Journal of Theoretical and Applied Information Technology
28th February 2014. Vol. 60 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

S-ARMA MODEL FOR NETWORK TRAFFIC PREDICTION IN WIRELESS SENSOR NETWORKS

S.PERIYANAYAGI[1], Dr.V.SUMATHY[2]
[1]Assistant Professor, Department of ECE
Angel College of Engineering and Technology,Tirupur
[2]Associate Professor, Department of ECE
Government College of Technology
E-mail: [1]periyanayagiphd@gmail.com

ABSTRACT

Future network traffic in WSN can be predicted by time series models. The knowledge of traffic can be used for routing, load balancing and QoS provisioning. S-ARMA model has been proposed to predict the future traffic in WSN.The abnormality in traffic is predicted and it indicates the possibility for Dos attack and it initiates frequency hopping to avoid this. Increase in the frequency hopping time is identified by S-ARMA model, alerts the network to avoid the anomaly channel. Effectiveness of this model is been proved to be efficient in detecting the anomaly channel from the simulation results since the information about the attackers in the channel can be known using swarm intelligence (ants).

Keywords: *S-ARMA, Network Traffic, Frequency Hopping, Swarm Intelligence*

1. INTRODUCTION

In Network technology, measure of Network Traffic improves the efficiency of communication network .The knowledge of traffic can be used in routing, load balancing and QoS provisioning. The accurate prediction of network traffic is the prerequisite for network management. Therefore, the network traffic prediction becomes the key in the research areas. Traditional network traffic prediction models are linear regression model, Poisson model, Markov models and time series forecasting model, since the network traffic data is essentially a time series, time series model is the most commonly used network traffic prediction model among the traditional models. In the earliest work, network traffic prediction models use linear time series models, e.g. Auto Regressive Moving Average (ARMA) and Auto Regressive Integrated Moving Average (ARIMA) [2][7].

In this paper, Time series S-ARMA model is proposed to predict the network traffic in future using Swarm intelligence Auto Regressive Moving Average (S-ARMA). This model estimates the difference in actual and predicted traffic, based on the inaccuracy of traffic, Frequency hopping is initiated. Frequency hopping time is calculated and the information about each channel in the network is collected by swarm intelligence technique. S-ARMA model alerts the network to avoid the particular channel which is affected by DoS attack, based on inaccuracy of network traffic and frequency hopping time in wireless sensor networks [9][13].

The rest of this paper is organized as follows. Section 2 discusses related work in the area of network traffic prediction, section 3explores S-ARMA modeling, traffic prediction model based on future traffic and it provides a frame work for attacker mitigation using swarm intelligence. Section 4 validates this technique is effective in predicting Network traffic and anomaly detection. Finally Section 5 offers conclusions.

2. RELATED WORK

Chen Chen et al [1] have proposed a scheme to identify fake schedule switch with RSSI measurement which successfully defends the collision, exhaustion, broadcast and jamming attacks. The attacker with more battery power will be involved in the network for long time and disturbs the transmission.

Chunlai Du et al [2] have proposed an effective countermeasure based on ARMA prediction model and frequency hopping to react against split-network attack. proposed scheme while integration of network it needs time synchronization and two different solutions are given which are not feasible

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

if the node receives the communication frequency after a long time.

Mehmet Celenk, Thomas Conley, James Graham [7] have proposed a method of anomaly detection based on weiner filtering of noise followed by ARMA modeling of network flow data. Anomaly prediction using ARMA model and weiner filtering uses diverse feature set to detect signatures of complex anomalies. This reduces system accuracy and reliability.

Mehmet Celenk, Thomas Conley, John Willis [6] proposed an approach that uses short-term observations of network features and their respective time averaged entropies. Acute changes are localized in network feature space using adaptive Wiener filtering and auto-regressive moving average modeling.

Dingding Zhou,Songling Chen ,Shi Dong[4] have proposed a network traffic prediction based on ARFIMA modeling is a time series forecasting model, which is an improved ARMA model, deeply study on ARFIMA model and adopts ARFIMA model to predict real trace records and net flow sampling flow records.

David R. Raymond et al [3] have presented three contributions to the area of sensor network security. Proposes a framework for defending against denial-of- sleep attacks and provides four leading WSN MAC protocols techniques that can be used against each denial-of-sleep vulnerability. It provides a frame work for preventing DoS attack with full protocol knowledge.

Thomas Martin, et al [15] and Matthew Pirretti et al [5] have described sleep deprivation attacks on general-purpose battery-powered computing devices. Three methods have been proposed for mitigating this attack. This scheme requires that each sensor node must maintain a list indicating which nodes are in its cluster at all times.

S. Qureshi, A. Asar, A. Rehman, and A. Baseer [12] proposed an algorithm to Detect Malicious Beacon Nodes based on swarm intelligent water drop to provide Secure Localization in Wireless Sensor Networks. The method proposed based on swarm intelligence does not detect Denial of Sleep attack in WSN.

Muhammad Saleem Gianni A. Di Caro, and Muddassar Farooq[10] provides an extensive survey of network routing protocols which are developed using the principle of swarm intelligence and its application to routing has been discussed.

3. S-ARMA MODEL

A defense technique for anomaly detection based upon the future Network traffic prediction using S-ARMA model is proposed in this paper. Initially, ARMA (p,q) model analyze and predicts the future traffic in wireless sensor network. If the order of p and q are increased, the computation and error also increased in ARMA (p,q) model. So S-ARMA model proposed uses a simple ARMA (1,1) model and future network traffic abnormality is predicted using swarm intelligence. It estimates the difference in actual and predicted traffic. If the difference is above a threshold value, the current traffic is abnormal and the node requests for frequency hopping. The number of nodes requesting for the frequency hopping is identified and if it is below a threshold value, then the frequency hopping is not initiated.

Swarm intelligence is a kind of communication system which communicates directly or indirectly with the channels using a distributed approach. This follows the behavior of a group of social insects, namely ant, birds, etc for communication. The ant agents which are placed randomly in a network have three features Pheromone Level, Transition Probability and the Tabu-Lists. In order to make the trial of other ants easier, each ant deposits a chemical substance known as pheromone. Swarm intelligence follows the same procedure as these ants. Two mobile agents called Forward Ant (FA) and Backward Ant (BA) which are similar in structure but different in the type of work they perform, are used [11].

In S-ARMA model, the nodes are assigned separate channels. The source node which initiates the request will be considered as Administrator node. The administrator node sends its communication frequency and the frequency hopping time through the forward ants during the route discovery. The forward ants collect the information from all the nodes and when it reaches the destination, the collected frequency hopping time is verified. The Node having a frequency hopping time greater than the threshold is identified as a node with fault channel. This information is sent to the administrator node through the backward ants. Administrator node obtains the information and omits the node with fault channel from the network and transmits the data through remaining channels. This technique proves to be efficient in detecting the faulty channel and consumes less energy since the information about all the attackers is known using S-ARMA model.

Journal of Theoretical and Applied Information Technology
28th February 2014. Vol. 60 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Taxonomy in Route Discovery

Route discovery is responsible for generating all possible routes between source and destination. control packet is used to discover the routes. The control packets are nothing but mobile agents which walk through the network to establish routes between nodes. In S-ARMA model, FAs either unicast or broadcast the node's channel information. The channel information's like frequency hopping time H_T and Pair wise Key E_{KS} are collected by FAs and chooses the next hop based on the pheromone value. The pheromone value is calculated by Equation 1,

$$\sigma_{i,j,d}(a) = (\sigma_{i,j,d}(a-1)) + \frac{\chi}{C_{fre} \cdot en} \quad (1)$$

Where,

ϑ - Trail memory [11],

χ - Arbitrary parameter,

C_{fre} - channel frequency

en - Energy of an ant

The DoS attack is identified by intruder mitigation algorithm based on S-ARMA model and is given in Figure 1.

Begin
{
Step 1: The forward ant collects the pair wise shared key $E_{ks}(i)$ from all the nodes and computes the next communication channel C [16]

$$C = \{ E_{ks}(i) \bmod 16 \}, i \geq 0$$

Step 2: Check whether the next communication channel and the current communication channel (C) are the same.
Step 3: If they are same, then the administrator node again sends the information to the next channel via forward ants in the similar manner.
Step 4: Each node calculates the true frequency hopping time H_T and the forward ants collects it. The true hopping time is calculated as

$$H_T = (\Sigma Ti - HT_{min} - HT_{max}) / (n-2)$$

Where HT_{min} denotes minimum hopping time, HT_{max} denotes maximum hopping time.
Step 5: When the FA reaches the end of the channel, it is de-allocated and the backward ant (BA) inherits the stack contained in the FA.
Step 6: The BA is sent out on high priority queue. The backward ants retrace the path of the FA and utilize this information to update the data structures periodically.
Step 7: The frequency hopping time collected is verified and prevalence of attacker for long time in the channel is identified by the administrator node.
Step 8: Each node maintains a true hopping time H_T and when this time exceeds the threshold value η then it is assumed that the attacker is prevailed in the channel for longer time.
Step 9: When the source receives this information then it omits the channel containing an attacker. Simultaneously the forward ants are sent through other channels which are not detected before for attacks.
End
}

Figure 1: Intruder mitigation algorithm

Routing between the administrator node A and the destination node D is shown in figure 2, the administrator node A sends the frequency hopping time Ti to all the nodes through the forward ants. The forward ants collect the H_T value from all the nodes and send it to the destination. The Hopping time of each channel is as follows, H_T value of C1 as 4, H_T value of C2 as 9, H_T value of C3 as 8, H_T value of C4 as 5, and H_T value of C5 as 6. The H_T which is above the threshold value η is considered to be an attacker.

The frequency hopping time is calculated based on the pair wise key $E_{ks.}$The pair wise key generation method [16](Pseudo Noise Sequence-PN sequence) is unknown to the attacker. So it calculates the frequency hopping time incorrectly.

The η value considered here is 8. The channel 2 has a H_T value of 9 and is considered as a attacker node with fault channel. The information about the Fault channel (FC) is sent to the Administrator node through the backward ants. Once the administrator node receives this information, it omits the fault channel. Here the fault channel C2 is deleted and the data is transmitted through A–C1-C3- C4- C5-D.

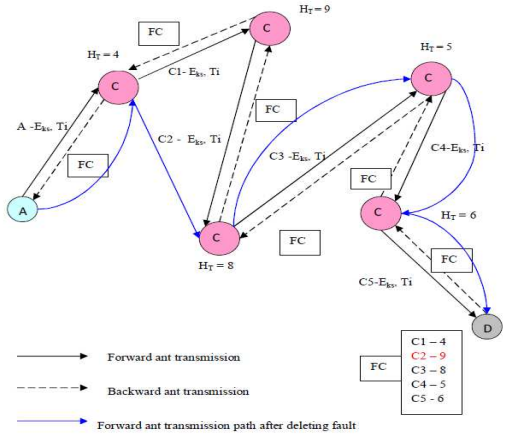


Figure 2: Frequency Hopping Technique using swarm Intelligence

Journal of Theoretical and Applied Information Technology
28th February 2014. Vol. 60 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3.1 Traffic Prediction Model

Time series analysis is a very effective short term Network traffic prediction method**.** Models for time series data of a stochastic process are classified into three broad categories Autoregressive(AR) models, Moving Average (MA) models and combination of two forms Autoregressive-moving-average ARMA models. The Network traffic can be represented by a continuous-time stochastic process

$$y(t) = x(t)+\mu, \quad (2)$$

Where

μ = mean rate,

x (t) = random process.

Swarm intelligence Auto Regressive-Moving-Average (S-ARMA) is a model of autocorrelation, in time series. S-ARMA models are widely used in hydrology, dendrochronology, econometrics, and Network traffic prediction. It can be used to predict the behavior of a time series from past values. Such prediction is used as a baseline to calculate the future traffic values.

S-ARMA (p,q) model for the traffic series $\{T_t\}$ in regression form is given by

$$T_t - \varphi_1 T_{t-1} - \ldots - \varphi_p T_{t-p} = w_t + \theta_1 w_{t-1} + \ldots + \theta_p w_{t-q} \quad (3)$$

Where

$w_t \sim WN(0,\sigma^2)$ White noise with zero mean

σ^2 - variance.

S-ARMA model starts the process of estimation by calculating the auto-correlation function for T_t using Yule walker equation in matrix form for S-ARMA(p,q) model is given below

$$\begin{pmatrix} R_{Tt}[q] & R_{Tt}[q-1] & \cdots & R_{Tt}[q-p+1] \\ R_{Tt}[q+1] & R_{Tt}[q] & \cdots & R_{Tt}[q-p+2] \\ \vdots & \vdots & \ddots & \vdots \\ R_{Tt}[q+p-1] & R_{Tt}[q+p-2] & & R_{Tt}[q] \end{pmatrix} \begin{pmatrix} \varphi_1 \\ \varphi_2 \\ \vdots \\ \varphi_p \end{pmatrix} = \begin{pmatrix} R_{Tt}[q+1] \\ R_{Tt}[q+2] \\ \vdots \\ R_{Tt}[q+p] \end{pmatrix}$$

In this paper, S-ARMA (1,1) model is used to predict the future traffic. If T_0 , T_1,T_2 …….T_n is the traffic series

$$T_t = \varphi_1 T_{t-1} + w_t + \theta_1 w_{t-1} \quad (4)$$

Introducing Lag parameter (or) Backshift operator in equation (4)

$$\varphi(L)T_t = \theta(L)\, w_t$$

where

$\varphi(L) = 1 - \varphi_1 L$

$\theta(L) = 1 + \theta_1 L$

φ_1 and θ_1 are traffic prediction parameters.

The auto-correlation function for T_t is given by

$$R_{Tt}(q+1) = \varphi_1 R_{Tt}(q) \quad (5)$$

Auto correlation function (ACF) for S- ARMA (1,1) model is given by

$$R_{Tt}(1) = \frac{(\varphi+\theta)(1+\varphi\theta)}{(1+\theta^2+2\varphi\theta)}$$

$R_{Tt}(k) = \varphi R_{Tt}(k-1)$, for k > 1

Stationary condition: $|\varphi|< 1$

Invertability condition: $|\theta|< 1$

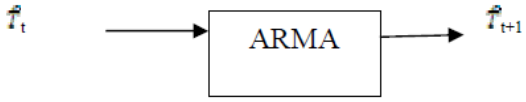
The traffic values are predicted by the values of φ_1 and θ_1. Only when $|\varphi_1|< 1$ and $|\theta_1|< 1$ the traffic series is smooth. If this condition is satisfied traffic time series can be predicted.

The future traffic is predicted according to the prediction formula

$$T_t = \hat{\varphi}_1 T_{t-1} + w_t + \hat{\theta}_1 w_{t-1} \quad (6)$$

Where $\hat{\varphi}_1$ and $\hat{\theta}_1$ are estimated from φ_1 and θ_1 using least square method.

The 1-step prediction, predicts the value of T_{t+1} when T_t and T_{t-1} are known



The prediction error (or) inaccuracy of 1 step prediction is described by

$$\varepsilon_{Tt} = T_{t+1} - \hat{T}_{t+} \quad (7)$$

where $\hat{T}_{t+1}$ → represents prediction values of T_{t+1} when T_t and T_{t-1} are known.

The confidence interval [6] of this 1 step prediction is 95 %.($\varepsilon_{Tt} = 0.01$)

3.2 Traffic Prediction model based Intruder Detection

The prediction traffic flow values and the actual value are compared to check the inaccuracy of the two whether they are in the confidence level or not. The nodes subjected to attack when it is not in the confidence interval. T_P represents prediction traffic at certain time and T_A represents actual traffic. The difference between two is denoted as

$$F = |T_A - T_P| \quad (8)$$

Let P represents the threshold value.

When $F - \varepsilon_{Tt} > P$. The current traffic is abnormal.

So this node should send the Frequency hopping time request to administrator node.

Administrator node is responsible for initiating the frequency hopping technique.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

When a channel of a node suffers from an attack, it immediately starts hopping consultation. When administrator node receives the hopping request from the attacker node, it evaluates the risk level, according to the ratio of the number of hopping request nodes to the total number of the nodes, to determine whether frequency hopping should start or not.

If only fewer nodes request frequency hopping, frequency hopping will not be started. When the number of frequency hopping request from the member node exceeds the threshold, administrator nodes start frequency hopping using the communication frequency and frequency hopping time estimation. The administrator nodes obtains frequency hopping request from most of the nodes and thus starts the frequency hopping process. Intruder mitigation algorithm is applied to identify the DoS attack and thus S-ARMA model alerts the network about the fault channel.

4. PERFORMANCE ANALYSIS

4.1 Simulation Parameters

The IEEE 802.15.4 MAC layer is used for communication among the nodes; it provides access to the physical channel of all types of transmissions and appropriate security mechanisms. IEEE 802.15.4 provides 16 channels separated by 5 MHz [11]. The IEEE 802.15.4 Zigbee supports Frequency Hopping Spread Spectrum (FHSS) options. It adopts the same basic frame structure for low-duty-cycle, low-power operation and different frequency bands: low-band (868/915 MHz) and high band (2.4 GHz). The PHY layer uses a common frame structure, containing a 32-bit preamble frame length.

The simulation settings and parameters are summarized in table.

No. of Nodes	50
Area Size	750 X 750
Mac	IEEE 802.15.4
Transmission Range	40m
Simulation Time	10,20,30,40 and 50 sec
Traffic Source	CBR
Packet Size	512
Sources	4
Attackers	2
Rate	50kbps to 250kbps

4.2 Performance Metrics

The proposed S-ARMA model for Network traffic prediction is compared with existing ARMA model for Split network [2]. The performance is evaluated mainly, according to the following metrics.

- **Packet Delivery Ratio:** It is the ratio between the number of packets received and the number of packets sent.
- **Packet Drop**: It refers the average number of packets dropped during the transmission
- **Overhead**: It is the number of control packets exchanged between the source and destination for detection of nodes with faulty channel.

4.3 Results

Simulation results are presented and discussed in this section. Graph shows the average of multiple runs for a given set of parameters values. The parameter values evaluated for performance metric are summarized in the Table 1.

Table 1: Parameter values evaluated

Parameter	Values
Packet Transmission Rate	50,100, ,250 Kbps
Packet Delivery Ratio	0,0.2, … , 0.8
Packet Drop	0,400, ,16000 pkts
Overhead	0,10000, ..,30000 pkts

4.3.1 Packet Transmission Rate Vs Packet Delivery Ratio

In Figure 3, depicts packet transmission rate Vs packet delivery ratio is depicted for S-ARMA model and Existing ARMA model. The packet delivery ratio in S-ARMA model is increased by 28% compared to ARMA model. At a rate of 200 kbps, improvement in packet delivery ratio is less ie. Only 20% is achieved due to more number of faulty channels in the network.

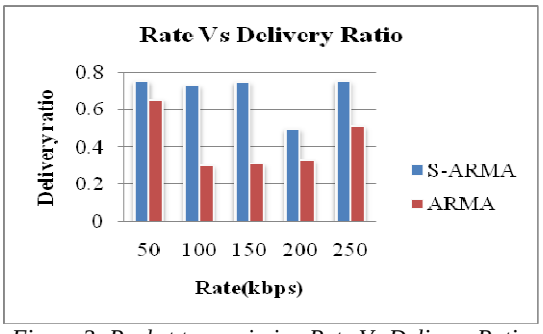


Figure 3: Packet transmission Rate Vs Delivery Ratio

4.3.2 Packet Transmission Rate Vs Packet Drop

The Packet drop with the transmission rate varying from 50 to 250 Kbps is illustrated in Figure 4. Number of packet drop in S-ARMA is reduced

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

by 67% compared to ARMA model. The reduction in packet drop is less at 200 Kbps ie. about 30% due to increased in frequency hopping time. Number of packet drop increases linearly with the packet transmission rate. S-ARMA model detects malicious nodes which improves the performance of transmission both at lower rates (50 kbps) and at higher rates (250 kbps).

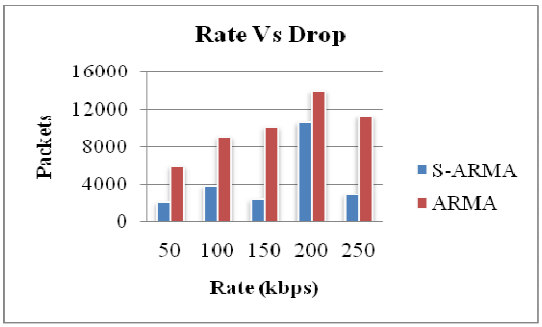


Figure 4: Packet Transmission Rate Vs Packet Drop

4.3.3 Packet Transmission Rate Vs overhead

The performance of S-ARMA and ARMA model is evaluated in Figure 5 based on transmission rate Vs Overhead as shown. S-ARMA model achieves 43% reduction in overhead compared to ARMA model. At a transmission rate of 100 kbps, number of control packets exchanged between Administrator node and destination node in S-ARMA model is approximately same as control packets exchanged between management nodes in ARMA model for split network due to more number of attacker mitigation.

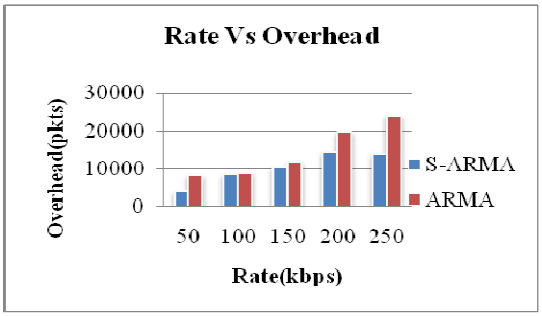


Figure 5: Packet Transmission Rate Vs Overhead

The simulation results revels that S-ARMA model improves the performance of the intruder detection algorithm.

5. CONCLUSION AND FUTURE WORK

A Time series S-ARMA model for Network traffic prediction has been proposed. Initially traffic prediction model detects the inaccuracy in the network traffic based on the actual and predicted traffic values. If the difference is above a threshold value, current traffic is abnormal and the node sends frequency hopping request to the Administrator node. When administrator node receives the hopping request from the attacker node, it evaluates the risk level and it initiates the frequency hopping based on the number of nodes requesting hopping. Intruder mitigation algorithm proposed identifies the nodes with faulty channel and alerts the network to avoid the anomaly channel. The Effectiveness of S-ARMA model has been evaluated from the simulation results and performance metrics of S-ARMA model is better than existing ARMA model for split networks.

In future, A Swarm based mitigation algorithm for capture and tampering attack in IEEE 802.15.4 based Wireless Networks has been planned to develop using specific mechanism which improves the performance of WSN.

REFERENCES

[1] Chen Chen,Li Hui,Qingqi Pei,Lv Ning, and Peng Qingquan,(2009), "An Effective Scheme for Defending Denial-of-Sleep Attack in Wireless Sensor Networks", *Fifth International Conference on Information Assurance and Security*, pp 446 – 449.

[2] Chunlai Du Jianshun Zhang Li Ma (2011), "Split-Network in Wireless Sensor Network:Attack and Countermeasures" *I.J.Computer Network and Information Security*, vol 5, pp 61-67.

[3] David R. Raymond, Randy C. Marchany, Michael I. Brownfield, and Scott F. Midkiff (2009), "Effects of Denial-of-Sleep Attacks on Wireless Sensor Network MAC Protocols" *IEEE Transactions on Vehicular Technology*, Vol. 58, No. 1, pp 367 - 380.

[4] Dingding Zhou,Songling Chen ,Shi Dong (2012),"Network traffic prediction based on ARFIMA model" ,*IJCSI International Journal of Computer Science Issues*, Vol. 9,Issue 6, No 3,pp 106 – 111.

[5] Matthew Pirretti, Sencun Zhu, Richard Brooksand Vijaykrishnan Narayanan (2006),"The Sleep Deprivation Attack in Sensor Networks: Analysis and Methods of Defense", *International journal of distributed sensors*, Vol 2 ,No 3,pp267 -287.

[6] Mehmet Celenk, Thomas Conley, John Willis, James Graham (2010),"Predictive Network Anomaly Detection and Visualization", *IEEE*

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Transactions on Information forensics and security, vol. 5, No. 2,pp 288 – 299.

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

[8] Brownfield, Yatharth Gupta, and Nathaniel Davis (2005), "Wireless Sensor Network Denial of Sleep Attack", *Proceedings of the 2005 IEEE Workshop on Information Assurance*, pp 356 - 364.

[9] Michael Krishna (2006),"Intrusion Detection in Wireless Sensor Networks",pp 1 – 7.

[10] Muhammad Saleem Gianni A. Di Caro, and Muddassar Farooq (2011), "Swarm intelligence based routing protocol for wireless sensor networks: Survey and future directions",*Journal information sciences: an international journal archieve*, Vol 181 Issue 20,pp 1 - 28.

[11] S.Periyanayagi and Dr.V.Sumathy (2011), "A Swarm Based Defense Technique for Jamming Attacks in Wireless Sensor Networks", *IJCTE: International journal of computer theory and engineering*,Vol 3 issue 6, pp 816 – 821.

[12] S. Qureshi, A. Asar, A. Rehman, and A. Baseer, (2011),"Swarm Intelligence based Detection of Malicious Beacon Node for Secure Localization in Wireless Sensor Networks" *Journal of Emerging Trends in Engineering and Applied Sciences (JETEAS) 2 (4) Scholarlink Research Institute Journals*, (ISSN: 2141-7016) ,pp 664-672.

[13] Shivangi Raman, Amar Prakash, Kishore Babu Pulla, and Prateek Srivastava,(2010), "Wireless sensor networks: A Survey of Intrusions and their Explored Remedies" *International Journal of Engineering Science and Technology* Vol. 2(5), pp 962-969.

[14] Tapalina Bhattasali, Rituparna Chaki, and Sugata Sanyal (2012), "Sleep Deprivation Attack Detection in Wireless Sensor Network", *International Journal of Computer Applications* (0975 – 8887) Vol 40 No.15,pp 19 - 25.

[15] Thomas Martin, Michael Hsiao, Dong Ha, and Jayan Krishnaswami,(2004), "Denial-of-Service Attacks on Battery-powered Mobile Computers", *Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications* (PERCOM'04),ISBN:0-7695-2090-1,pp 309-318.

[16] Wood.A.D, J.A. Stankovic, and G. Zhou.(2007), "DEEJAM: Defeating energy-efficient jamming in IEEE 802.15.4-based wireless networks". *In IEEE Proceeding of SECON '07*, ISBN: 1-4244-1268-4, pp 60-69.