equation (11) and suppose that$\frac{dx}{dt} = F(x) = 0$ then get x=0 or x=1. Since the value of I_3-C is uncertainty, it is necessary to conduct evolutionary stable analysis for the value range of different parameters. And the analysis of websites can be done in the same way. When the evolution comes to a stable state, there is an x* which meets F'(x*) = (1-2x*) (I_2-I_1-yC+yI_3) <0. We can easily get the following result through different parameters:

(1) When C>I_3 and y>$\frac{I_2\text{-}I_1}{C\text{-}I_3}$, if x=0, it is evolutionary stable strategy; if x=1, it is not evolutionary stable strategy;(2) When C>I_3 and y<$\frac{I_2\text{-}I_1}{C\text{-}I_3}$, if x=0, it is not evolutionary stable strategy; if x=1, it is evolutionary stable strategy;(3) When C<I_3, if x=1, it is evolutionary stable strategy; if x=0, it is not evolutionary stable strategy;

Similarly, when the evolution comes to a stable state, there is a y* which meets F'(y*) = (1-2y*)*X*(V_2-R). We can easily get the following result through different parameters:

(1)When x=0, y is always the evolutionary stable solution; (2) When x≠0 and V_2>R, if y=1, it is evolutionary stable solution; if y=0, it is not evolutionary stable solution; (3) When x≠0 and V_2<R, if y=1, it is not evolutionary stable solution; if y=0, it is evolutionary stable solution;

Furthermore, replication dynamic relationship and stability between websites and users are shown in Figure1，2, 3 and 4 respectively.

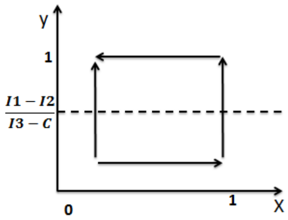

Figure1: C>I_3,V_2>R

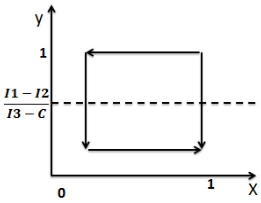

Figure2: C>I_3,V_2<R

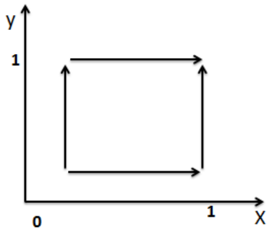

Figure3: C<I_3,V2>R

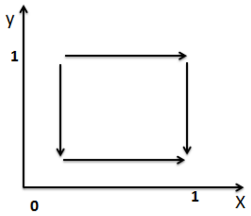

Figure4: C<I_3,V_2<R

It can be Charted out from Figure1 and Figure2 that y= $(I_2 - I_1)/(C - I_3)$is a critical value of the evolutionary trend of x. By analyzing the critical value, it can be found that the denominator(C-I_3) is the difference between the loss of users for providing private information and safety income they get when their private information are being threatened, they tend to change their privacy settings or install privacy protection software so that they will feel safer. This difference is the cost of users for leaking their private information. The numerator (I_2-I_1) is the extra income of users for leaking their private information（hereafter referred to as extra income）. Therefore, this critical value is ratio of income and cost of leaking private information. With further analysis, it is found that when the critical value is a negative number, y is surely greater than the critical value and cannot affect the trend of x; besides, when income is greater than cost, the critical value will be greater than 1 and cannot affect the trend of x either. In other words, only when C>I_3 and income is less than cost can the critical value be effective.

DATA SIMULATION ANALYSIS

Based on the evolutionary game model construction and analysis, data simulation analysis is used to describe the evolution of the social network privacy. The paper adopts 2*2d evolutionary game model for simulation, and use Matlab for simulation and analysis, and the specific evolution process and analysis are as follows:

Setting of Parameters are as follows：Initial Value
Of X(0.3)；Initial Value Of Y(0.3/0.7);I_1(6); I_2(10); I_3 (4/10);V_1 (4); V_2 (6/10); C (10/4); R (6/10).

(1) When the initial value of X (the proportion of users who choose to provide their private information) is 0.3 and 0.7, the simulation result is shown in the Figure5.

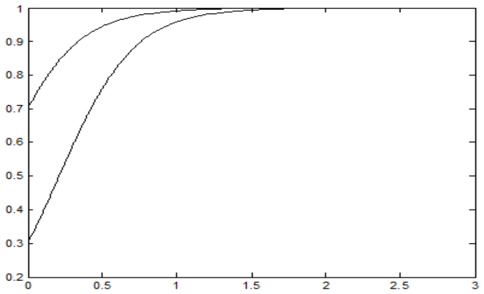

Figure5 Simulation Result When the Initial Value Is 0.3 and 0.7

(2) Similarly, an evolutionary analysis can be conducted for the initial value of y (the proportion of websites which leak users' private information). When the value is separately 0.3 and 0.7, the simulation result is shown in the Figure6.

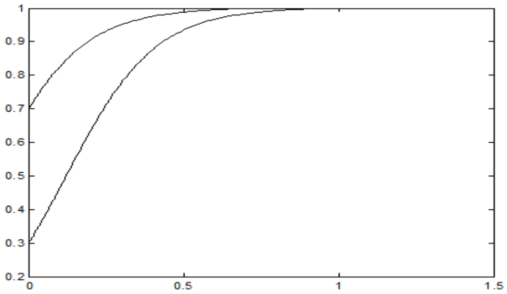

Figure 6 Simulation Result When the Initial Value of X Is 0.7

The simulation results above prove that the final trend of evolution has nothing to do with the initial value of x and y. So the following analysis will be classified according to parameters and situations. When emergent factors are introduced, the matrix will be changed into the payoff matrix of users and social networks involving the emergencies above. Then:

(1) When $C>I_{3,}$ $y>\frac{I_2-I_1}{C-I_3}$and $V_2>R$:

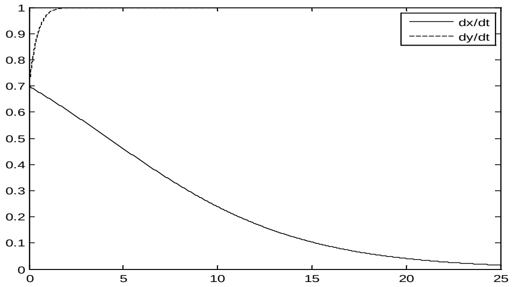

Figure 7 Simulation Result in Situation 1

As shown inFigure7,x is gradually close to 0 from 0.7. Finally, it infinitely approaches 0 and then reaches a stable state. And Y is also gradually close to 1 from 0.7. Finally, it infinitely approaches 1 and reaches a stable state.

Its practical significance is that when the information cost is greater than security earnings, the initial ratio of the websites which leak user privacy is greater than critical value, and, the benefit that websites obtain from leaking user privacy is greater than the loss of reputation, all websites would tend to leak user privacy and all users would tend to not provide their privacy. The result of long-term evolution is that the business related to user privacy cannot be implemented, and users extremely distrust websites. Also, websites will not get benefit from leaking user privacy. It can be said a lose-lose result.

(2) When $C>I_3$, $y<\frac{I_2-I_1}{C-I_3}$and $V_2>R$:

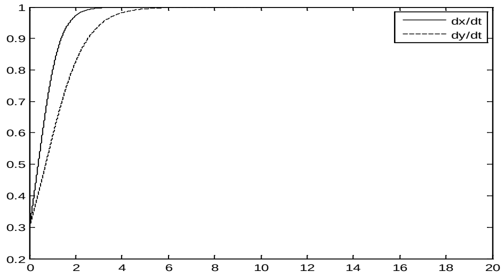

Figure8 Simulation Result in Situation 2

Figure8 shows that when C>I_3, y<$\frac{I_2\text{-}I_1}{C\text{-}I_3}$and V_2>R, x is gradually close to 1 from 0.3. Finally, it infinitely approaches 1 and then reaches a stable state. And Y is also close to 1 from 0.3. Finally, it infinitely approaches 1 and reaches a stable state.

Its practical significance is that when the information cost is greater than security earnings, the initial ratio of the websites which leak user privacy is less than critical value, and, the benefit that websites obtain from leaking user privacy is greater than the loss of reputation, all websites would tend to leak user privacy and all users would tend to not provide their privacy. The result of long-term evolution is, once users log in, their privacy will be leaked, from which all websites can get benefit.

(3) When C>I_3, y<$\frac{I_2\text{-}I_1}{C\text{-}I_3}$ and V_2<R：

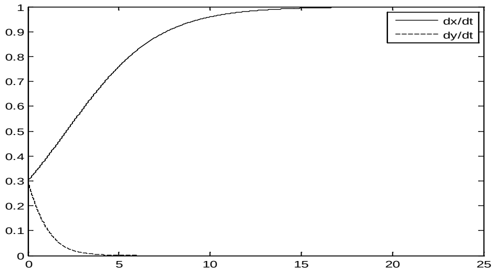

Figure 9 Simulation Result in Situation 3

Figure9 shows that when C>I_3, y<$\frac{I_2\text{-}I_1}{C\text{-}I_3}$ and V_2<R, x is gradually close to 1 from 0.3. Finally, it infinitely approaches 1 and then reaches a stable state. And Y is also gradually close to 0 from 0.3. Finally, it infinitely approaches 0 and reaches a stable state.

Its practical significance is that when the information cost is greater than security earnings, the initial ratio of the websites which leak user privacy is less than critical value and the benefit that websites obtain from leaking user privacy is less than the loss of reputation, all websites tend to not leak user privacy and all users would tend to provide their privacy. The result of long-term evolution is that websites cannot gain benefit by leaking user privacy, and all users are not concerned about their privacy, and will provide their private information for websites without worrying about leaking their privacy.

(4) When C>I_3, y>$\frac{I_2\text{-}I_1}{C\text{-}I_3}$and V_2<R：

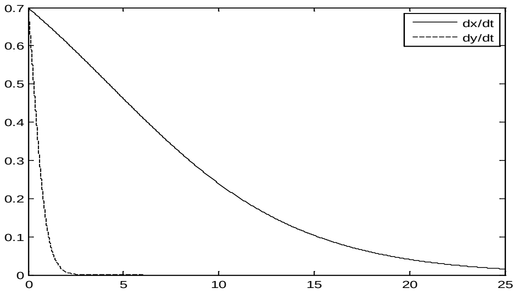

Figure 10 Simulation Result in Situation 4

Figure 10 shows that when $C>I_3$, $y>\frac{I_2-I_1}{C-I_3}$ and $V_2<R$, x is gradually close to 0 from 0.3. Finally, it infinitely approaches 0 and then reaches a stable state. And Y is gradually close to 0 from 0.7. Finally, it infinitely approaches 0 and reaches a stable state.

Its practical significance is that when the information cost is greater than security earnings, the initial ratio of the websites which leak user privacy is greater than critical value and the benefit that websites obtain from leaking user privacy is less than the loss of reputation, all websites would choose to protect user privacy without gaining benefits from trafficking in privacy. Even so, users would not provide their privacy to websites. The result of long-term evolution is that some business related to user privacy such as LBS cannot be implemented. No one wants this result, especially the websites.

(5) When $C<I_3$ and $V_2>R$:

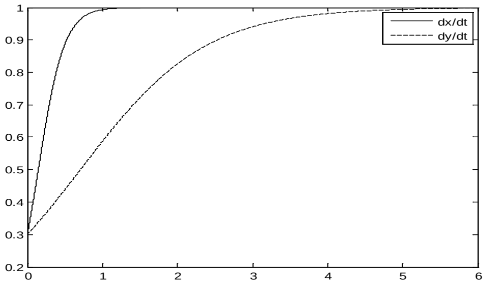

Figure 11 Simulation Result in Situation 5

Figure 11 shows that when $C<I_3$ and $V_2>R$, x is gradually close to 1 from 0.3. Finally, it infinitely approaches 1 and then reaches a steady state. Y is gradually close to 1 from 0.3. Finally, it infinitely approaches 1 and reaches a steady state.

Its practical significance is that when the information cost is less than security earnings, the initial ratio of the websites which leak user privacy is less than critical value and the benefit that websites obtain from leaking user privacy is greater than the loss of reputation, all users are evolved to provide their privacy and all websites are evolved into websites of selling user information. The result of long-term evolution is that, once users log in, their privacy will be leaked and then be sold. Then the right of privacy cannot be guaranteed.

(6) When $C<I_3$ and $V_2<R$:

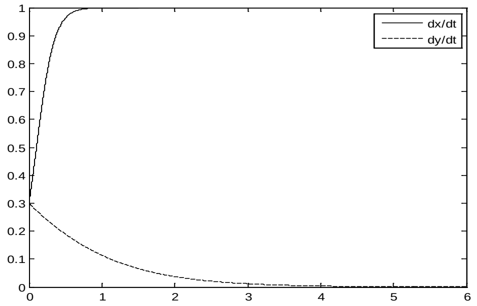

Figure 12 Simulation Result in Situation 6

Figure 12 shows that when $C<I_3$and $V_2<R$, x is gradually close to 1 from 0.3. Finally, it infinitely approaches 1 and then reaches a stable state. And Y is gradually close to 0 from 0.3. Finally, it infinitely approaches 0 and reaches a stable state.

Its practical significance is that when the information cost is less than security earnings, the initial ratio of the websites which leak user privacy is greater than the critical value and the benefit that websites obtain from leaking user privacy is less than the loss of reputation, all users could safely provide their privacy to websites, and even so, all websites would not leak user privacy. The result in this situation is the same as that in situation 3, but the conditions required are different.

CONCLUSION

4.1 Websites' angle

The most favorable evolution results of whom is shown in the figure 11 and figure 8.

The most favorable evolution results of whom is shown in the figure 11 and figure 8.It is not difficult to see that, to achieve the evolution results of these two pictures, the premise is V>R, which means the benefits of revealing the users' information outweigh the possible loss of reputation. If this premise is met, then further consider:

(1)If the information cost outstrip the yield, which means the total cost of the disclosuring of information is above zero, and the user feel a loss, then it is time to control the number of initial websites who leak information within the industry, in order to make the amount less than the critical value.

(2)If the information cost is less than the safety benefit, which means users whose information has been leaked obtain income instead of feel a loss because of a series of safety measures provided by the websites, then the site can be assured of the leakage of user privacy.

4.2 Users' angle

Users expect that the network sites will not disclose any of the personal information provided by themselves, the most favorable evolution results of whom is shown in the figure 9 and figure 12.

Users expect that the network sites will not disclose any of the personal information provided by themselves, the most favorable evolution results of whom is shown in the figure9 and figure 12.It can be found that the result of the above figure is beneficial not only to users, but also to the healthy development of the entire social network industry. In order to reach the above result, it has to be ensured that V2 <R, that is, the interest gained by information sale of the website shall be smaller than its loss of reputation, so R can be improved and V_2 can be decreased fur the purpose of ensuring this point. On this basis:

(1) If there are only several websites disclosing users' information in the industry (below the threshold), users should try to improve C or the information cost, and reduce I_3 or the security benefit. In addition, if the information provided by the user is of great value, it may lead to $C >> I_3$, while the websites can turn users into high-privacy concerning groups by reducing the private safety settings and improve users' privacy concerns to ensure this, so as to achieve the effect shown in the figure 9.

(2)If the users belong to low-privacy concerning groups, who would have no loss in privacy disclosure or would stay in a relatively safe and closed social contact environment, it may lead to the situation of $C<I_3$, so as to achieve the effect shown in the right figure12.

4.3 Social's angel

If it is to achieve the goal of healthy development of social network sites with win-win solution, it requires V2<R, that is, the interested gained by information sale of the websites shall be smaller than their own loss of reputation. From the perspective of V2 control, users should provide their own private information as little as possible. Besides, privacy purchasing shall not be allowed as far as possible with the strengthening efforts made by supervisors to focus on the purchasing source and market demands. From the perspective of R control, on the one hand , it is still the safety awareness of users themselves; on the other hand, media supervisory still plays an important role whose coverage degree is much more powerful than the spreading power of users themselves. In short, a satisfactory social network operating environment can be formed only with the emphasis on various aspects such as the system, media, and precautions.

acknowledgment

The research is supported by National Basic Research Program of China (973 Program) (2012CB315805), Project of National Natural Science Foundation of China (71172135，71231002), and the Fundamental Research Funds for the Central Universities（2013RC0603）.

REFERENCES

[1] S.B.Zhang, W.D.Cai, Y.J.Li J*ournal of Northwestern Polytechnical University*, vol.29,no.4, **2011**.

[2] J.Blocki, C.Nicolas ,D.Anupam, "AruneshSinha.Regret Minimizing Audits:A Learning-theoretic Basis for Privacy Protection," *24th Computer Security Foundations Symposium*, **2011**.

[3] F.Ding, Y. Liu, et, *International Journal of Modern Physics C*, vol.20,no.03,pp. 479-490, **2009**.

[4] K.Safarzyńska, *Journal of Evolutionary Economics*, vol.20,no.03, pp. 329-373, **2010**.

[5] A.K.Charles，P.Niki,M.Kia , "Game Theoretic Modeling and Evolution of Trust in Autonomous Multi-Hop Networks,"*IEEE ICCC*, **2011**.