Intrusion Detection System Using ARIMA Model for Wireless Networks

Amita A. Patil[1], Prof. S. R. Patil[2]
[1]*Sinhgad Institute of Technology, Lonavala, India*
[1]aamu.patil@gmail.com [2]srp.sit@sinhgad.edu

Abstract- **The detection of intrusion attacks in wireless networks is one of the most challenging security issues. The various types of attacks can be detected by change or modification in the traffic. So to know about the change in the traffic flow in this paper, the prediction problem is studied. Basically the ARIMA model is used for the traffic prediction. Based on the trained data the ARIMA model gives more accuracy. We proposed an intrusion detection system for wireless network. The traffic is analyzed by using the time-sequence technique. The result will give a effective intrusion detection system which will effectively detect the intrusion attacks as well as it will improve the network performance.**

Index Terms— ARIMA (Autoregressiv Integrated Moving Averages), Intrusion Detection, Wireless Networks, Traffic Prediction, Anomaly Detection.

I. INTRODUCTION

The intrusion detection system is developed in all the type networks. There are many solutions present for detecting the intrusion attacks in wired as well as wireless networks. We developed the intrusion detection system for wireless because it's most challenging task. Intrusion detection system is the software to detect the intrusion attacks infected in to the network traffic and inform the network security manager. Some systems may stop an intrusion attempt but neither required nor expected to monitor system. Intrusion detection are primarily focused on identifying possible incidents, logging information about them, and reporting attempts. In organizations use Intrusion detection system for other purposes, such as identifying problems with security policies, documenting existing threats, and deterring individuals from violating security policies. Intrusion detection system has become a necessary addition to the security infrastructure of nearly every organization. Intrusion detection system typically record information related to observed events, notify security administrators of important observed events, and produce reports. Much Intrusion detection system can also respond to a detected threat by attempting to prevent it from succeeding. They use several response techniques, which involve the intrusion detection stopping the attack itself, changing the security environment or changing the attack's content.

The intrusion detection system has following functions:

1. Monitoring and analyzing both user and system activities.
2. Analyzing system configurations and vulnerabilities.
3. Assessing system and file integrity.
4. Ability to recognize patterns typical of attacks.
5. Analysis of abnormal activity patterns.
6. Tracking user policy violations.

There are two types of intrusion detection systems are available

1) Misuse based detection (Signature Based):
- Network discovering attacks
- Man-in-middle attack
- DOS attack

2) Anomaly based detection:
- Unknown attacks
- Abnormal patterns in network
- Signatures not yet generated

TABLE I
MISUSE V/S ANOMALY INTRUSION DETECTION SYSTEM

Technique	Advantage	Disadvantage
Misuse Detection	Accurately and generate much fewer false alarm	Cannot detect Novel or unknown attacks
Anomaly Detection	Is able to detect unknown attacks based on audit data collected over normal	High false-alarm, More time consuming, Requires more overhead and processing capacity

The intrusion detection system architecture is depicted in Fig.1. We assumed that the wireless network is divided in to two nonoverlapping zones as the network is in wireless and the coverage can be designed. Prevention of the intrusion attack is another challenging task beyond this paper.

A full channel analyzer is used as lightweight mobile agent in the network to achieve the real time data. The full channel analyzer collects the data and analyzes it and the result will be sent to the security manager. The third party intrusions detection system analyze the real traffic and if any attacks occurred it will report the security manager and security manager will report to the network manager.

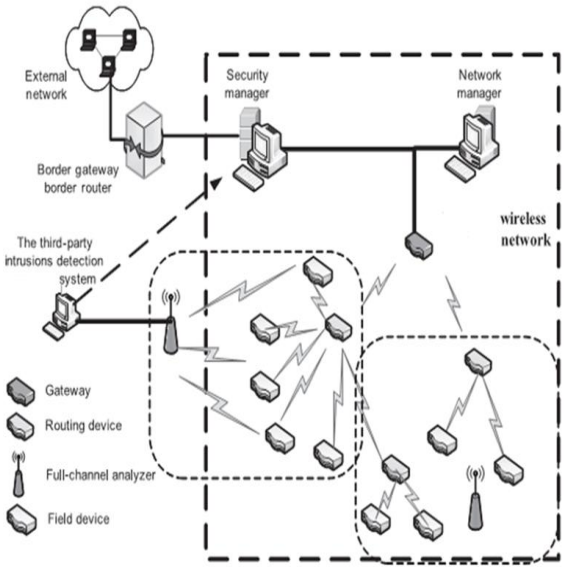

Fig.1. Intrusion detection system architecture in wireless network.

This means that each and every devices communicating each other in some period of time which is distributed evenly. Therefore with these assumption we can consider the all the network traffic as high frequency and we set up our model based on these assumption.

II. LITERATURE SURVEY

Some international organizations have begun to actively promote the industrial wireless network technology standardization process, which primarily consists of WIA-PA, ISA100.11a [2] and WirelessHART [3].

ISAl00.11a [2] is a standard proposed by the ISA100 committee for industrial as well as commercial applications. It has not yet been approved. However, its advantageous features, such as asymmetric cryptography, object-based application layer security, and key management, make it a suitable standard for industrial process automation and control systems. ISA100.11a defines network intrusion detection system.

WirelessHART [3] is another international and recently developed standard. It specifies a security manager to provide key management. It provides communication security between two devices, i.e., the source and the destination at the data-link layer. At the network layer this provides confidentiality by encrypting the network protocol data unit payload and integrity by calculating the keyed message integrity code over the entire network protocol data unit.

ZigBee [4] is a wireless mesh network standard that is lowcost, and has low-power requirements. It is secured by employing the AES-128 algorithm, which defines security at the application layer. However, no frequency diversity and path redundancy is offered and the mechanism also lacks robustness. These issues make ZigBee less reliable and inappropriate for use in industrial process automation. We have used data mining techniques in an intrusion detection module in order to improve the security of the wireless nodes.

In this paper, we have determined that traffic-based intrusion detection has the most potential of all the data mining intrusion detection techniques, because of its ability to detect new attacks. Many traditional intrusion detection techniques are limited by the collection of training data from real networks and the manual labeling of behaviors and states as normal or abnormal [5], [6]. It is very time consuming to manually collect data from a wireless network and to classify the data.

Recently, some researchers have investigated some works on intrusion detection methods in WSNs. In Y. Zhang [7], proposed an intrusion detection and response system structure for mobile ad hoc network (MANET), which was the foundation of most of the work that followed in this area.

Based on pattern matching and statistical analysis. J. F. Tian [8] proposed and designed an intrusion detection system model called misuse and anomaly based intrusion detection system. Misuse and anomaly does not provide a solution to improve the security of an entire wireless network in response to all channel intrusion attacks, to improve the detection speed of the IDS.

For wireless mobile environments, L. Liu [9] proposed two intrusion detection mechanisms, which are anomaly mechanism and signature-based mechanism.

Based on anomaly detection, Piya [10] proposed a self-organized criticality and stochastic learning based IDS for wireless sensor networks.

S. Bo [11] proposed a nonoverlapping zone-based intrusion detection system for mobile ad-hoc networks. The zone based intrusion detection system uses the local intrusion detection system agent and the nonoverlapping zone-based framework.

Min Wei and Keecheon Kim[1] proposed an intrusion detection system based on traffic prediction. For traffic prediction they used the ARMA model. It will give the better result but some non serial data cycle this system may not work as well as accurate result will be not displayed.

III. IMPLEMENTATION DETAILS

A. System Architecture

The intrusion detection scheme in wireless network architecture shown in fig. 2.

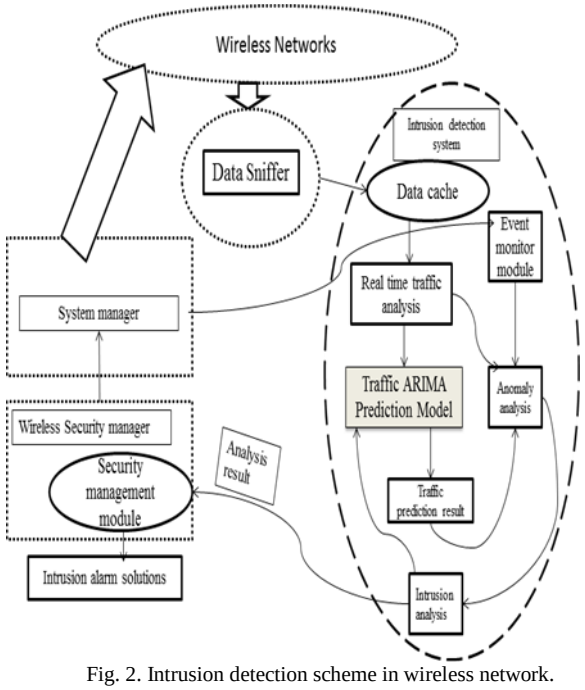

Fig. 2. Intrusion detection scheme in wireless network.

B. ARIMA Model

The ARIMA model is Autoregressive Integrated Moving Average model. The ARIMA model is better than ARMA model. It gives more accurate result than ARMA model. So we are proposed ARIMA model in this paper. The ARIMA model is defined as,

$$\Phi_p(B)\,\nabla^d Y_t = \Theta_q(B)\,\varepsilon(t) \quad (1)$$

Where,

$Y(t) = \{y(t), y(t-1), \ldots\ldots, y(t-n)\}$, n=1,2,3,……

$\nabla^d Y_t$ is $\{Y(t)\}$'s d-step difference.

$\varepsilon(t) = \{e(t), e(t-1), \ldots, e(t-n)\}$, n=1,2,3,……

$\Phi_p(B) = 1 - \varphi_1 B - \varphi_2 B^2 - \ldots\ldots - \varphi_p B^p$

$\Theta_q(B) = 1 + \phi_1 B + \phi_2 B^2 + \ldots\ldots + \phi_q B^q$

Where, p is the step of the autoregressive, d is the difference steps and q is the steps of the moving average model. e(t) is the noise with zero average value. B is the delay arithmetic operator

C. ARIMA model parameter estimation

In this paper, the training process include 5 steps,

1. In this step, the real traffic is captured and it is processed to get error data.
2. Using the analysis result of real traffic the autocorrelation and partial correlation function to decide the number of step number of (p , q) for the ARIMA model.
3. Then the ARIMA model parameters are estimated using the least squares optimization algorithm.
4. Based on the parameters the traffic flow is predicted.
5. The real traffic and predicted traffic will be compared to know any intrusion is infected in real traffic.

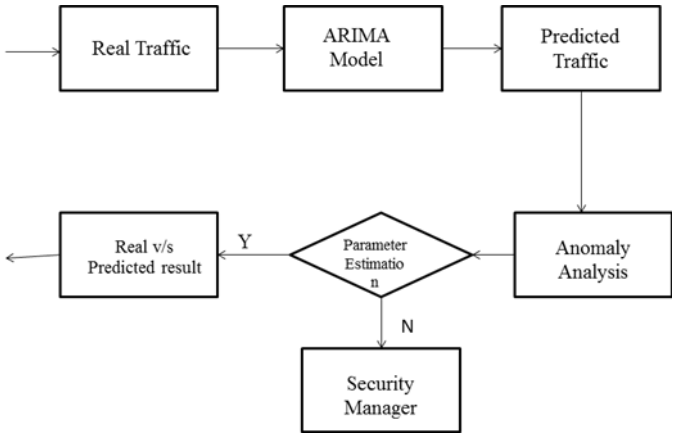

Fig. 3. ARIMA model process.

According to these results the autocorrelation and partial autocorrelation function as well as the real traffic and predicted traffic results will compared and tested.

The Mean Absolute Percentage Error formula will be used to test whether the predicted traffic is same as real traffic or any intrusion is affected to real traffic. If any intrusion is injected then it will be consider as abnormal traffic and it will be reported to security manager.

The MAPE is defined as,

$$\text{MAPE} = \frac{1}{N}\sum_{t=1}^{n}\left|\frac{y(t) - \hat{y}(t)}{y(t)}\right|$$

Where, y(t) is the real value of the traffic flow and $\hat{y}(t)$ is the predicted value of the traffic flow.

CONCLUSION

The use of wireless communication in commercial as well as industry applications is growing rapidly. So providing security becomes an important task. Securing wireless networks is unique research challenges because of the fundamental differences between a wireless network and a traditional wired network. The design of an intrusion detection system for wireless networks represented in this paper. The proposed intrusion detection method uses an ARIMA model based approach to establish security. It provides a new security detection mechanism. In our Intrusion Detection System, the real data traffic the predicted traffic is compared. So can predict the network traffic precisely and quickly. The analysis shows that our scheme can ensure detection of intrusion attacks to improve the whole performance of the system, and prolong the lifetime of the network, while isolating the malicious traffic injected by the nodes or illegal intrusions into the network.

REFERENCES

[1] Min Wei and Keecheon Kim, "Intrusion Detection Scheme Using Traffic Prediction for Wireless Industrial Networks", journal of communications and networks, vol. 14, no. 3, June 2012.

[2] IEC/PAS 62734, "Industrial Communication Networks— Field bus specifications—Wireless Systems for Industrial Automation: Process Control and Related Applications (based on ISA 100.11a)," Sept. 2011.

[3] IEC 62591 Ed.1, "Industrial Communication Networks—Wireless Communication Network and Communication Profiles —WirelessHART TM," Apr. 2010.

[4] IEEE 802.15.4, "Information Technology-Telecommunications and Information Exchange between Systems-Local and Metropolitan Networks- Specific Requirements-Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (LR-WPANs)," 2006.

[5] P. Wang and H. Wang, Heng Wang, and Min Xiang. The Technology of Wireless Communication for Measuring and Controlling, Beijing: Publishing House of Electronics Industry, Mar. 2008.

[6] M. Wei, X. Zhang, W. Ping, K. Kim, and Y. Kim, "Research and implementation of the security method based on WIA-PA standard," in Proc. ICECE, China, Nov. 2010. pp. 1580–1585.

[7] Y. Zhang and W. Lee, "Intrusion detection in wireless ad hoc networks," in Proc. the 6th MobiCom, USA, Aug. 2000, pp. 275–283.

[8] [8] J. Tian, Z. Zhang, and W. Zhao, "The design and research of intrusion detection system based on misuse and anomaly," J. Electron. Inf. Technol., vol. 28, pp. 2163–2166, Nov. 2006.

[9] L. Lijun and L. Zhuowei, "A anomaly-based intrusion detection system in mobile wireless networks," Computer. Eng. Appl., vol. 42, pp. 165–167, July2006.

[10] T. Piya and J. Andrew, "Energy efficiency of intrusion detection systems in wireless sensor network," in Proc. IEEE/WIC/ACM Int. Conf. Web Intelligence and Intelligent Agent Technol., Dec. 2006, pp. 227–230.

[11] S. Bo, Intrusion Detection in Mobile Ad Hoc Networks, Doctoral thesis, Texas A&M University, May 2004.