CHAPTER 4

SWARM BASED DEFENCE TECHNIQUE FOR DENIAL OF SLEEP ATTACK

4.1 INTRODUCTION

The next step towards the detection scheme is to introduce a resistant countermeasure for defending against specific attack like denial of sleep attack in wireless sensor networks. A set of effective and efficient algorithm have been introduced after a comprehensive analysis of attacks. More specifically, SBDT model has been extended to detect denial of sleep attack. It consumes more amount of energy which leads to depletion of battery power. This consumption of power makes the nodes more susceptible to the vulnerabilities and hence to the denial of service through denial of sleep. If a large percentage of network nodes, or a few critical nodes, are attacked, the network lifetime is reduced severely.

Time series S-ARMA (Swarm intelligence Auto Regressive Moving Average) model is proposed to predict the network traffic in future using Swarm intelligence and Auto Regressive Moving Average. 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.

4.2 DENIAL OF SLEEP ATTACK

In WSN, the nodes which usually consumes less power, consumes more energy due to the denial of sleep attack. Since the load imposed on the network consumes more amount of charge, there are possibilities for nodes to stop working or deny the service.

The constrained resources are tired out due to the denial of sleep attack which targets upon consuming power of battery powered device. The lifespan of the network is affected severely by this attack which prevails for longer time since large percentage of network nodes or a few critical nodes are subject to this attack. Usually an attempt which aims at interrupting, weakening or destroying the network is known as DoS attack. In order to perform its expected attacking function, the DoS attack events diminish or eliminate a network’s capacity. The denial of sleep attack can be caused due to hardware failures, software bugs, resource exhaustion and environmental conditions.

Denial of sleep is caused mainly due to low battery power in the nodes. The following are the possible methods for the battery power discharge in wireless sensor nodes has been proposed by Thomas martin et al (2004).

- **Service request power attack** – Repeated service requests to the sensor nodes lead to loss of power. The sensor nodes waste their energy by responding to the request from the attackers.

- **Begin power attack** – In this attack, when the task requiring more energy is executed by a victim, the sensor nodes waste much of its energy in responding their requests. Generally the time consumed
to begin a task is more comparing to executing it. This kind of malicious request to begin a task is executed frequently to reduce the battery power of sensor nodes.

- **Malignant power attack** – This attack targets upon the particular program which replaces the entire program of the sensor node which helps in conserving power of the batteries. A malicious program which consumes more energy than expected or required replaces the original program of the node in this attack.

### 4.3 TIME SERIES MODELS

The analysis of experimental data at different points of time leads to new and unique problems in statistical modeling and inference. The obvious correlation introduced by the sampling of adjacent points in time can severely restrict the applicability of the many conventional statistical methods which traditionally dependent on the assumption that these adjacent observations are independent and identically distributed. The systematic approach by which one goes about answering the mathematical and statistical questions posed by these time correlations is commonly referred to as “**Time series analysis**”.

The time series analysis adopted by Robert H. Shumway & David S. Stoffer is generally motivated by the assumption that correlation between adjacent points in time is best explained in term of a dependence of the current value on past values. The time series analysis focuses on modeling some future values of a time series as a parametric function of the current and past values.

The primary objective of time series analysis is to develop mathematical models that provide probable descriptions for sample data. In order to provide a statistical setting for describing the character of data that
seemingly fluctuates in a random fashion over time. A time series analysis is defined, as a collection of random variables (Peyton Z. Peebles, 2002)

\[ \{x(t)\} = \{\ldots x_{t-1}, x_t, x_{t+1}, \ldots \} \]

where the random variable,

- \(x_t\) - value taken by the series at time ‘t’
- \(x_{t-1}\) - value at time ‘t-1’
- \(x_{t+1}\) - value at time ‘t+1’

In general, a collection of random variables \(\{x(t)\}\) indexed by \(t\) is referred as a stochastic process discussed by Averill M. Law & David Kelton (2000). The observed values of a stochastic process are referred to realization of the stochastic process. Time series analysis occurs physically in many application areas as follows

- **Economics** - e.g., monthly data for unemployment, hospital admissions.
- **Finance** - e.g., daily exchange rate, a share price.
- **Environmental** - e.g., daily rainfall, air quality readings.
- **Medicine** - e.g., ECG brain wave activity every 2–8 secs.
- **Network** – e.g. network traffic prediction, number of users served.

The wireless network traffic is nonlinear and non-stationary due to application characteristics and user behavior. The traffic prediction is based on traditional network traffic prediction models such as linear regression model, Poisson model, Markov model, and time series model. In wireless
sensor networks the time varying behavior of the traffic due to network characteristics uses time series model to predict the network traffic. Time series analysis is a very effective short term Network traffic prediction method (Gowrishankar 2008). Models for time series data of a stochastic process are classified into three broad categories namely 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

\[ y(t) = x(t) + \mu \]  \hspace{1cm} (4.1)

where

\[ \mu = \text{mean rate} \]

\[ x(t) = \text{random process} \]

ARMA model can be used to predict the behavior of a time series from past values. Such predictions are made to know the future Network Traffic. One subset of ARMA models is autoregressive, or AR models. An AR model expresses a time series as a linear function of its past values. The order of the AR model tells how many lagged past values are included. The simplest AR model is the first-order autoregressive, or AR (1), model

\[ y_t - \phi_1 y_{t-1} = e_t \]  \hspace{1cm} (4.2)

where

\[ y_t \] - the mean-adjusted series at time t

\[ y_{t-1} \] - the series at time t-1

\[ \phi_1 \] - lag-1 autoregressive coefficient

\[ e_t \] - noise.
The noise indicates the error, the random-shock and the residual. The name autoregressive refers to the regression on self (auto). Higher-order autoregressive models include more lagged terms as predictors. The $P^{th}$ order autoregressive model is given by

$$y_t - \phi_1 y_{t-1} - \phi_2 y_{t-2} - \ldots - \phi_p y_{t-p} = e_t$$

(4.3)

The moving average (MA) model is a form of ARMA model in which the time series is regarded as a moving average (unevenly weighted) of a random shock series. The first-order moving average, or MA(1), model is given by

$$y_t = e_t + \theta_1 e_{t-1}$$

(4.4)

where

- $e_t$ – Residuals at time ‘$t$’
- $\theta_1$ – moving average coefficient
- $e_{t-1}$ – Residuals at time ‘$t$-1’

MA models of higher order more than one include more lagged terms. The $q^{th}$ order moving average model is given by

$$y_t = e_t + \theta_1 e_{t-1} + \ldots + \theta_q e_{t-q}$$

(4.5)

The autoregressive model includes lagged terms on the time series itself, whereas the moving average model includes lagged terms on the noise or residuals. The combination of auto regressive model and moving average model leads to autoregressive-moving-average (ARMA) models. The order of the ARMA model is included in parentheses as ARMA ($p,q$),
\[ y_t - \phi_1 y_{t-1} - \ldots - \phi_p y_{t-p} = e_t + \theta_1 e_{t-1} + \ldots + \theta_q e_{t-q} \]

(4.6)

where

- \( p \) - Autoregressive model order
- \( q \) - Moving-average model order

The simplest ARMA model is first-order autoregressive and first-order moving average, i.e., ARMA (1,1)

\[ y_t - \phi_1 y_{t-1} = e_t + \theta_1 e_{t-1} \]

(4.7)

### 4.4 S-ARMA MODEL

Based upon the future Network traffic prediction, a defense technique for anomaly detection is proposed using S-ARMA model. Initially, ARMA (p,q) model analyzes 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 the proposed S-ARMA model 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 such as 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.

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 value 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 since the information about all the attackers is known using S-ARMA model.

4.4.1 Taxonomy in Route Discovery

Route discovery is responsible for generating all possible routes between source and destination. Control packets are 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 like frequency hopping time $H_T$ and Pair wise Key $E_{KS}$ are collected by FAs and the next hop is chosen based on the pheromone value.
The DoS attack is identified by intruder mitigation algorithm based on S-ARMA model and is given in Figure 4.1. Routing between the administrator node A and the destination node D is shown in Figure 4.2. The administrator node A sends the frequency hopping time $T_i$ 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 $C_1$ as 496µs, $H_T$ value of $C_2$ as 700µs, $H_T$ value of $C_3$ as 490µs, $H_T$ value of $C_4$ as 520µs, and $H_T$ value of $C_5$ as 510µs. The $H_T$ which is above the threshold value $\eta$ 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 proposed by Wood et al (2007) using Pseudo Noise Sequence-PN sequence (Simon haykin, 1988) which is unknown to the attacker. So it calculates the frequency hopping time incorrectly.

```
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 $C$ as

$$C = \{ E_{ks}(i) \mod C_B \} , \ i \geq 0$$

Where,

$C_B$ – Number of channels in the band

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

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

Where,

$HT_{min}$ - minimum hopping time
$HT_{max}$ - maximum hopping time
$T_i$ – frequency hopping time
$n$ – Number of nodes
```
Figure 4.1 (Continued)

| 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 \( \eta \) 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 4.1 Intruder mitigation algorithm

The \( \eta \) value considered here is 548\( \mu \)s. The channel 2 has a \( H_T \) value of 700\( \mu \)s and is considered as an 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.
4.4.2 Traffic Prediction Model

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

\[
T_t - \phi_1 T_{t-1} - \ldots - \phi_p T_{t-p} = w_t + \theta_1 w_{t-1} + \ldots + \theta_q w_{t-q}
\]

(4.8)

where

\[
T_t \text{ - Traffic series at time } t
\]

\[
\phi_p \text{ - autoregressive coefficient}
\]

\[
w_t \sim WN(0, \sigma^2) \text{ White noise with zero mean and } \sigma^2 \text{ - variance}
\]

\[
\theta_p \text{ - moving average coefficient}
\]

Using lag parameters (or) backshift operator

\[
L^k T_t = T_{t-k} \text{ (or) } B^k T_t = T_{t-k}
\]

(4.9)

Equation (4.8) becomes by using lag parameters (or) backshift operator

\[
\phi(L) T_t = \theta(L) w_t
\]

(4.10)

where

\[
\phi(L) = 1 - \phi_1 L - \phi_2 L^2 - \ldots - \phi_p L^p
\]

\[
\theta(L) = 1 + \theta_1 L + \theta_2 L + \ldots + \theta_q L^q
\]

\[
T_t - \phi_1 L T_{t-1} - \ldots - \phi_p L^p T_t = w_t + \theta_1 L T_{t-1} + \ldots + \theta_q L^q w_t
\]

(4.11)

S-ARMA model starts the process of estimation by calculating the auto-correlation function for \(T_t\) using Yule walker equation given by Monson H.Hayes (1996) for S-ARMA \((p,q)\) model is given below
Equation (4.12) in matrix form is given for \( k = q+1, q+2, \ldots, q+p \)

\[
\begin{bmatrix}
R_{\mathbf{T}}[q] & R_{\mathbf{T}}[q-1] & \ldots & R_{\mathbf{T}}[q-p+1] \\
R_{\mathbf{T}}[q+1] & R_{\mathbf{T}}[q] & \ldots & R_{\mathbf{T}}[q-p+2] \\
\vdots & \vdots & \ddots & \vdots \\
R_{\mathbf{T}}[q+p-1] & R_{\mathbf{T}}[q+p-2] & \ldots & R_{\mathbf{T}}[q]
\end{bmatrix}
\begin{bmatrix}
\varphi_1 \\
\varphi_2 \\
\vdots \\
\varphi_p
\end{bmatrix}
= 
\begin{bmatrix}
R_{\mathbf{T}}[q+1] \\
R_{\mathbf{T}}[q+2] \\
\vdots \\
R_{\mathbf{T}}[q+p]
\end{bmatrix}
\]

S-ARMA (1,1) model is used to predict the future traffic. If \( T_0, T_1, T_2, \ldots, T_n \) is the traffic series

\[
T_t = \phi_1 T_{t-1} + w_t + \theta_1 w_{t-1}
\]  
(4.13)

Introducing Lag parameter (or) Backshift operator in Equation (4.13)

\[
\phi(L)T_t = \theta(L) w_t
\]  
(4.14)

where

\[
\phi(L) = 1 - \phi_1 L \\
\theta(L) = 1 + \theta_1 L
\]

\( \phi_1 \) and \( \theta_1 \) are traffic prediction parameters.

The auto-correlation function for \( T_t \) is given by

\[
R_{\mathbf{T}}(q+1) = \phi_1 R_{\mathbf{T}}(q)
\]  
(4.15)

Auto correlation function (ACF) for S-ARMA (1,1) model is given by
The traffic values are predicted by the values of $\phi_1$ and $\theta_1$. Only when $|\phi|<1$ 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

$$T_t = \hat{\phi}_1 T_{t-1} + w_t + \hat{\theta}_1 w_{t-1}$$

(4.18)

where $\hat{\phi}_1$ and $\hat{\theta}_1$ are estimated from $\phi_1$ and $\theta_1$ using least square method.

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

$$\hat{T}_t \rightarrow \text{ARMA} \rightarrow T_{t+1}$$

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

$$e_{T_t} = T_{t+1} - \hat{T}_{t+1}$$

(4.19)

where

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

The confidence interval adopted by Averill M.law & David Kelton (2000) for this 1 step prediction is 95% ($e_{T_t} = 0.01$)
4.4.3 Traffic Prediction model based Intruder Detection

The predicted traffic flow values and the actual values are compared to check the inaccuracy in them whether they are in confidence level or not. When these values are not in confidence interval the nodes are subjected to attack. The difference between two is denoted as

\[ F = |T_A - T_P| \]  \hspace{1cm} (4.21)

where

\[ T_P \] - prediction traffic at certain time

\[ T_A \] - actual traffic at certain time

Let P represents the threshold value which is an average traffic divided by total time interval. When \( F - \varepsilon_{\text{rt}} > P \), the current traffic is abnormal. The node affected sends the Frequency hopping time request to administrator node, since it is responsible for initiating the frequency hopping technique.

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 be started or not.

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

4.5 SIMULATION RESULTS AND PERFORMANCE ANALYSIS

4.5.1 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 2.4 GHz frequency band separated by 5 MHz. 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 4.1.
Table 4.1 Simulation Parameters

<table>
<thead>
<tr>
<th>Number of Nodes</th>
<th>50</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area Size</td>
<td>50 X 50</td>
</tr>
<tr>
<td>MAC</td>
<td>IEEE 802.15.4</td>
</tr>
<tr>
<td>Transmission Range</td>
<td>40m</td>
</tr>
<tr>
<td>Simulation Time</td>
<td>10,20,30,40 and 50 sec</td>
</tr>
<tr>
<td>Traffic Source</td>
<td>CBR</td>
</tr>
<tr>
<td>Packet Size</td>
<td>512</td>
</tr>
<tr>
<td>Sources</td>
<td>4</td>
</tr>
<tr>
<td>Attackers</td>
<td>1,2,3,4 and 5</td>
</tr>
<tr>
<td>Rate</td>
<td>50kb to 250kb</td>
</tr>
</tbody>
</table>

4.5.2 Performance Metrics

The proposed S-ARMA model for Denial of Sleep attack based on network traffic prediction is compared with existing ARMA model for Split network proposed by Chunlai Du et al (2011) to evaluate the performance of the proposed model. 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.
4.5.3 Simulation Results

Simulation results are presented and discussed in this section. The graph shows the average of multiple runs for a given set of parameter values. The parameter values evaluated for performance metric are summarized in the Table 4.2.

Table 4.2 Parameter values evaluated

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet Transmission Rate</td>
<td>50, 100, …, 250 Kbps</td>
</tr>
<tr>
<td>Packet Delivery Ratio</td>
<td>0.2, …, 0.8</td>
</tr>
<tr>
<td>Packet Drop</td>
<td>400, …, 16000 pkts</td>
</tr>
<tr>
<td>Overhead</td>
<td>10000, …, 30000 pkts</td>
</tr>
<tr>
<td>Time</td>
<td>10, 20, …, 50 sec</td>
</tr>
<tr>
<td>Attackers</td>
<td>1, 2, …, 5</td>
</tr>
</tbody>
</table>

4.5.3.1 Based on rate

S-ARMA model is compared with ARMA technique in terms of Packet delivery ratio, Packet drop and overhead with respect to Packet transmission rate. The performance at different transmission rate from 50 kbps to 250kbps proves the proposed method to be feasible and effective.

Variation of packet delivery ratio with packet transmission rate

The packet delivery ratio varies with packet transmission rate as illustrated in Figure 4.3. When the traffic rate is increased from 50Kbps to 250Kbps, it results in large volume of traffic leading to drop of overloaded packets. Also the traffic prediction becomes complex leading to failure of
detections. Hence the packet delivery ratio decreases. In S-ARMA, the packet delivery ratio is increased by 39.65% due to swarm based ARMA model which depicts the future traffic. Based on the traffic, the channel with attacker is made known to the source from the true frequency hopping time. Initially, the performance of delivery ratio is more and gradually it is reduced in ARMA compared to S-ARMA as given in Table 4.3.

In ARMA, the packet delivery ratio is reduced 54% when the transmission rate increases from 50Kbps to 100Kbps and it maintains the performance till 200kbps and then increases at 250 kbps. Frequency hopping is initiated, based on the abnormality in the traffic. The channel information is unknown to the source which reduces the delivery ratio.

<table>
<thead>
<tr>
<th>Rate (Kbps)</th>
<th>Packet Delivery Ratio</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>S-ARMA</td>
</tr>
<tr>
<td>50</td>
<td>0.752309</td>
</tr>
<tr>
<td>100</td>
<td>0.728878</td>
</tr>
<tr>
<td>150</td>
<td>0.748387</td>
</tr>
<tr>
<td>200</td>
<td>0.49653</td>
</tr>
<tr>
<td>250</td>
<td>0.752399</td>
</tr>
<tr>
<td>Average</td>
<td>0.695701</td>
</tr>
</tbody>
</table>
The Packet drop in S-ARMA and ARMA are compared in Table 4.4 with varying transmission rate. The number of packets drop is more in existing ARMA technique compared to S-ARMA model, due to unknown information about the channel. The performance of S-ARMA model is improved by 59.47% as depicted in Figure 4.4. This variation is due to swarm intelligence which alerts the network about the channel with an attacker based on the frequency hopping time and network traffic.

Initially at a transmission rate of 50kbps, the packet drop in S-ARMA model is fairly less compared to ARMA technique. In ARMA, the packet drop increases with transmission rate due to synchronization of frequency hopping between the management nodes in the cluster. The S-ARMA model uses SI to detect the channel with Denial of Sleep attack which improves the performance by reducing the packet drop.
Table 4.4 Variation of Packet Drop with rate

<table>
<thead>
<tr>
<th>Rate (Kbps)</th>
<th>Packet Drop</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>S-ARMA</td>
</tr>
<tr>
<td>50</td>
<td>2071</td>
</tr>
<tr>
<td>100</td>
<td>3882</td>
</tr>
<tr>
<td>150</td>
<td>2362</td>
</tr>
<tr>
<td>200</td>
<td>10568</td>
</tr>
<tr>
<td>250</td>
<td>2829</td>
</tr>
<tr>
<td>Average</td>
<td>4342.4</td>
</tr>
</tbody>
</table>

Figure 4.4 Transmission Rate Vs Packet Drop

Variation of overhead with transmission rate

The variation of overhead with the transmission rate for S-ARMA model and ARMA technique is illustrated in the Figure 4.5. The overhead increases with the number of data packets in both the techniques. In S-ARMA
model, overhead is reduced by 27.84% compared to ARMA technique due to the information about the attacker in the channel is known using ant agents.

The overhead is increased in ARMA technique due to frequency hopping escape from the evaluation of network traffic, synchronization of frequency hopping and integration of network. As the transmission rate increases, the overhead also increases since the node joins as a new member if time delay is increased.

Effectiveness of the proposed method is proved by the values of delivery ratio as given in the Table 4.5, since the overhead is reduced due to swarm intelligence.

**Table 4.5 Variation of Overhead with rate**

<table>
<thead>
<tr>
<th>Rate (Kbps)</th>
<th>Overhead</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>S-ARMA</td>
</tr>
<tr>
<td>50</td>
<td>3963</td>
</tr>
<tr>
<td>100</td>
<td>8429</td>
</tr>
<tr>
<td>150</td>
<td>10340</td>
</tr>
<tr>
<td>200</td>
<td>14434</td>
</tr>
<tr>
<td>250</td>
<td>13869</td>
</tr>
<tr>
<td>Average</td>
<td>10207</td>
</tr>
</tbody>
</table>
4.5.3.2 Based on time

The packet delivery ratio, Packet drop and overhead with respect to transmission time which varies from 10 sec to 50 sec are analyzed for the proposed method and ARMA technique. The performance with respect to time confirms the superior nature of the proposed model.

**Variation of packet delivery ratio with time**

The packet delivery ratio of S-ARMA and ARMA technique at different time instants is shown in Figure 4.6. When the time interval is increased from 10 seconds to 50 seconds, it increases the possibility of attacks for the attackers. Hence the packet delivery ratio will decrease. In S-ARMA, packet delivery ratio is maintained at time instants from 20sec to 50sec, since the anomaly channel is avoided for transmission by using information of ant agents. On comparing the packet delivery ratio of both the schemes, the performance of S-ARMA model is increased by 5.72%.

In ARMA, the packet delivery ratio increases from 10 to 30sec and then decreases by 6% from 40sec onwards due to synchronization of
frequency hopping time. At initial time instants, the difference in packet delivery ratio for both the cases is only 2% and it increases to 13% at 50sec as given in Table 4.6, since the information about the node with faulty channel is identified using ant agents based on frequency hopping time in S-ARMA model.

Table 4.6 Variation of Packet Delivery Ratio with time

<table>
<thead>
<tr>
<th>Time (sec)</th>
<th>Packet Delivery Ratio</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>S-ARMA</td>
<td>ARMA</td>
</tr>
<tr>
<td>10</td>
<td>0.72</td>
<td>0.70557</td>
</tr>
<tr>
<td>20</td>
<td>0.759091</td>
<td>0.733788</td>
</tr>
<tr>
<td>30</td>
<td>0.755072</td>
<td>0.739666</td>
</tr>
<tr>
<td>40</td>
<td>0.753454</td>
<td>0.693454</td>
</tr>
<tr>
<td>50</td>
<td>0.752309</td>
<td>0.652375</td>
</tr>
<tr>
<td>Average</td>
<td>0.747985</td>
<td>0.704971</td>
</tr>
</tbody>
</table>

Figure 4.6 Time Vs Packet Delivery Ratio
Variation of packet drop with time

The packet drop for S-ARMA model and ARMA at various time instants is analyzed in Figure 4.7. When the time interval is increased from 10 seconds to 50 seconds, it increases the possibility of attacks for the attackers, which leads to more packet drops. In S-ARMA model, the packet drop decreased by 54.69% compared to ARMA technique. The packet drop varies by 25.73% from 10 sec to 50 sec in S-ARMA model and 56.75% in ARMA model as shown in Table 4.7.

Table 4.7 Variation of Packet Drop with time

<table>
<thead>
<tr>
<th>Time (sec)</th>
<th>Packet Drop</th>
<th>S-ARMA</th>
<th>ARMA</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>1538</td>
<td>2552</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>1883</td>
<td>3996</td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>1962</td>
<td>4193</td>
<td></td>
</tr>
<tr>
<td>40</td>
<td>2009</td>
<td>5396</td>
<td></td>
</tr>
<tr>
<td>50</td>
<td>2071</td>
<td>5901</td>
<td></td>
</tr>
<tr>
<td>Average</td>
<td>1892.6</td>
<td>4407.6</td>
<td></td>
</tr>
</tbody>
</table>

Figure 4.7 Transmission time Vs Packet Drop
In ARMA technique, the synchronization of frequency hopping time should be fast. Otherwise the Administrator node considers the member node to be a dead node due to physical damage or energy depletion. Those nodes wait for next round to join the network. Thus the packet drop increases with time in ARMA compared to S-ARMA model.

**Variation of overhead with time**

Variation of overhead with transmission time for S-ARMA and ARMA technique is evaluated. The overhead in both the schemes increases with respect to time which is illustrated in Table 4.8. When the time is increased from 10 to 50 seconds, it results in more number of frequency hopping. In S-ARMA model, the overhead is reduced by 55.21% compared to ARMA technique as shown in Table 4.8.

<table>
<thead>
<tr>
<th>Time (sec)</th>
<th>Overhead</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>S-ARMA</td>
</tr>
<tr>
<td>10</td>
<td>835</td>
</tr>
<tr>
<td>20</td>
<td>1896</td>
</tr>
<tr>
<td>30</td>
<td>2583</td>
</tr>
<tr>
<td>40</td>
<td>3274</td>
</tr>
<tr>
<td>50</td>
<td>3963</td>
</tr>
<tr>
<td><strong>Average</strong></td>
<td><strong>2510.2</strong></td>
</tr>
</tbody>
</table>

In ARMA, the Administrator node sends frequency hopping notification based on traffic. On receiving the notification, member sends response to the administrator node. If the response is delayed, the node has to rejoin the cluster in the next round and this increases the overhead with time.
Overhead is reduced in S-ARMA model; Based on the traffic, frequency hopping is initiated and the abnormality in the channel is identified using ant agents. Reduced overhead is achieved in S-ARMA which confirms the superior nature of this scheme as depicted in Figure 4.8.

![Time Vs Overhead](image)

**Figure 4.8 Transmission time Vs Overhead**

### 4.5.3.3 Based on attackers

The Performance of S-ARMA and ARMA Technique are compared with varying number of Attackers up to 5. Packet delivery ratio, Packet drop and overhead are analyzed and discussed.

**Variation of packet delivery ratio with attackers**

The performance of packet delivery ratio with number of attackers of S-ARMA model and ARMA model are analyzed in Figure 4.9. The packet delivery ratio reduces with the number of attackers in both the schemes. In S-ARMA model, packet delivery ratio increases by 36.44% compare to ARMA technique due to identification of anomaly channel are done by using traffic prediction model and swarm intelligence.
In ARMA, delivery ratio reduces with number of attackers as evaluated in Table 4.9. As number of attackers is increased, the network adopts frequent change in frequency hopping which reduces the delivery ratio by 49.41%, when the number of attackers is increased from 1 to 5.

Table 4.9 Variation of Packet Delivery Ratio with attackers

<table>
<thead>
<tr>
<th>Attackers</th>
<th>Packet Delivery Ratio</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>S-ARMA</td>
</tr>
<tr>
<td>1</td>
<td>0.999737</td>
</tr>
<tr>
<td>2</td>
<td>0.917988</td>
</tr>
<tr>
<td>3</td>
<td>0.835297</td>
</tr>
<tr>
<td>4</td>
<td>0.759367</td>
</tr>
<tr>
<td>5</td>
<td>0.496530</td>
</tr>
<tr>
<td>Average</td>
<td>0.801784</td>
</tr>
</tbody>
</table>

Figure 4.9 Attackers Vs Packet Delivery Ratio
Variation of packet drop with attackers

The packet drop in S-ARMA model and ARMA technique is compared with number of attackers as shown in Figure 4.10. In S-ARMA model, the packet drop is reduced by 44.03% compared to ARMA. Initially, the packet drop is less and it increases gradually with more number of attackers in both the schemes. Better performance is achieved in S-ARMA model due to swarm based detection of Denial of Sleep attack using traffic prediction and frequency hopping.

In ARMA, when network identifies the malicious node it change its frequency. As the number of attackers is increased the rate of packet drop is larger as in Table 4.10 due to frequent change in frequency and thus degrades the performance under more number of attackers compared to proposed model.

Table 4.10 Variation of Packet Drop with attackers

<table>
<thead>
<tr>
<th>Attackers</th>
<th>Packet Drop</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>S-ARMA</td>
</tr>
<tr>
<td>1</td>
<td>2378</td>
</tr>
<tr>
<td>2</td>
<td>2682</td>
</tr>
<tr>
<td>3</td>
<td>4782</td>
</tr>
<tr>
<td>4</td>
<td>5204</td>
</tr>
<tr>
<td>5</td>
<td>10568</td>
</tr>
<tr>
<td>Average</td>
<td><strong>5122.8</strong></td>
</tr>
</tbody>
</table>
Variation of overhead with attackers

Variation of overhead with number of attackers for S-ARMA model and ARMA technique is depicted in Figure 4.11. Overhead increases with number of attackers in both the schemes. Increase in number of attackers from 1 to 5 leads to more frequency hopping which in turn increases the overhead. Initially, with less number of attackers in S-ARMA model the overhead reduced by 45.61% and as the number of attackers are increased its performance is reduced by 26.94% compared to ARMA technique.

On comparing both the schemes, the overhead is reduced by 23.70% as the number of attackers is increased from 1 to 5. In S-ARMA; the attackers are identified using ant agents which reduce the overhead. Effectiveness of the proposed method is proved by simulation results shown in Table 4.11.
Table 4.11 Variation of Overhead with attackers

<table>
<thead>
<tr>
<th>Attackers</th>
<th>Overhead</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>S-ARMA</td>
</tr>
<tr>
<td>1</td>
<td>9781</td>
</tr>
<tr>
<td>2</td>
<td>10527</td>
</tr>
<tr>
<td>3</td>
<td>12465</td>
</tr>
<tr>
<td>4</td>
<td>13036</td>
</tr>
<tr>
<td>5</td>
<td>14434</td>
</tr>
<tr>
<td>Average</td>
<td>12048.6</td>
</tr>
</tbody>
</table>

Figure 4.11 Attackers Vs Overhead

4.6 CONCLUSION

Denial of sleep attack is considered to be a one of the prominent attack in wireless sensor networks. The detection of such attacks is considered to be significantly a challenging task. A Time series S-ARMA model has been proposed to detect denial of sleep attack in IEEE802.15.4 based wireless sensor network. 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. In general, the results of this chapter provide a way for designing more resilient intruder detection schemes.