I.J.Computer Network and Information Security, 2011, 5, 61-67
Published Online August 2011 in MECS (http://www.mecs-press.org/)

Split-Network in Wireless Sensor Network: Attack and Countermeasures

Chunlai Du Jianshun Zhang Li Ma
College of Information Engineering
North China University of Technology
Beijing, China
zhangjs0322@163.com

Abstract—**Wireless Sensor Network usually is deployed open environment to collect some sensitive information and has special features of its own are different from traditional network, which is vulnerable to internal and external attacks. Whole network can be split up into many separate subnets which cannot communicate with each other because some vital sensor nodes are attacked. This paper proposed an effective countermeasure based on ARMA prediction model and frequency hopping to react against split-network attack. ARMA model is used to evaluate the behavior of sensor nodes. Frequency hopping makes the communication frequency of the network escape from attack frequency. Then wireless sensor network is integrated into single network from split-network. Simulation results show the proposed countermeasure significantly reduces the success rate of split-network attack and increases the lifetime of network.**

Index Terms—Wireless Sensor Network, split-network attack, ARMA, frequency hopping, integrate

I. INTRODUCTION

When wireless sensor network (WSN) is deployed in a hostile environment, it is important to ensure network connectivity and security. Split-Network Attack (SNA) is to split the whole network into many separate subnets which cannot properly communicate with each other by attacking some vital nodes so that the collected data can not be uploaded to the monitoring center. SNA includes frequency interference attack, denial of service attack and sleep deprivation attack [1, 2]. Frequency interference attack interfere the vital node to receive the legitimate data at the same frequency. Denial of service attack make the vital node has no chance to receive the data from legitimate node. Sleep deprivation attack make vital nodes forward lots of data to exhaust their energy. Result of SNA is emergence of separate subnets. How to reduce the success rate of attack and how to fast reintegrate the separate subnets into a whole network are two questions. A defense scheme which based on frequency hopping and fast network integration was proposed to react against split-network attack. Frequency hopping makes the communication frequency of the network escape from attack frequency while fast network integration makes the separate subnets reintegrate into a whole network in new communication frequency. Simulation results show the proposed scheme significantly reduces the success rate of attack and increases the lifetime of network.

Funding Project for Academic Human Resources Development in Institutions of Higher Learning Under the Jurisdiction of Beijing Municipality. PHR201007121

The sections were organized as follows. Section Ⅱ shows the related work. Section Ⅲ describes the countermeasure to SNA including frequency hopping escape and fast network integration. Section Ⅳ shows the simulations results. Section Ⅴ is the conclusion and future work.

II. RELATED WORK

David [3] proposed a framework to mitigate the threats of Sleep deprivation attack, which includes Strong Link-Layer Authentication, Anti-Replay Protection, Jamming Identification and Mitigation and Broadcast Attack Protection. David [4] proposed mechanisms to detect and mitigate the effect of Sleep deprivation attack. Rainer Falk [5] proposed a secure wake-up scheme that entities of holding secret wake-up token can wake up a sleeping sensor node. Matthew [6] proposed three algorithms of cluster dead selection to make it much more difficult for the attacker to become cluster head. These algorithms greatly reduce the impact of the sleep deprivation attack. David [7] proposed a mechanism, Clustered Adaptive Rate Limiting (CARL), based on lightweight intrusion detection techniques to defeat Sleep deprivation attack.

Frequency interference attack is a physical layer attack for WSN. The common strategy against physical layer interference attack is spread spectrum communication. But the low-power, low-cost sensor nodes are usually limited to simple radio transceiver, spread spectrum technology can not directly applied in sensor nodes [8-14]. Aristides [8] introduced several strategies against frequency interference attack, Regulated Transmitted Power, FHSS, DSSS, Hybrid FHSS/DSSS [9], Ultra Wide Band Technology, Antenna Polarization, and Directional Transmission. In [8], Aristides emphasized and evaluated the advantages and disadvantages of each strategy, and

discussed some open issues about jamming attack. Mario [10] proposed Uncoordinated Frequency Hopping (UFH), a new spread-spectrum anti-jamming technique that does not rely on secret keys. MULEPRO (MULtichannel Exfiltration PROtocol) has been presented in [11]. The protocol is designed to rapidly exfiltrate sensor data from an attacked region to areas of the network that are not under attack. Xu [12-14] researched on radio interference attack and countermeasures.

Denial of service attack [15-17] can also cause paralysis of the vital nodes to form network segmentation.

Time series analysis [18-23] is a very effective short-term prediction method. Assumption the time series is a sample implementation of a random process. In statistics, signal processing, econometrics and mathematical finance, a time series is a sequence of data points, measured typically at successive times spaced at uniform time intervals. Time series analysis comprises methods for analyzing time series data in order to extract meaningful statistics and other characteristics of the data. Time series forecasting is the use of a model to forecast future events based on known past events to predict data points before they are measured. An example of time series forecasting in econometrics is predicting the opening price of a stock based on its past performance. A time series model will generally reflect the fact that observations close together in time will be more closely related than observations further apart. In addition, time series models will often make use of the natural one-way ordering of time so that values for a given period will be expressed as deriving in some way from past values, rather than from future values.

There are several types of data analysis available for time series [18-23] which are appropriate for different purposes. Simple or fully formed statistical models to describe the likely outcome of the time series in the immediate future, given knowledge of the most recent outcomes. Models for time series data can have many forms and represent different stochastic processes. When modeling variations in the level of a process, three broad classes of practical importance are the *autoregressive* (AR) models [19], the *integrated* (I) models, and the *moving average* (MA) [19] models. These three classes depend linearly on previous data points. Combinations of these ideas produce autoregressive moving average (ARMA) [19] and autoregressive integrated moving average (ARIMA) [19] models. In practice, the ARMA(p,q) model has great practical value because ARMA(p,q) model required to needs low order which are not exceed 2.

III. PROPOSED SCHEME

Frequency interference attack, denial of service attack and sleep deprivation attack make the some attacked vital nodes lose their abilities of forwarding data, so the whole network can be split up into many separate subnets which cannot communicate with each other. The collected data from sensor node may not be transmitted to the monitoring center due to unconnected wireless signal between attacked vital nodes.

We propose a scheme of frequency hopping escape and fast integration in a new frequency against SNA. Frequency hopping escape includes active escape and passive escape. Active escape which reduces the probability of attackers' finding the communication bandwidth is an active self-protection. It actively adjusts the frequency according to the preset rule. Passive escape hops the frequency according to the affected degree when nodes suffered from malicious attack. The most important of frequency hopping is consistency which includes frequency selection and frequency hopping time. The proper frequency hopping time is more important to ensure consistency and network connectivity. The frequency selection ensures that it is difficult for attackers to capture the selected new frequency.

This scheme consists of evaluation of behavior, negotiation of frequency hopping, synchronization of frequency hopping and integration of network. The following discussion based on clustering topology includes sink node, cluster head node, management node and cluster member node. The management nodes are mainly used for the management of frequency selection and frequency hopping time.

A. Evaluation of nodes' behavior based on ARMA model

Taking into account the wireless sensor network node resources, including nergy, computing power, storage capacity, communication bandwidth, are limited. This paper uses simple ARMA(p,q) model to analyze and predict traffic of wireless sensor network. ARMA model can effectively analyze the relevance of the smooth stationary data series and predict the data series. The ARMA (p, q) model, the greater the order of p and q, the greater the computation and the error is also large. Taking into account the limited resources of sensor nodes and real-time prediction, so in this paper uses a simple ARMA (1,1) model.

1) Smooth of traffic series

Assuming traffic series are $y_0,y_1,\ldots y_n$, where n is the sliding window size and yn is network traffic within a certain time interval. This traffic series may be non-stationary. But because ARMA model is smooth model, so these traffic series should be smooth. This paper get the logarithm of un-smooth traffic series, which is $LOG(y_0,y_1,\ldots y_n)$. Then $LOG(y_0,y_1,\ldots y_n)$ be processed using First-Order-Difference to get $Y_0,Y_1,\ldots Y_n$ are smooth series. Then ARMA model be established make use of the smooth traffic series to predict the n+1 traffic.

2) Modeling of traffic series

This section establishes ARMA model according to $Y_0, Y_1, \ldots Y_n$. This paper uses ARMA(1,1) model to predict future traffic. The form as equation (1):

$$Y_t = \varphi_1 Y_{t-1} + u_t - \theta_1 u_{t-1} \quad (1)$$

After introduction of lag operator L, the equivalent formula of (1) as equation (2):

$$\varphi(L) Y_i = \theta(L) u_i \quad (2)$$

In (2), L is lag operator. u_i , independent and identically distributed random variables, is white noise. Its expectation value is zero and variance value is σ_u^2 . $\varphi(L) = 1 - \varphi_1 L$, $\theta(L) = 1 - \theta_1 L$.

φ_1 and θ_1 are estimated parameters. Whether traffic series is smooth judged through the value of φ_1 and θ_1. Only when $|\varphi_1|<1$ and $|\theta_1|<1$, this series is smooth. Series can be predicted only to satisfy this condition.

3) Model Estimation and Prediction

This paper obtained estimated value $\hat{\varphi}_1$, $\hat{\theta}_1$ of estimated parameters φ_1 , θ_1 using the least square method. The conditions of smooth series are $|\varphi_1|<1$ and $|\theta_1|<1$. If this condition is met then the series is smooth series. The fitted model of ARMA (1,1) is as follows.

$$Y_t = \hat{\varphi}_1 Y_{t-1} + u_t - \hat{\theta}_1 u_{t-1} \quad (3)$$

The future traffic Y_t can be predicted according to the above prediction formula. The norm of prediction is to predict optimally, which means inaccuracy between predicted value and actual value as small as possible. The l-step prediction, $\hat{Y}_t(l)$ represent prediction value of Y_{t+l} when Y_t and Y_{t-1} have been known. The inaccuracy of l-step prediction can be described as $\varepsilon_t(l) = Y_{t+l} - \hat{Y}_t(l)$.

The more prediction steps, the greater variance of prediction inaccuracy. So this paper uses one step prediction. The confidence interval of this prediction is formula (4) which confidence level is 95%.

$$\hat{Y}_t(l) \pm 1.96 \sqrt{\left(1 + \sum_{j=1}^{l-1} \hat{\psi}_j^2\right)} \hat{\sigma}_u \quad (4)$$

In (4), ψ can be calculated using $\psi(L) = \varphi^{-1}(L)\theta(L)$. σ_u^2 represents the inaccuracy of white noise u.

4) Anomaly detection and evaluation

Model parameters are estimated making use of traffic series in lengthen of the sliding time window. ARMA (1, 1) is used in each sensor node to implement one step prediction to predict the next time traffic value. Comparison of the predicted traffic flow values and the actual value to check the inaccuracy of the two is in the confidence interval or not. When the inaccuracy is not in the confidence interval, the nodes may be suffered attack. T represents threshold. $\hat{Y}$ represents prediction traffic at certain time. Y represents actual traffic. The difference between the two denoted $D = \left|Y - \hat{Y}\right|$. When $D - \varepsilon_t(L) > T$, the current traffic is abnormal. So this node should send the Frequency Hopping request to its management node.

According to the received request, management node decides whether to start frequency hopping. If cluster head is suffering from attack, it immediately starts hopping consultation. When received the hopping request from cluster member nodes, management node evaluates the risk level, according to ratio of the number of hopping request node in the certain time slice to the total number of the nodes, to determine whether frequency hopping start. If only fewer nodes request frequency hopping, frequency hopping will not be start. When the number of frequency hopping request from cluster member node exceeds the threshold, management nodes start frequency hopping consultation.

B. Negotiation of frequency hopping

When frequency hopping consultation is started, management nodes will negotiate about next communication frequency and frequency hopping time. Consultations between the management nodes use the secret and not commonly used frequency. Thus, communication between the management nodes will not be interfered.

1) *Selection of communication frequency:* Next communication frequency use contribution mechanism described as below.

a) Each management node contributes a random number F_k and broadcast F_k to other management nodes.

b) Each management node receives these random numbers from other management nodes and then calculates the next communication channel F using (5):

$$F = \sum F_k \bmod 16 \quad (5)$$

c) If the communication channel F is equal with current communication channel, go to a).

2) *Selection of frequency hopping time:* to ensure synchronization of frequency hopping time, the process is described as below.

a) Management node i broadcast its hopping time T_i to other management nodes.

b) Each management node receives hopping time from other management nodes. Each management node calculates the true hopping time T according to the (6):

$$T= (\sum Ti - Tmin - Tmax)/(n-2) \quad (6)$$

In (6) T_{min} denotes minimum time, T_{max} denotes maximum time.

C. Synchronization of frequency hopping

When the hopping time arrives, each cluster begins frequency adjustment. Because of unreliability of wireless, synchronization of frequency hopping must be taken into consideration.

Management nodes send frequency hopping notification to its cluster member node, and then cluster member nodes acknowledge the notification. Management nodes according to the received responses determine whether all nodes in the cluster have received notification. If there are some nodes don't acknowledge the notification, management nodes resend the hopping notification within the tolerance. When beyond tolerance, the management nodes deem that those nodes have become dead node due to physical damage or energy depletion. Management nodes will abandon those nodes, and those nodes wait for next round to join the network. When the cluster member nodes received hopping notification, they will forward notification to the neighbor nodes to make up for the unreliability of the link between management nodes and member nodes.

D. Integration of network

There have two meanings about integration of network. One is maintaining the connection of whole network when it is attacked; the other one is integration of network after it was separated into subnets due to SNA.

For the former, WSN implement frequency hopping according to the evaluation of nodes' behavior. For the latter, there are two cases after frequency hopping shown as follows:

a) Each node executes the frequency hopping according to the negotiated next frequency and start time, and then communicates with each other.

b) Some nodes do not execute frequency hopping. If nodes have a good performance on section Ⅲ.C, the success rate of SNA is little. Taking into account wireless network congestion, time delay and packet loss, the member nodes may be not receives the frequency hopping notification all along. So after the frequency hopping network will form temporary separate subnets. The solution is described as follows.

a) The separated nodes first wait for a time slice to check whether there is arrival of delayed hopping notification. If there is arrival of notification, the node executes frequency hopping immediately;

b) If there no notification arrives all along, the node will select a frequency one by one from the communication channel pool in local to match the communication frequency. If the frequency is successful to be matched, the nodes communicate each other;

c) If the two solutions above are not feasible, the node will join the network as a new member of network.

IV. Simulation and Analysis

A. Simulation parameters

Experimental environment is Fedora12 and NS2.34. 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. There are three clusters in the scene shown in Fig. 1. 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 Fig.3. The other nodes are the cluster member nodes. Table Ⅰ.show the parameters used in the simulation.

B. Simulation parts

Simulation has been divided in three parts (i) No-Attack No-FH. In this part, the WSN is in the security environment having no attack, shown in Fig.2. (ii) Attack No-FH. WSN is suffered attack but have no countermeasures, shown in Fig.3. The small squares denote the drop packets in Fig.3. (iii) Attack with FH. Simulation is with malicious node and with Frequency Hopping, shown in Fig.4. When WSN starts frequency hopping the frequency changed from 2412e+6 to 2432e+6. This paper assumes the frequency of attacker is constant and FH execute only one time.

C. Simulation results and Analysis

This section includes 1) Jitter Analysis, 2) Delay Analysis and 3) Packet drop Analysis.

1) Jitter Analysis: Fig. 5 shows jitter under attack with Frequency Hopping. Network traffic is relatively small when WSN is not under attack, so the network has lower jitter. But when sensor network is under attack, network traffic is sharply increased and the network has higher jitter. When the network identified malicious node and changed the frequency to the security frequency, the jitter back to the lower jitter. Simulation shows the scheme

effectively defends against SNA, and it makes the network rapid escaping from communication channel interference and reduces the success ratio of SNA.

TABLE I. SIMULATION PARAMETERS

Parameter Name	Parameter Value
Channel Type	Channel/WirelessChannel
Radio Model	Propagation/TwoRayGround
PphyType	Phy/WirelessPhy
MacType	Mac/802_11
Queue Type	Queue/DropTail/PriQueue
Llink LlayerType	LL
AantType	Antenna/OmniAntenna
Max packet in ifq	50
Packet Size	512
Number of Nodes	20
Number of malicious nodes	1
Routing Protocol	AODV
Traffic Type	CBR
Topo Size	100*100 m

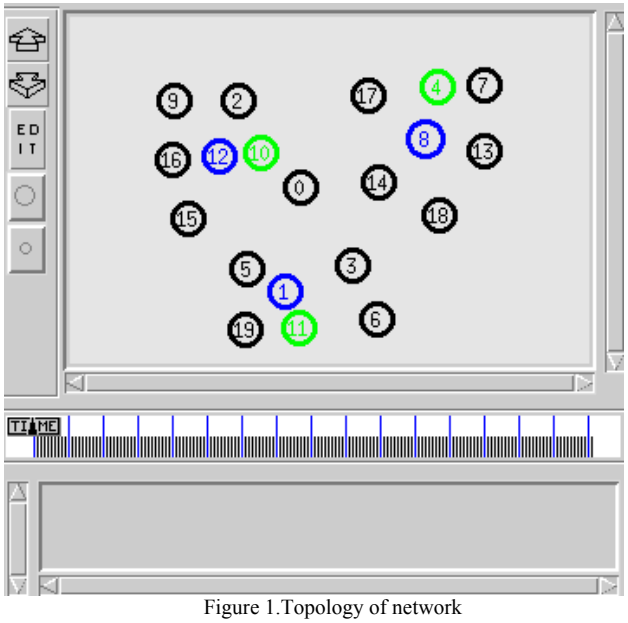

Figure 1.Topology of network

2) Delay Analysis: In Fig.6, ordinate denotes delay and abscissa denotes simulation time. When network traffic increases, it must lead to channel competition and will cause significant transmission delay. Network delay is relatively small when WSN is not under attack, but when WSN is under attack the delay increase sharply. When frequency hopping is applied to the network, the delay was back to the normal. The delay after hopping is less than under attack. Simulation results were shown in Fig.6.

3) Packet drop Analysis: In Fig.7, ordinate denotes drop rate and abscissa denotes simulation time. Attacker launches SNA and then causes packet drop. The rate of packet drop under these attacks is larger than not under attack. By means of the defense scheme on SNA, the rate of packet drop is normal. Simulation results were shown in Fig. 7.

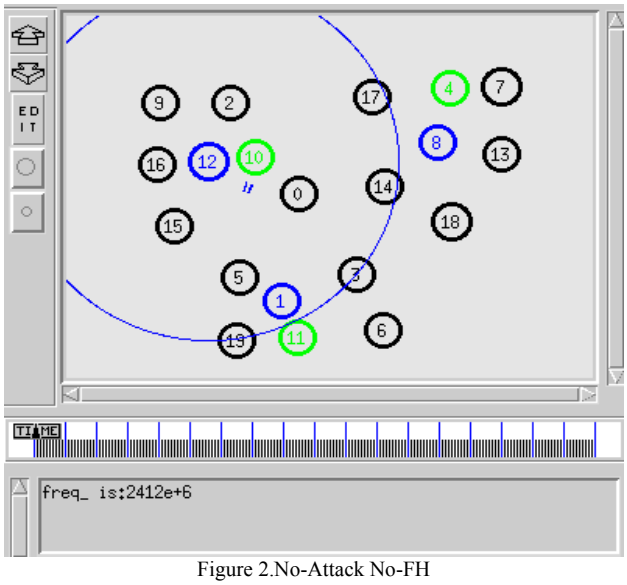

Figure 2.No-Attack No-FH

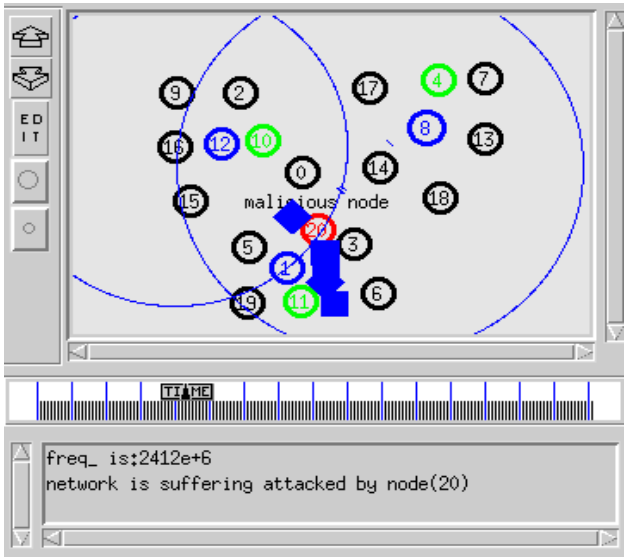

Figure 3.Attack No-FH

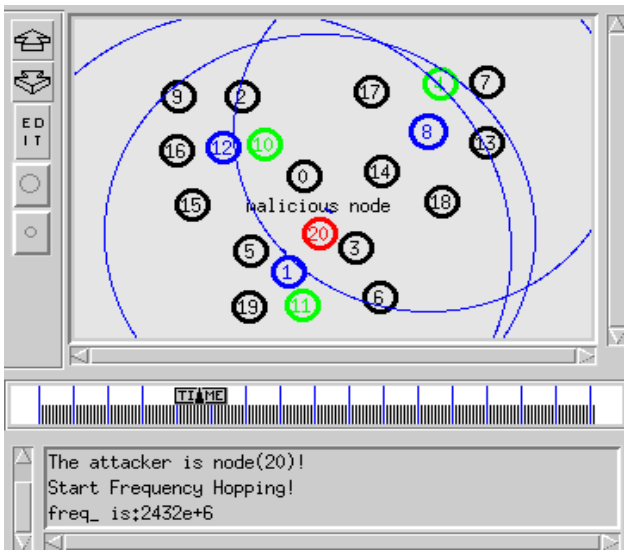

Figure 4.Attack with FH

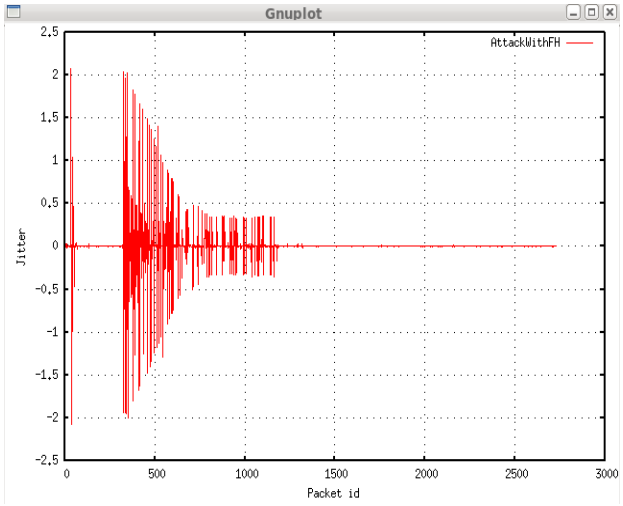

Figure 5.Jitter

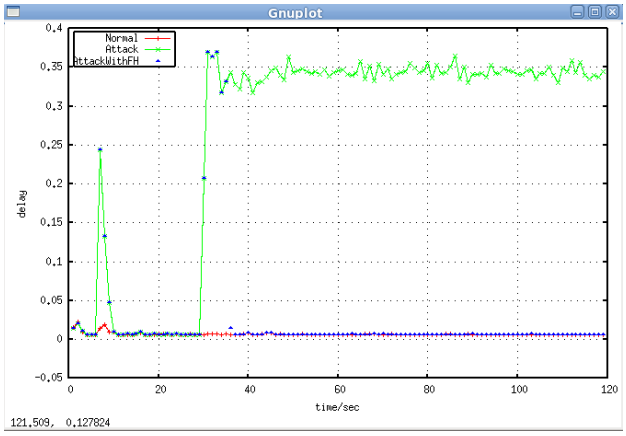

Figure 6.Transmission delay comparison

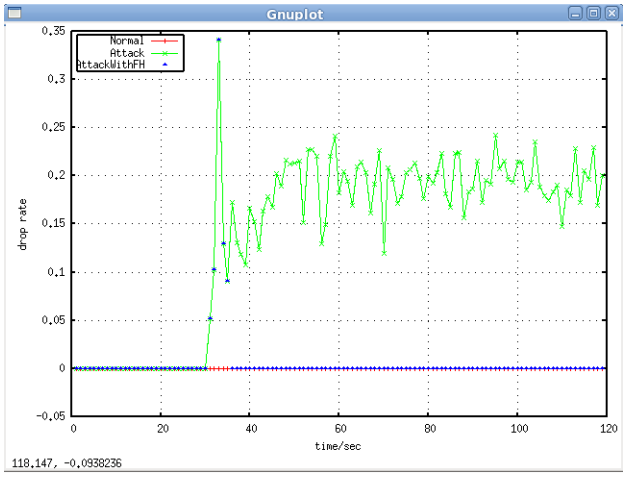

Figure 7.Drop rate comparison

V. CONCLUSION

In this paper we have proposed an effective countermeasure to defense split-network attack. This countermeasure consists of evaluation of behavior based on ARMA model, negotiation of frequency hopping, synchronization of frequency hopping and integration of network. The simulation results show the countermeasure effectively resists SNA, not only decreases the rate of packet drop but also reduces network delay and jitter. Through this way WSN will have good performances.

Future, more attentions will be paid to improve the accuracy of evaluation of behavior and optimization of frequency synchronization algorithm.

ACKNOWLEDGMENT

The authors would like to thank the reviewers, whose comments helped to improve this paper. This work was supported by “Funding Project for Academic Human Resources Development in Institutions of Higher Learning Under the Jurisdiction of Beijing Municipality”. And its number is PHR201007121.

REFERENCES

[1] Giruka, V. C., Singhal, M., Royalty, J. and Varanasi, S. (2008), Security in wireless sensor networks. Wireless Communications and Mobile Computing, 8: 1–24. doi: 10.1002/wcm.42

[2] Kashif Kifayat, Madjid Merabti, Qi Shi and David Llewellyn-Jones, Security in Wireless Sensor Networks. Handbook of Information and Communication Security, 2010, Part E, 513-552, DOI:10.1007/978-3-642-04117-4_26

[3] Raymond,D.R.Marchany,R.C.Brownfield,M.I.Midkiff, S.F, ”Effects of Denial-of-Sleep Attacks on Wireless Sensor Network MAC Protocols”,*Vehicular Technology, IEEE Transactions on* On page(s): 367 – 380, Volume: 58 Issue: 1, Jan. 2009

[4] David Richard Raymond,”Denial-of-Sleep Vulnerabilities and Defenses in Wireless Sensor Network MAC Protocols”, Dissertation, Virginia Polytechnic Institute and State University, 2008

[5] Rainer Falk, Hans-Joachim Hof, "Fighting Insomnia: A Secure Wake-Up Scheme for Wireless Sensor Networks," securware, pp.191-196, 2009 Third International Conference on Emerging Security Information, Systems and Technologies, 2009

[6] MatthewPirretti,SencunZhu, N.Vijaykrishnan,Patrick McDaniel, Mahmut Kandemir and Richard Brooks, ”The Sleep Deprivation Attack in Sensor Networks: Analysis and Methods of Defense “in International Journal of Distributed Sensor Networks, Volume 2, Issue 3 September 2006, pages 267 - 287

[7] David R. Raymond and Scott F. Midkiff, “Clustered Adaptive Rate Limiting: Defeating Denial-of-Sleep Attacks in Wireless Sensor Networks” in Military Communications Conference 2007, MILCOM, IEEE, pages -1-7.

[8] Aristides Mpitziopoulos et al..”A Survey on Jamming Attacks and Countermeasures in WSNs”, IEEE COMMUNICATIONS SURVEYS&TUTORIALS, VOL. 11, NO. 4, FOURTH QUARTER 2009

[9] Mpitziopoulos,A.and Gavalas, D.(2009),”An effective defensive node against jamming attacks in sensor networks”. Security and Communication Networks,2:145–163.doi: 10.1002/sec.81

[10] M.Strasser,C. Popper, and S. Capkun, "Efficient Uncoordinated FHSS Anti-jamming Communication," Proceedings of the tenth ACM International Symposium on Mobile Ad Hoc Networking and Computing, pages 207-218, 2009.

[11] Ghada Alnifie, Robert Simon,"A multi-channel defense against jamming attacks in wireless sensor networks", Proceedings of the 3rd ACM workshop on QoS and security for wireless and mobile networks, October 22-22, 2007, Chania, Crete Island, Greece

[12] W. Xu, W. Trappe and Y. Zhang, "Channel surfing: defending wireless sensor networks from interference", in Proc. 6th international conference on Information processing in sensor networks, New York, NY, USA, pages.499-508, 2007.

[13] W. Xu, K. Ma, W. Trappe, Y. Zhang, "Jamming sensor networks: attack and defense strategies", IEEE Network Magazine,vol. 20, pages. 41-47,2006.

[14] WENYUAN XU, WADE TRAPPE and YANYONG ZHANG, "Defending wireless sensor networks from radio interference through channel adaptation" in ACM Transactions on Sensor Network, Vol. 4, No. 4, Article 18, Publication date: August 2008

[15] Khusvinder Gill and Shuang-Hua Yang, "A Scheme for Preventing Denial of Service Attacks on Wireless Sensor Networks" in Industrial Electronics, 2009. IECON '09. 35th Annual Conference of IEEE, Identifier: 10.1109/IECON.2009.5415233, pages: 2603 - 2609

[16] Pelechrinis,K; Iliofotou,M; Krishnamurthy,V., "Denial of Service Attacks in Wireless Networks:The Case of Jammers", in Communications Surveys & Tutorials of IEEE, Issue: 99, Identifier: 10.1109/SURV.2011.041110.00022, pages:1-13

[17] Raymond, D.R.; Midkiff, S.F.; "Denial-of-service in wireless sensor networks:Attacks and defenses", Pervasive Computing, IEEE, Vol: 7 , Issue: 1, Identifier: 10.1109/MPRV.2008.6, pages: 74 – 81

[18] http://en.wikipedia.org/wiki/Linear_regression

[19] Damodar N.Gujarati, Basic Econometrics, China Renmin University Press,2005

[20] Li Baoren, Econometrics, China Machine Press,2008

[21] Tong Guangrong, ECONOMETRICS, WUHAN UNIVERSITY PRESS, 2006

[22] Mehmet Celenk, Thomas Conley, James Graham, and John Willis, "Anomaly prediction in network traffic using adaptive Wiener filtering and ARMA modeling", *2008 IEEE International Conference on Systems, Man and Cybernetics (SMC 2008)*,pages:3548-3553,2008

[23] Mehmet Celenk, Thomas Conley, John Willis, *James Graham*,"Predictive Network Anomaly Detection and Visualization", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 5, NO. 2, JUNE 2010

Chunlai Du is a lecturer of North China University of Technology in Beijing of China. His research interests include network and information security, mobile ad hoc networks, wireless sensor works, embedded system and information process. He is member of ACM and China Computer Federation.

Jianshun Zhang is a master of North China University of Technology in Beijing of China. His research interests include wireless sensor works, embedded system and information process. He is student member of ACM and China Computer Federation.

Li Ma is a professor of North China University of Technology in Beijing of China. His research interests include high performance computing, wireless sensor works, embedded system and information process. He is a member of ACM, IEEE and senior member of China Computer Federation. And he is special committee members of CCF information storage and education

