FHGM: A Frequency Hopping Game Model with Communication Security Awareness for WSN

Chunlai Du[1], Jixiang Zhang[1], Jianshun Zhang[1, 2], Li Ma[1] and Xianxian Wang[1]

[1]*College of Information Engineering, North China University of Technology, No.5 Jinyuanzhuang Road, Beijing 100144, China*
[2]*Hopen Software Engineering Co., Ltd, Building 4#, 4# South Fourth Street, Zhong Guan Cun, Beijing 100190, China*
zhangjs0322@163.com

Abstract

Wireless sensor networks (WSNs) are in an open wireless environment which is complex and volatile, and often subject to inadvertent or intentional interference, sensor networks can use frequency hopping technology to get away from the interference. Therefore how accurate and timely frequency hopping is particularly important issue. To solve that, this paper built a Bayesian frequency hopping game model based on Nash equilibrium game theory. The formal definition and quantified description of the impact factors in the game model are described, and Bayesian Nash equilibrium is proved. Through the simulation and analysis shows that this model with communication security awareness can improve the accuracy of the frequency hopping, make the time of frequency hopping become more rational, prolong the network lifetime and maintain the overall network connectivity.

Keywords: *Wireless sensor networks, frequency hopping, Nash equilibrium game theory*

1. Introduction

As the extensive application of wireless technology, a variety of wireless communication devices work simultaneously in narrow space. When a variety of wireless mobile networks work at the same time in the wireless personal area network, wireless signals using different protocol will exist simultaneously, and bring the inevitable noise jamming with each other. Serious mutual interference between the various wireless signals, it will affect the stability of the entire WSNs. Meanwhile, in certain application areas, wireless sensor networks will also be attacked by some intentional malicious attacks, ultimately making wireless sensor networks do not work properly.

With the improvement of the security requirements of the WSNs, how to make WSNs avoid frequency band interference or congested attacks is the urgent problem needed to be studied and solved. Frequency hopping communication is a very effective method against frequency band interference and congested attack. When the communication channel of nodes in WSNs subject to frequency band interference or channel block, it can jump to a good quality channel in order to maintain the stability of the entire wireless sensor networks. We proposed a frequency hopping game model based on the Nash equilibrium game theory. Simulation experiment proved that the model had made the frequency hopping more rational and maintained the overall connectivity of WSNs.

This paper is organized as follows: Section 2 gave an overview on related work. Section 3 proposed our frequency hopping game model, providing formal definition and

quantified description of the impact factors. Section 4 is simulation and analysis. Section 5 is the conclusion and the future work.

2. Related work

Literature [1] focuses on whether the WSN, which consists of a large number of short single-hop links and a small number of long single-hop nodes, is more stable or not. Based on the different hopping strategy, an analytical expression to compute the metric aggregate multi-hop information efficiency is derived. Literature [2] introduced online optimization theory into anti-jamming communication based on UFH (uncoordinated frequency hopping) and quantitatively analyzes anti-jamming communications based on UFH. By formulating the UFH-based anti-jamming communication as a non-stochastic multi-armed bandit (MAB) problem, Literature [2] proposed online learning UFH algorithm and proved that the algorithm can achieve asymptotic optimum. Literature [3] proposed an anti-jamming cooperation broadcast scheme for wireless networks, used the non-coordinated frequency hopping technology to be against interference problem caused by pre-shared keys, and makes the wireless sensor network become more and more robust immunity through nodes' mutual cooperation. It has proved that this anti-jamming cooperation broadcast scheme is a valid way to be against interference. In [4], adaptive rapid channel hopping mechanism was proposed. The new concept of consolidated reside window (Dwell Window) and spoofing mechanisms (Deception Mechanism) were put forward in this paper. DW and DM were integrated into adaptive fast channel transition mechanism. Numerical analysis and simulation results showed the effective suppression of interference attack. Literature [5] investigated the performance of coherent time delay estimation technique for frequency hopping GSM signals. Compared to state-of-the-art techniques, coherent time delay estimation techniques can achieve high bandwidth delay estimation and localization. In [6], EPA-based Frequency Hopping Metric is proposed and applied to frequency-hopping algorithm. In [7], this paper points out that FH / MFSK WSN (M-ary frequency-shift keying (MFSK) modulation and frequency-hopping (FH)) can monitor multiple ESa (source events) in different states at the same time. FH / MFSK WSN using non-fusion rules has lower complexity, and can be used in wide range of application scenarios. Literature [8] explores a novel application of cognitive radios for reliable satellite communication. By using dynamically adjusted frequency hopping (FH) sequences, the communication sequences were more robust against smart eavesdropping and targeted interference than fixed FH sequences. In [9], detection and avoidance mechanism for resisting the interference of the channel was proposed. Based on the rapid detection of same frequency disturbance existence, the coordinator selected the best carrier frequency by frequency hopping through multiple predetermined channels. Literature [10] proposed adaptive slot channel hopping (A-TSCH) which utilized blacklist technology. Compared to TSCH, A-TSCH can significantly improved the reliability of channel hopping scheme and provided better protection from interference for WSNs. In [11] and [12] study on Intrusion Detection, and [13] study on the Cross Layer Security Framework.

When some parts of WSNs are suffering from attacks or interference, while the other parts have high-quality communication channel and some key nodes are in interference region, whether to carry out frequency hopping or not? In order to maintain these several disturbed key nodes active, whether to carry out frequency hopping? We introduce the game theory into the scheme of frequency hopping. From a global

perspective, all the nodes rationally evaluate the situation and adopt the rational decision for getting the maximized overall network performance.

3. Frequency Hopping Game Model (FHGM)

Assume that all nodes are rational decision-making entities to maximize their payoff. And assume that attack has been detected and some nodes proposed hopping request.

The game between proposing frequency hopping and not proposing frequency hopping is game of the conflict of interest mutual. The double players expect to maximize themselves payoff. The two players are rational. Therefore the profit between proposing frequency hopping and not proposing frequency hopping is opposite. Their strategy space are hopping or not hopping. So the game between proposing frequency hopping and not proposing frequency hopping is incomplete information, non-cooperative, finite and static confrontational Game.

3.1. Related Definitions and factors

3.1.1. Related definitions: In this paper, sensor nodes in WSN are divided into Hop and the Non-Hop. Hop denotes the set of proposing frequency hopping. Let i, players, denotes sensor nodes of Hop. Non-Hop denotes the set of not proposing frequency hopping. Let j, players, denotes sensor nodes of Non-Hop.

Definition 1. The cost of frequency hopping: The consumption of resources or energy due to launch frequency hopping and the cost of the throughput decrease temporarily. That is the cost of frequency hopping.

Definition 2. The payoff of frequency hopping: Considering from the interests of the overall network, wireless sensor network gains the payoff when deciding to hop. For example, the network away from attack, the lifetime of network is extended, throughput of the network back to normal. These make up the payoff of frequency hopping.

Definition 3. The cost of not frequency hopping: The cost is caused by that the nodes do not select frequency hopping when the network is suffering attack.

Definition 4. The payoff of not frequency hopping: The payoff is gained from that the nodes do not select frequency hopping when frequency hopping is unnecessary considering from the profit of whole network.

Definition 5. The expect payoff of frequency hopping: The expect payoff of the network select frequency hopping.

Definition 6. The expect payoff of not frequency hopping: The expect payoff of the network don't select frequency hopping.

3.1.2. Influencing factors of payoff about not hop: Influencing factors of payoff about not hop are shown in Figure 1.

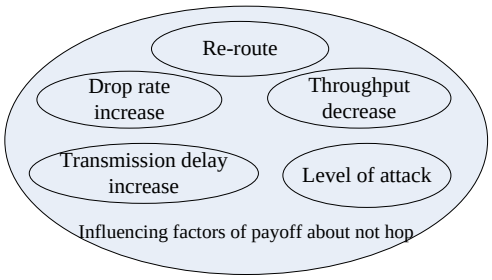


Figure 1. Influencing Factors of Payoff about not Hop

Factor 1. The cost of re-route: If the networks don't select frequency hopping it will be split. Then some nodes could not communicate with other nodes keeping the previous route. So the route path must be changed to transmit data. That will result in re-route.

Factor 2. Throughput decrease: When the network is under DDoS attack or interference attack, data cannot be forwarded in time or even cause packet drop. That greatly affects the throughput of the network, resulting in throughput decrease.

Factor 3. Level of attack: When the network suffers attack, fierce or mild, thus the level of attack is different. The level of attack is defined according to the affect of the attack.

Factor 4. Drop rate increase: When the network is under DDoS attack or interference attack, drop rate increase compared to normal conditions which has not been attacked.

Factor 5. Delay increase: When the network is under attack, packet forward and receive have delay. Packets cannot reach their destination within the tolerance time.

3.1.3. Influencing factors of payoff about hop: Influencing factors of payoff about hop are shown in Figure 2.

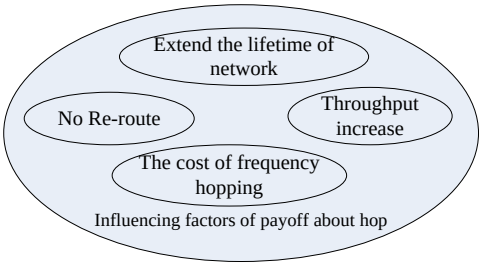


Figure 2. Influencing Factors of Payoff about Hop

Factor 6. No need to re-route: The integration strategy of network in this paper is to make every effort to maintain the original route. So the route do not need rebuild after frequency hopping, which eliminate the cost of re-route.

Factor 7. Throughput increase: when the frequency hopping is launched, the frequency is firstly switched, and then data transmission is stop temporarily. Those results in throughput decrease which may be neglected compared to the network under attack don't launch frequency hopping. So as a whole, the throughput of network relatively increases.

Factor 8. The cost of frequency hopping: when the network launch frequency hopping, energy must be consumed due to communication between the nodes. And frequency hopping will occupy the bandwidth of the wireless communication.

Factor 9. Extend the lifetime of network: The life of the network will be extended when the network under attack properly launch frequency hopping.

3.2. Proposed Frequency Hopping Game Model (FHGM)

3.2.1. FHGM foundation: The FHGM contains three elements: the players, the strategy space and the utility function.

Definition 7.FHGM is denoted by triples (P, S, U).

Players P: $\{P_h, P_{nh}\}$ denote the nodes of WSNs. P_h denotes the nodes of proposing frequency hopping; P_{nh} denotes the nodes of not proposing frequency hopping.

Strategy space S: $\{S_h, S_{nh}\}$ denote the strategy space of nodes. S_h denotes the strategy set of proposing frequency hopping. S_{nh} denotes the strategy set of not proposing frequency hopping. Each node has two strategies: (Hop, Non-Hop) which also be expressed as (H, NH).

Utility function U: $\{U_h , U_{nh}\}$ denote the utility function of the game model, which are benefits of both sides of the game. U_h denotes the payoff after hopping. U_{nh} denotes payoff non-hopping.

The symbols used in FHGM hopping game model shown in Table 1.

Table 1. Symbols used in the Game Model

Symbol	Meaning
C_h^i	The cost of frequency hopping (Nodes of proposing frequency hopping)
C_h^j	The cost of frequency hopping (Nodes of not proposing frequency hopping)
C_{nh}^i	The cost of not frequency hopping (Nodes of proposing frequency hopping)
C_{nh}^j	The cost of not frequency hopping (Nodes of not proposing frequency hopping)
U_h	Earnings of frequency hopping
U_{nh}	Earnings of not frequency hopping
α	The probability of hop(Normal)
β	The probability of hop(False alarm)

As shown in Table 1, let α denotes the probability that node decides to hop in normal condition. Let β denotes the probability that node decides to hop under the condition of false alarm from intrusion detection system. Let C_h^i denotes the cost of the nodes selecting frequency hopping strategy, in which nodes denoted by subscript i propose the hopping request. And let C_h^j denotes the cost of the nodes carry out frequency hopping strategy, in which nodes don't propose the hopping request. Define C_{nh}^i as the cost of the nodes not selecting frequency hopping strategy, in which the nodes denoted by subscript i propose the hopping request. And define C_{nh}^j as the cost of the nodes not carrying out frequency hopping strategy, in which nodes don't propose the hopping request.

The payoff matrix of frequency hopping game model is shown in Table 2 and Table 3. Table 2 is the payoff matrix in normal condition. And Table 3 is the payoff matrix in the

condition of false alarm. Where α and β represent the probability of frequency hopping, (1-α) and (1-β) represent the probability of not frequency hopping.

Table 2. Payoff Matrix (Normal)

		Non-Hop	
		H	NH
Hop	H	$\{\alpha C_h^i,\ \alpha C_h^j\}$	$\{\alpha C_h^i,\ (1-\alpha) C_{nh}^j\}$
	NH	$\{(1-\alpha) C_{nh}^i,\ C_h^j\}$	$\{(1-\alpha) C_{nh}^i,\ (1-\alpha) C_{nh}^j\}$

Table 3. Payoff matrix (False alarm)

		Non-Hop	
		H	NH
Hop	H	$\{\beta C_h^i,\ \beta C_h^j\}$	$\{\beta C_h^i,\ (1-\beta) C_{nh}^j\}$
	NH	$\{(1-\beta) C_{nh}^i,\ \beta C_h^j\}$	$\{(1-\beta) C_{nh}^i,\ (1-\beta) C_{nh}^j\}$

The relationship between the cost of hopping or not hopping and influencing factors is shown in Figure 3.

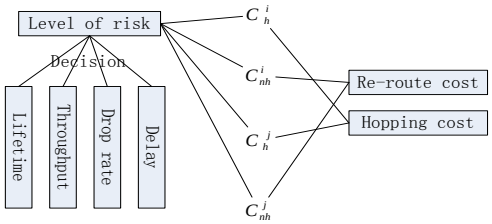


Figure 3. The relationship between the cost and factors

The influencing factors consist of network lifetime, throughput, drop rate and transmission delay.

Unnecessary Hopping and frequent Hopping will both affect the overall network performance. When the attacks only seriously affect the small parts of network but in which parts some important key nodes exist, such as cluster head nodes or the management nodes, while other parts have good quantity communication channel, whether to carry out frequent hopping is a game problem.

Theorem 1. There is Nash equilibrium in the frequency hopping game model.

Proof:

According to Nash's theorem, a game with n participants is described as formula (1).

$$G = \{S_1, S_2, ..., S_n; u_1, u_2, ..., u_n\} \quad (1)$$

If n is limited, and Si is limited set (i =1, 2, … , n), then this game exist at least a Nash equilibrium. That every finite strategy game has at least one mixed strategy Nash equilibrium.

The strategy space of the players in the FHGM is limited. Every player has two strategies, hopping or not hopping. According to the Nash equilibrium existence theorem, any finite

strategy space game exist at least Nash equilibrium. Hop or Non-Hop player in the FHGM is rational. Only when the FHGM model achieves the Nash equilibrium, then the utility of player gains is maximization. The strategy to achieve the Nash equilibrium is the better selection. Finally, the players decide frequency hopping or not hopping simultaneously.

3.2.2. Bayesian Nash Equilibrium Analysis: The priori probability of false alarm form intrusion detection system in WSNs is assigned. Let p denotes the probability of false alarm from intrusion detection system. α denotes the probability of Player j selecting hopping strategy in normal condition. β denotes the probability of Player j selecting hopping strategy in false alarm condition. With the above assumption, the static Bayesian hopping game tree is shown in Figure 4. Here N denotes the sensor nodes. In game theory it is always assumed that players are rational and wants to maximize their payoffs. So Player i always want to launch frequency hopping to resist the interference or attack. On the other hand, Player j always does not want to launch frequency hopping to maintain the current throughput or save energy.

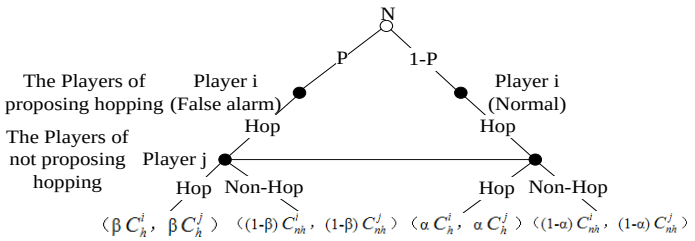


Figure 4. Bayesian Hopping Game Tree

Nodes are divided into two types of roles, the players of proposing hoping and the players of not proposing hopping. Every player calculated his expected payoff under each of strategy.

The expected payoff for Player j to carry out hopping strategy is calculated according to the formula 2

$$E_{uj}(H) = p\beta C_h^j + (1-p)\alpha C_h^j \quad (2)$$

The expected payoff for Player j not to carry out hopping strategy is calculated according to the formula 3

$$E_{uj}(NH) = p(1-\beta) C_{nh}^j + (1-p)(1-\alpha) C_{nh}^j \quad (3)$$

So if $E_{uj}(H) > E_{uj}(NH)$, then the best response of player j is to carry out hopping strategy. If $E_{uj}(H) < E_{uj}(NH)$, then the best response of player j is not to carry out hopping strategy.

The expected payoff for Player i to carry out hopping strategy is calculated according to the formula 4.

$$E_{ui}(H) = p\beta C_h^i + (1-p)\alpha C_h^i \quad (4)$$

The expected payoff for Player i not to carry out hopping strategy is calculated according to the formula 5.

$$E_{ui}(NH) = p(1-\beta) C_{nh}^i + (1-p)(1-\alpha) C_{nh}^i \quad (5)$$

So if $E_{ui}(H) > E_{ui}(NH)$, then the best response of player j is to carry out hopping strategy. If $E_{ui}(H) < E_{ui}(NH)$, then the best response of player j is not to carry out hopping strategy.

According to the Theorem 1, Nash Equilibrium is existent in the FHGM model. The two players, Player i and Player j, will both play the hopping strategy or not hopping strategy through weigh their payoff using themselves' utility function. Therefore, the final strategy of game in the FHGM model is only two, hopping or not hopping. Thus achieve equilibrium.

4. Simulation and performance evaluation

4.1. Simulation Scene

Experimental environment is Fedora12 and NS2.34. The specific parameters used in the simulation are shown Table 4.

Table 4. Simulation Parameters

Parameter Name	Parameter Value
Channel Type	Channel/WirelessChannel
Radio Model	Propagation/TwoRayGround
PhyType	Phy/WirelessPhy
MacType	Mac/802_11
Queue Type	Queue/DropTail/PriQueue
Link Layer Type	LL
AntType	Antenna/OmniAntenna
Max packet in ifq	50
Number of Nodes	20
Number of malicious nodes	1
Routing Protocol	AODV
Traffic Type	CBR
Topo Size	100*100 m
Energy Model	EnergyModel
Initial Energy	10000.0 J
txPower	0.660 W
rxPower	0.395 W
idlePower	0.035 W

Main parameters of simulation scenarios: Topology of the network is in the range of 100×100 square regions. 20 nodes are laid randomly and kept still. IEEE802.11 protocol is used as MAC protocol. CBR is used to generate network traffic.

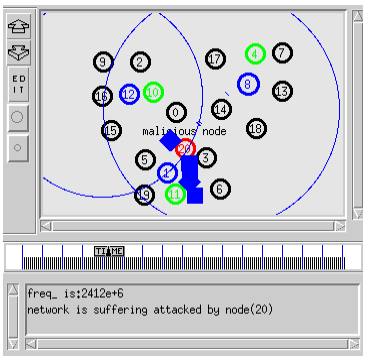


Figure 5. Simulation Scene

In scene, the nodes, 1, 8 and 12, are the cluster head node. The nodes, 4, 10 and 11, are management node. The node, 20, is malicious node shown in Figure 5. The other nodes are the cluster member nodes.

We make three scenes to analyze the network. The network is suffering attack and using the FHGM model to resist the attack shown in Figure 5.

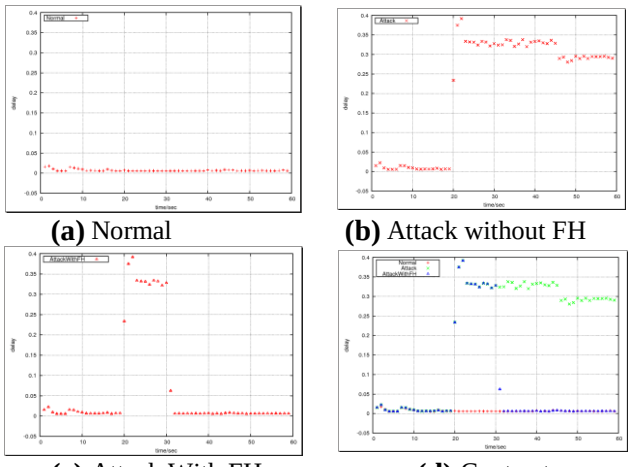
Assume that false alarm rate of the intrusion detection system is 0.05 which can be modified according to the actual situation. The type of attack is specified. The attack nodes send largely useless packets within the set time interval.

According to parameters of the FHGM model related about payoff, taking into account the Bayesian Nash Equilibrium, the simulation and performance evaluation of FHGM model is made in the same attack scene. The value of parameters used in cost of hopping model are calculated by initial energy, transmission power, receive power and idle power that is set in the energy model. α and β are determined by the specific application and their security needs. So the FHGM model is universal and self-adaptive. The initial value of α and β are set to 0.8 and 0.2 in this section.

4.2. Performance Analysis

To evaluate the effectiveness of FHGM model, this section uses the evaluation index include transmission delay, drop rate and jitter to analyze the network performance under attack.

4.2.1. Transmission delay: The transmission delay of the network is shown in Figure 6. The Figure 6(a) shows the delay of network in normal. The Figure 6(b) shows the delay of network under attack but without frequency hopping (FH). The transmission delay of the suffering attack network to resist the attack using the FHGM model is shown in Figure 6(c). The Figure 6(d) shows the contrast of delay in three scenes. The network suffer attack begin from 20th second in the simulation scene. As shown in Figure 6, the delay is great when network under attack. The transmission delay basically back to normal by applying the FHGM model. That fully proved that the effectiveness of FHGM model to resist the above specified attack.



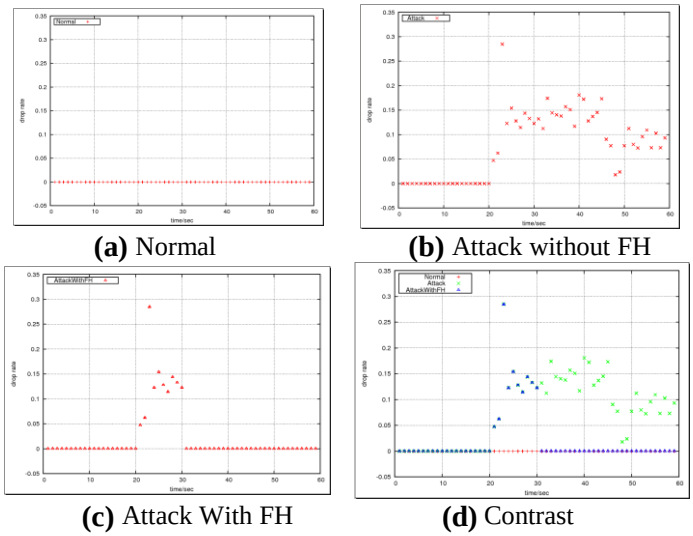
(a) Normal **(b)** Attack without FH

(c) Attack With FH **(d)** Contrast

Figure 6. Transmission Delay

4.2.2. Drop rate: The drop rate of the network is shown in Figure 7. The Figure 7(a) shows the drop rate of network in normal condition. The Figure 7(b) shows the drop rate of network under attack but without frequency hopping. The drop rate of the suffering attack network to resist the attack using the FHGM model is shown in Figure 7(c). The Figure 7(d) shows the

contrast of drop rate in three scenes. The network suffer attack begin from 20th second in the simulation scene. As shown in Figure 7, the drop rate when network under attack is higher than before suffering attack or after frequency hopping. The highest drop rate is up to 0.29. The drop rate basically back to normal by applying the FHGM model. The effectiveness of FHGM model to resist the above specified attack is fully proved.



(a) Normal **(b)** Attack without FH

(c) Attack With FH **(d)** Contrast

Figure 7. Drop Rate

4.2.3. Jitter: As shown in Figure 8, the jitter of the delay is larger when the network is under attack. The value of jitter is range from -2.4 to +2.3. Jitter, the greater also illustrates the instability of the network. Jitter back to normal level when using the FHGM model to resist attack.

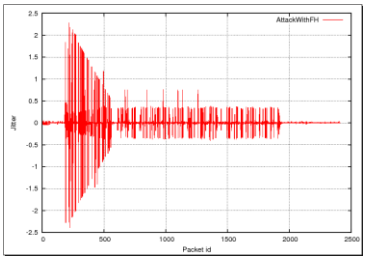


Figure 8. Jitter

5. Conclusions

This paper proposed a frequency hopping model based on incomplete information game. Firstly, some definitions and influencing factors in the frequency hopping game model are defined and described. Then the Frequency Hopping Game Model (FHGM) is modeled. The relevant influencing factors in the model are defined in formal and quantified. And this paper built a static Bayesian hopping game tree. Existence of Bayesian Nash equilibrium in the FHGM mode is subsequently proved. The Nash equilibrium plays an important decision role in the FHGM model. Finally, the FHGM model is verified through simulation and performance analysis. The FHGM model play important role in decision-making that is

proved and analyzed. The time to launch frequency hopping is more rational and more precision due to the payoff of in the FHGM model considers from the overall interests of the network. And the FHGM model is universal and adaptability.

Acknowledgements

This work was supported by "Funding Project for Academic Human Resources Development in Institutions of Higher Learning under the Jurisdiction of Beijing Municipality (PHR201007121)" , supported by "2012 Youth key Foundation of North China University of technology" and supported by "Beijing Natural Science Foundation (4132026)". The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

References

[1] P. H. J. Nardelli, "Efficiency of Wireless Networks under Different Hopping Strategies", IEEE Transactions on Wireless Communications, **(2012)**, pp. 15-20.
[2] Q. Wang, P. Xu, K. Ren and X. -Y. Li, "Towards Optimal Adaptive UFH-Based Anti-Jamming Wireless Communication", IEEE journal on selected areas in communication, vol. 30, no. 1, **(2012)**.
[3] L. Xiao, China H. Dai and P. Ning, "Jamming-Resistant Collaborative Broadcast Using Uncoordinated Frequency Hopping", IEEE Transactions on Information Forensics and Security, **(2012)**, pp. 297-309.
[4] J. Jeung, S. Jeong and J. Lim, "Adaptive rapid channel-hopping scheme mitigating smart jammer attacks in secure WLAN", The 2011 Military Communications Conference, **(2011)** November, pp. 1231-1236.
[5] A. Goetz, R. Rose, S. Zorn, G. Fischer and R. Weigel, "Performance of coherent time delay estimation techniques for frequency hopping GSM signals", Wireless Sensors and Sensor Networks (WiSNet), 2012 IEEE Topical Conference on, **(2012)** January 15-18, pp. 25-28.
[6] D. Fu, D. Feng and H. Zhang, "Mean LQI and RSSI based link evaluation algorithm and the application in frequency hopping mechanism in wireless sensor networks", 2011 International Conference on Consumer Electronics, Communications and Networks (CE CNet), **(2011)** April, pp. 3252-3257.
[7] F. Yang and L. -L. Yang, "Frequency-Hopping/M-Ary Frequency-Shift Keying Wireless Sensor Network Monitoring Multiple Source Events", Vehicular Technology Conference (VTC Spring), 2012 IEEE 75th, **(2012)** May 6-9, pp. 1-5.
[8] M. J. A. Rahman, M. Krunz and R. Erwin, "Out-of-band sensing scheme for dynamic frequency hopping in satellite communications", Communications (ICC), 2012 IEEE International Conference on, **(2012)** June 10-15, pp. 3234-3238.
[9] J. -S. Han, S. -H. Lee, H. -S. Kim and Y. -H. Lee, "Performance improvement of IEEE 802.15.4 in the presence of co-channel interference", 2011 IEEE Wireless Communications and Networking Conference (WCNC), **(2011)** March 28-31, pp. 49-54.
[10] P. Du and G. Roussos, "Adaptive time slotted channel hopping for wireless sensor networks", Computer Science and Electronic Engineering Conference (CEEC), **(2012)**, pp. 29-34.
[11] S. K. Singh, M. P. Singh and D. K. Singh, "Intrusion Detection Based Security Solution for Cluster-Based Wireless Sensor Networks", International Journal of Advanced Science and Technology, vol. 30, **(2011)** May, pp. 83-95.
[12] J. Xu, J. Wang, S. Xie, W. Chen and J. -U. Kim, "Study on Intrusion Detection Policy for Wireless Sensor Networks", International Journal of Security and Its Applications, vol. 7, no. 1, **(2013)** January, pp. 1-6.
[13] K. Sharma and M. K. Ghose, "Cross Layer Security Framework for Wireless Sensor Networks", International Journal of Security and Its Applications, vol. 5, no. 1, **(2011)** January, pp. 39-52.