IDS Using Traffic Prediction based on ARIMA for Wireless Industrial Network

Dhanya Jayan
Dept. of Computer Science & Engg.
Sree Buddha College of Engg.
Alappuzha, Kerala, INDIA
dhanyajayan4u@gmail.com

Gopu Darsan
Dept. of Computer Science & Engg.
Sree Buddha College of Engg.
Alappuzha, Kerala, INDIA
gops601@gmail.com

Abstract— **Most challenging security problem in wireless network is detecting intrusion attack. An intrusion detection system is mainly used for detecting the intruders present in the system. Intrusion is defined as the set of action mainly consist of integrity of data, confidentiality, and availability of the system. Intrusion detection is the identification of the unauthorized user trying to access the data. Intrusion detection system is hardware or software tool is used to detect the intruder present in the system. Intrusion attack of various types can be detected by using change in the traffic flow. An ARMA and ARIMA based model is mainly used for detecting the change in the traffic flow. For that, in proposed system want proper intrusion detection schema architecture for ARIMA model is introduced. A full channel analyzer which captures the data from the real network and analysis the data, calculate the ACF and PACF using the ARMA and ARIMA based model, if any inappropriate occurrences find it will generate an alarm. Intrusion detection scheme method uses an ARMA and ARIMA based model approach to establish security in WIA-PA networks. We can predict the network traffic precisely and quickly. This Scheme can ensure the detection of intrusion attacks; improve the whole performance of the system and prolong the lifetime of the network, while isolating the malicious traffic injected by the compromised nodes or illegal intrusions into the network.**

Keywords— IDS; ACF; PACF; ARIMA; ARMA; WIA-PA network.

I. Introduction

An intrusion detection system is mainly used for detecting the intruders present in the system. Intrusion is defined as the set of action mainly consist of integrity of data, confidentiality, and availability of the system. Intrusion detection is the identification of the unauthorized user trying to access the data. Intrusion detection system is hardware or software tool is used to detect the intruder present in the system. Intrusion attack of various types can be detected by using change in the traffic flow. An ARMA based model and ARIMA based model is mainly used for detecting the change in the traffic flow. Calculate the ACF and PACF using the ARMA and ARIMA model. The intrusion detection system for wireless industrial network analysis the data, if any inappropriate occurrences find it will generate an alarm. Intrusion detection scheme method uses an ARMA and ARIMA based model approach to establish security in WIA-PA networks. This scheme can ensure the detection of intrusion attacks.

II. Related Works

J. F. Tian, Z. Zhang, and W. Zhao [1] proposed and designed an IDS model called misuse and anomaly based IDS (MAIDS). In anomaly based detection technique, normal profiles of system states or user behaviors are stored in the database and if any current activities occur, it will check the new data and old data in data base, if any inappropriate occurrence will occur. It generates an alarm. In misused based detection system encodes known attack signatures and system vulnerabilities, if any inappropriate occurrence will occur it will generate an alarm. The disadvantage is that the Intrusion detection systems can detect only two type of detection anomaly based detection system and misused based system.

For wireless mobile environments, L. Liu and L. Zhuowei [2] proposed two intrusion detection mechanisms, which are anomaly mechanism and signature-based mechanism. In anomaly based detection technique, normal profiles of system states or user behaviors are used for the detection of intruders present in the system. In signature-based mechanism encodes known attack signatures and system vulnerabilities, if any inappropriate occurrence will occur it will generate an alarm. The disadvantage of this paper is that the Intrusion detection systems have an Inability to detect new attacks.

Piya and J. Andrew [3] proposed a non-overlapping zone-based IDS (ZBIDS). The network could be divided into non-overlapping zones, because the network is wireless, the coverage can be designed to have non-overlapping zones. The partitioning of the network could be based on the monitoring range of the channel analyzer. The disadvantage of this paper is limited collection of data from real networks.

A Willig, K. Matheus, and A. Wolisz [4] proposed a wireless intrusion detection system, in this paper channel analyzer capture the data from the real networks but it can capture only limited amount of data from the real networks. Wireless intrusion detection system analysis the capture data if any inappropriate occurrence will find it will generate an alarm. The disadvantageous of this system is inability to detect the new type of attack. In this system the analysis of the behavior and state is done by manually, so time consuming. The speed of the intrusion detection system is low. It is challenging to design an approach capable of detecting all types of attacks. To overcome the disadvantageous of these systems proposed intrusion detection system using traffic prediction for wireless industrial networks.

Min kim and Keecheon kim [5] proposed Intrusion detection scheme using traffic prediction for wireless industrial networks. The partitioning of the network could be based on the monitoring range of the channel analyzer and also assumed that the field devices receive the beacons and send data in every super frame cycle in the WIA-PA network. Third party intrusion detection schema architecture and algorithm for calculating the ACF and PACF using the ARMA model are introduced in it. A third party intrusion detection analysis system resides outside the WIA-PA wireless industrial networks. So it will not consume any network resources of wireless industrial networks. Another advantage is that, it can expand the system without interrupting any other local intrusion detection present in the wireless industrial networks. If the attacker only sends one or two falsified pieces of data, different data cycles, and the data series may not follow a normal distribution, it is difficult to detect the attacks.

III. System design

Most challenging security problem in wireless network is detecting intrusion attack. IDS using data traffic prediction model based on ARMA and ARIMA for WIA-PA network. Steps in Intrusion detection scheme are:-

- All channel analyzer.
- Intrusion detection analysis system.
- Data traffic prediction model based on ARIMA.
- WIA-PA security manager.
- WIA-PA system manager.
- Events monitor.
- Intrusion alarm solution.

Full channel analyzers mainly consist of data sniffer which captures the original data from the real network. In intrusion detection analysis system, data from the data sniffer is passed to the intrusion analysis system data cache in the intrusion analysis system store the data from the data sniffer and pass it to the real time traffic analysis. In the real time traffic analysis generate the real data input. The real data input is passed to both anomaly based system and the ARIMA prediction traffic model. In ARMA traffic model calculate the autocorrelation function and partial autocorrelation function. The calculated result is passed to the anomaly system. In anomaly system generate the WIA-PA traffic prediction result and it is passed to the intrusion analysis. In the intrusion analysis it will find any intruder present in the system using the analysis report and also generate an analysis result.

In WIA-PA security manager, the report from both the third party intrusion detection system and local intrusion detection system it will conform that any intruder present in the system, if any intruder present in the system it will inform the intrusion alarm solution. It also passes the newly generated repot to the WIA-PA system manager.

In WIA-PA system manager, the system manager will re-configure the network resources, and enhance the security of the entire system by expanding the functionality of the local intrusion detection module and blacklisting the channel where most of the intrusions took place to avoid any communication through this channel to reduce further intrusions. In events monitor, detect the emergencies and events motivated by the system manager. In intrusion alarm solution module is built into the security manager and the gateway. The external intrusion detection module is designed to prevent any attack from the cable network.

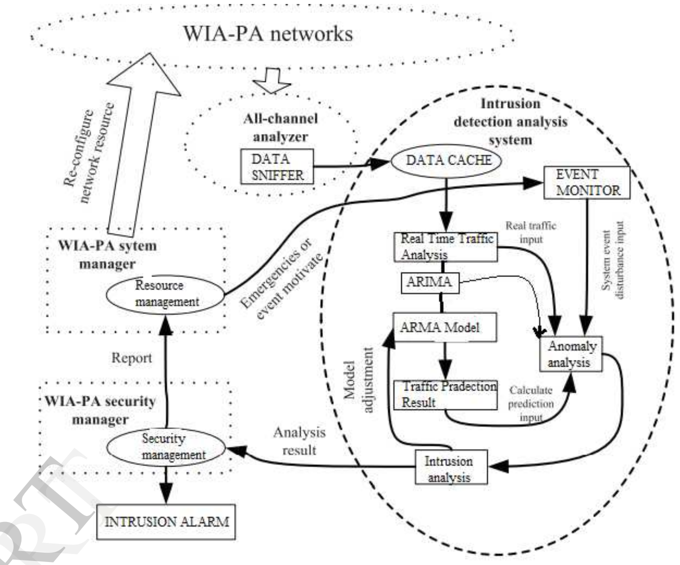

Fig. 1. Intrusion detection scheme

VI. Algorithm

In existing system have two disadvantages if the attacker only sends one or two falsified pieces of data, different data cycle, and the data series may not follow the normal distribution, it is difficult to detect the attacks. It will overcome by using the data traffic prediction ARIMA model. The ARIMA model consists of three parameters p, d and q. p is the auto regressive, d is the differencing and q is the moving average. Three stages of ARIMA model are

- Identification
- Estimating parameters
- Diagnosing a model

In identification stages consist of differencing, auto regressive and moving average. No differencing (d = 0), the models are usually referred to as ARMA (p, q) models. If the differencing is present then do ARIMA (p, d, q) model. The equation for calculating differencing is give below.

$$\Delta Xt = Xt - Xt - 1$$

$$Yt = (1 - L)Xt$$

Auto regressive can be calculated using the equation

$$Xt = \alpha 1Xt - 1 + \ldots + \alpha pXt - p + \varepsilon t$$

Moving average can be calculated using the equation.

$$Xt = \varepsilon t + \beta 1 \varepsilon t - 1 + ... + \beta q \varepsilon t - q$$

In diagnosing a model, error detection is performed in this module, it diagnoses and checks whether it is an intruder or a white noise [5]. In time series white noise have a constant variation only in the frequency. But intruder send one or more falsified data. It can be detected by using an intrusion detection system.

Estimating model parameters, Autocorrelation function (ACF) [5] and partial ACF (PACF) are estimated. The PACF is given as follow.

$$\phi kk = \frac{\begin{vmatrix} 1 & \rho 1 & .. & \rho 1 \\ \rho 1 & 1 & .... & \rho 2 \\ ... & ... & .... & .... \\ \rho k-1 & \rho k-2 & .... & \rho k \end{vmatrix}}{\begin{vmatrix} 1 & \rho 1 & ... & \rho k-1 \\ \rho 1 & 1 & .... & \rho k-2 \\ ... & ..... & ..... & .... \\ \rho k-1 & \rho k-2 & .... & 1 \end{vmatrix}}$$

A. Steps in algorithm

Step 1: Capture the real data traffic.
Step 2: If d=0 perform ARMA model.
Step 3: If d has a value perform
Calculate the ACF and PACF using ARIMA model
Three stages are
Step 3(a): Identification

$$\Delta Xt = Xt - Xt - 1$$

$$Yt = (1 - L)Xt$$

Step 3(b): Estimation

$$Xt = \alpha 1 Xt - 1 + ... + \alpha p Xt - p + \varepsilon t$$

Step 3(c): Diagnose
Error detection
Step 4: Generate alarm.

VI. Expected Result

The fig 2 shows intrusion detection ratios are the comparisons of intrusion detection system using ARMA and intrusion detection system based on ARMA and ARIMA. If the thresholds are higher, the intrusion detection rate will be decreased; if the threshold is lower, the false alarm rate will be increased.

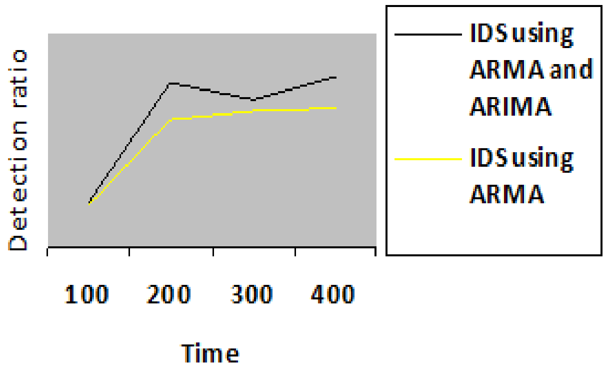

Fig. 2. Intrusion detection ratio

VII. Conclusion

Intrusion detection scheme method uses an ARMA and ARIMA based model approach to establish security in WIA-PA networks. It can detect the new attacks by using the ARIMA model. It can predict the network traffic precisely and quickly. This scheme can ensure the detection of intrusion attacks. Intrusion prevention system as a future work for preventing intruders enters into the wireless industrial network.

References

[1] J.F Tian, Z. Zhang, and W. Zhao, *"Intrusion detection system based on misuse and anomaly*," J. Electron. Inf. Technol, vol. 28, pp. 2163–2166, Nov. 2006.

[2] L. Liu and L. Zhuowei, "*A anomaly-based intrusion detection system in mobile wireless networks,"* Comput. Eng. Appl., vol. 42, pp. 165–167, July 2006.

[3] Piya and J. Andrew, *"Non overlapping zone based intrusion detection system"* in Proc. IEEE/WIC/ACM Int. Conf. Web Intelligence and Intelligent Agent Technol., Dec. 2006, pp. 227–230.

[4] A. Willig, K. Matheus, and A. Wolisz, "*Wireless intusion detection system*," proc. ieee, vol. 93, jun2006.

[5] Min Wei, Keecheon kim,"*Intrusion detection scheme using traffic prediction for wireless industrial* "IEEE, vol. 14, no. 3, june 2012