Intrusion Detection System using Traffic Prediction Model

Amita A. Patil
Sinhgad Institute of Technology,
Lonavala, Pune

S. R. Patil
Sinhgad Institute of Technology,
Lonavala, Pune

ABSTRACT
In Wireless Network, we will not limit the boundaries of network because it makes vulnerable association among the users. Therefore, the detection of intrusion attacks in wireless networks is challenging security issues. The various types of attacks can be detected by using various methods. The change or modification in the traffic flow studied in this paper. The ARIMA model is used for the traffic prediction. The ARIMA model gives more accuracy than other traffic prediction models. In this paper, an intrusion detection system is proposed for wireless network. The result shows an effective intrusion detection system which will effectively detect the intrusion attacks.

Keywords
ARIMA (Autoregressive Integrated Moving Averages), Intrusion Detection, Wireless Networks, Traffic Prediction, Anomaly Detection.

1. INTRODUCTION
As area of modern Wireless network replacing wired networks. Wireless network having open access nature. Any user in range is able to get connected to your wireless network. So once it is connected user can change or modify data. So the intrusion attack problem is studied in this paper. The intrusion detection system can be developed in all the type of wireless networks. There are many solutions present for detecting the intrusion attacks in wired as well as wireless networks. Intrusion detection system is the software to detect the intrusion attacks affected in to the network traffic and report to the security manager.

Intrusion detection systems 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 typically record information related to observed events, notify security administrators of important observed events, and produce reports. 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 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 [2].

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 [2].

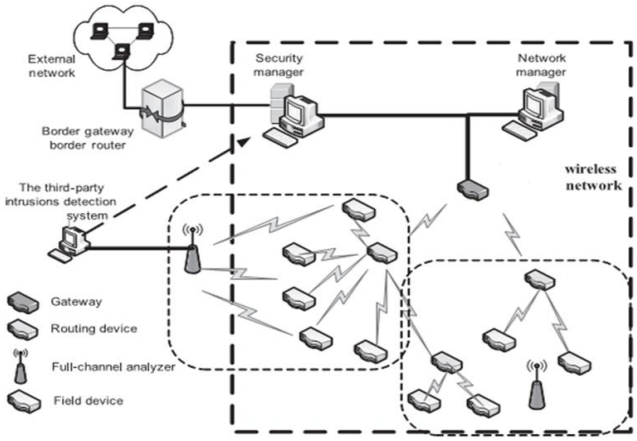

Fig 1: Intrusion detection system architecture in wireless network. [1]

2. LITERATURE SURVEY
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 [6], [7]. 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 [8], 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 [9] 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 [10] proposed two intrusion detection mechanisms, which are anomaly mechanism and signature-based mechanism.

Based on anomaly detection, Piya [11] proposed a self-organized criticality and stochastic learning based IDS for wireless sensor networks.

S. Bo [12] 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.

3. IMPLEMENTATION DETAILS

3.1 System Architecture

The intrusion detection system architecture shown in figure. 2.

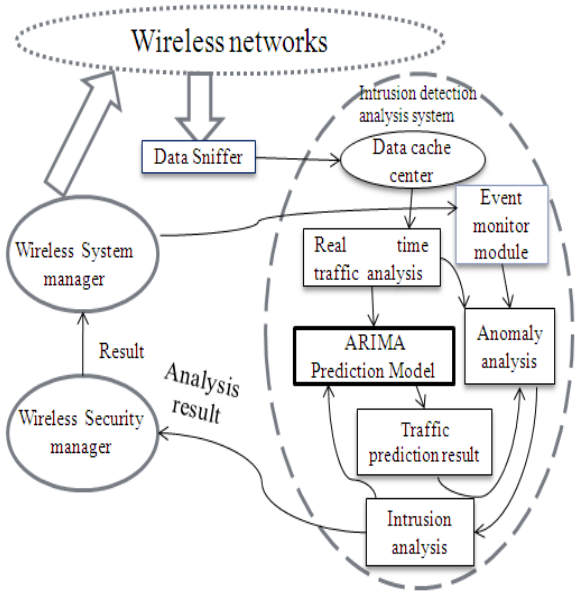

Fig 2: Intrusion detection system in wireless network

3.2 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,

$\Phi p\ (B)\ \nabla d\ Yt = \Theta q\ (B)\ \varepsilon(t)$ (1)

Where,

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

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

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

$\Phi p\ (B) = 1 - \varphi 1B - \varphi 2B2 - \ldots\ldots\ldots - \varphi pBp$

$\Theta q\ (B) = 1 + \phi 1B + \phi 2B2 + \ldots\ldots\ldots + \phi qBq$

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 [2].

3.3 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. [2]

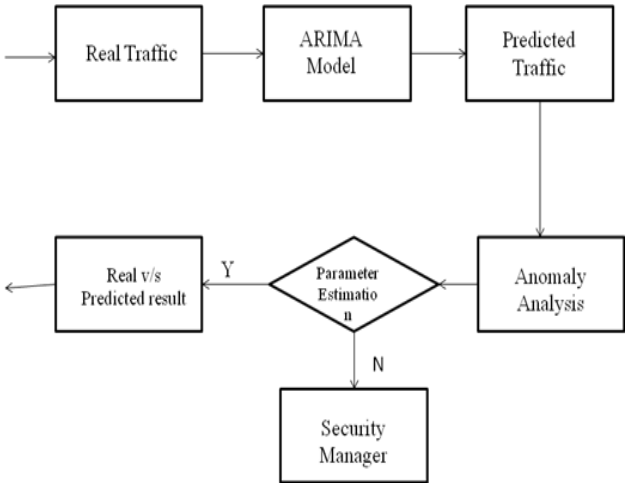

Fig 3: ARIMA model process [2]

The real traffic and predicted traffic results are compared and tested. The Mean Absolute Percentage Error formula 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,

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

Where, y(t) is the real value of the traffic flow and y^(t) is the predicted value of the traffic flow [2].

4. EXPERIMENTAL RESULTS

The results are taken and tested for 50 nodes samples.

The figure 4 shows the original data traffic flow sent from one node to another node.

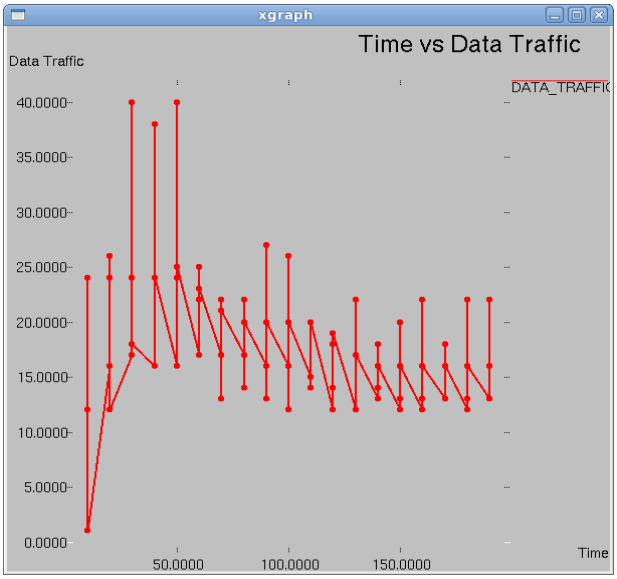

Fig 4: The original data sniffer

The figure 5 shows the stationary time series of original data traffic flow which is obtained by taking logarithmic of original data values.

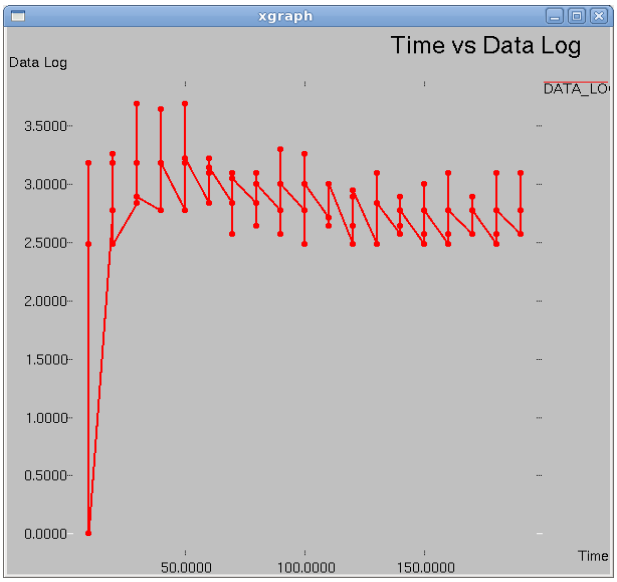

Fig 5: The stationary time series

The figure 6 shows the predicted data traffic calculated by using ARIMA model.

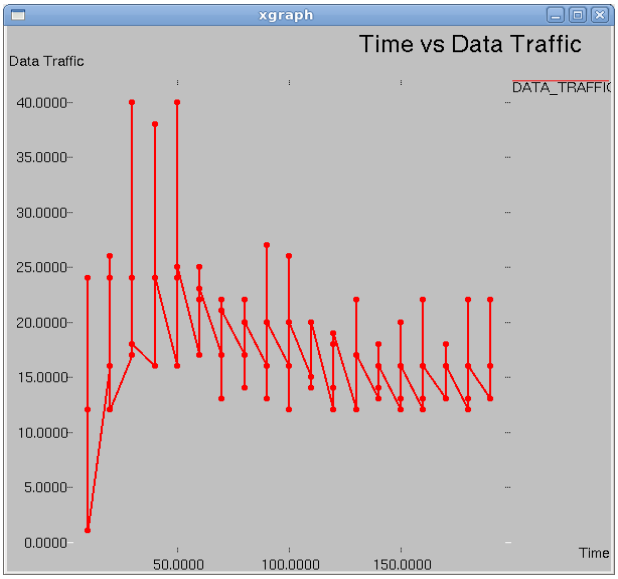

Fig 6: Predicted data traffic

5. CONCLUSION

In this paper, an intrusion detection system using ARIMA model provides good solution to detect the intrusion attacks in wireless networks. 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.

6. 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] Amita A Patil and prof. S. R. Patil. "Intrusion Detection System Using ARIMA Model for Wireless Networks" International Journal of Latest technology in engineering, management and applied science. Volume III, Issue VI, June 2014, ISSN 2278 - 2540

[3] 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.

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

[5] 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.

[6] 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.

[7] 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.

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

[9] 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.

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

[11] 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.

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