Intrusion Prevention System with Anomaly Detection In Wireless Sensor Network

Chakradhar Verma
Research scholar,UCE,RTU,Kota(Raj.)
Dr. C.P.Gupta
RTU,KOTA, Rajasthan ,India.

ABSTRACT : Inaccurate/incomplete data measurements of WSN are often known as WSN anomalies. Outliers in wireless sensor networks are measurements that deviate from the normal model of sensed data and result from errors, events or malicious attacks on the network. The dynamic nature of sensor data and the specificity of the wireless sensor network make traditional outlier detection techniques unsuitable for direct application in such contexts so it is essential to select and adapt appropriate techniques to implement in wireless sensor networks for better sensing quality and more reliable system. As wireless sensor networks are usually deployed in unattended areas, security policies cannot be updated in a timely fashion upon identification of new attacks. This gives enough time for attackers to cause significant damage.

Keywords: *WSN,anamoly detection,Intrusion Detection,Intrusion Prevention,outlier.*

INTRODUCTION:A wireless sensor network (WSN) consists of a number of sensor nodes usually deployed in difficult-to-access locations working together to monitor a region to obtain data about the environment. Sensor nodes are small low power devices equipped with one or more sensors, a processor, memory, a power supply, and a radio unit. These units are implemented for wireless communications and to transfer the data to a base station where sensor data is analyzed. Many reasons make measured and collected data, by WSNs,unreliable: First, transmitted data streams in the Wireless Network is delicate to errors and sensitive to noise caused by the nature of radio transmissions. Second, the low quality of sensor nodes, including limited computational capacity,restricted energy resources and particularly little communication range, causes sometimes loss of data in the network. The risk to have erroneous, missed or redundant data is high with considering the environmental effects. To improve the quality of sensor data measured by the network, detection of outliers is primordial to ensure reliability and accuracy and to deploy robust, efficient and secure wireless sensor network. The principal problem of outlier detection is due to fraudulent behavior, some changes in system behavior, mechanical faults,instrument error, human error or simply through natural deviations in populations.

ANOMALY DETECTION IN WSN: Anomalies are observations that do not correspond to a well defined notion of normal behaviors. [3] n WSNs, anomalies can occur in the nodes, networks, transmission channels and application data and can be caused by systematic errors,random errors and malicious attacks.

A. Types of anomalies

Anomalies in WSNs can be [4] classified into three broad categories.

- Node anomaly
- Network anomaly
- Data anomaly

Node Anomalies occur due to fault at single node. Main reason behind this anomaly is battery issue, i.e. battery failure or depletion. The node fault occur due to deployment of nodes in harsh environment

OUTLIER DETECTION IN WIRELESS SENSOR NETWORKS

We describe a fundamental of Outlier Detection in WSNs,including definitions of outliers, different use of outlier, and events of outlier detection in wireless sensor networks.

A. Outlier Definition

In WSNs, outliers can be defined as, “those measurements that significantly deviate from the normal pattern of sensed data" [4]. So outlier represents the subset of measurements that deviate in a clear manner from the normal model of sensed data in WSN where sensor nodes are assigned to monitor the physical world and thus a model or a pattern representing the normal behavior of sensed data may exist.

There are many definition of outlier. So, “*Grubbs*” defines outlier as: "An outlying observation, or outlier, is one that appears to deviate markedly from other members of the sample in which it occurs". Outlier is the value that deviates from other values of the same set.Then “Hawkins”: "An outlier is an observation, which deviates so much from other observations as to arouse suspicions that it was generated by a different mechanism". Outlier is the observation generated by different mechanism and witch significantly deviates from other observations.Also, “Barnett and Lewis” have mentioned that an outlier is a subset of observations which appears to be inconsistent with the remainder of that set of data". Outlier is an inconsistent observation in the same set of data [5].

B. Use of Outlier Detection in WSNs

Outlier detection or also called anomaly detection or deviation detection is one of the fundamental tasks in data mining which also includes predictive modeling, cluster analysis and association analysis.Besides, it was subject of research in many domains such as statistics, data mining, machine learning, information theory,and spectral decomposition [6]. Also, it has been widely applied to numerous applications domains such as fraud detection, network intrusion, performance analysis, weather prediction, etc.Outlier detection is an efficient way to find values that deviate significantly from the other measured data in the network. The value added by outlier detection appears in many real-life applications:

(i) Environmental monitoring, in which sensors such as temperature and humidity are deployed in harsh and unattended regions to monitor the natural environment. Outlier detection can identify when and where an event occurs and triggers an alarm upon detection.

(ii)Health and medical monitoring, in which patients are equipped with small sensors on multiple different positions of their body to monitor their well-being.Outlier detection showing unusual records can indicate whether the patient has potential diseases and allow doctors to take effective medical care.

(iii)Industrial monitoring, in which machines are equipped with temperature, pressure, or vibration amplitude sensors to monitor their operation. Outlier detection can quickly identify anomalous readings to indicate possible malfunction or any other abnormality in the machines and allow for their corrections.

(iv)Target tracking, in which sensors are embedded in moving targets to track them in real-time. Outlier detection can filter erroneous information to improve the estimation of the location of targets and also to make tracking more efficiently and accurately.

Event Detection in Wireless Sensor Networks

In the literature, WSNs are classified in accordance with four data delivery models: continuous, event-driven, observer initiated and hybrid. In event-driven type, sensors will reply to a request from applications. This model is the most deployed in WSNs applications due to their reactive behavior and the energy expenses of this model are low, when compared to the other cited approaches.

Event detection based applications such as military applications for detection of the invasion of enemy forces,health monitoring for detection of abnormal patient behaviour , fire detection for setting an alarm if a fire starts somewhere in the monitored area uses techniques to describe events in a way that sensor nodes can understand them using precise values to specify event thresholds [7].

Event detection techniques includes sql-like primitives, Petri nets extensions, stochastic methods such Bayesian classifiers and Hidden Markov Models and Fuzzy logic approaches to improve accuracy of event identification. It differs from outlier detections ones for many reasons: they have a priori knowledge of trigger condition or semantic of certain event issued by the sink node [8]. Furthermore, outlier detection techniques aim is to keep the detection rate high and the false alarm rate low by reducing the possibility to classify a normal value as outlier while event detection methods try to exclude erroneous data so that it is not believed as event condition or pattern.

DIFFERENT CLASSIFICATION CRITERIA

Here, we discuss different important aspects and classification criteria of outlier detection techniques developed for Wireless Sensor Networks. We start with differentiate between local models generated from data streams of individual nodes and the global one.

A. Types of Outlier

The outlier has divided into two types which are:

(i) Local Outliers: this type requires that each node identifies the abnormal values only depending on its

historical values [6]. Each sensor node collects the transmitted data of its neighboring nodes to identify the anomalous values. Due to the fact that local outliers are identified at individual sensor nodes, techniques for detecting local outliers save communication overhead and enhance the scalability.

(ii) Global Outliers: this is the second type of outlier. We can perform and identify global outliers at different levels in the network [6]. For example, in a centralized architecture, all data is transmitted to the sink node for identifying outliers. This mechanism consumes much communication overhead and delays the response time.

B. Sources of Outlier in WSNs

We present three sources of outliers occurred in WSNs:errors, events, and malicious attacks.

1) Errors

An error refers to a noise-related measurement or data coming from a faulty sensor [9]. Outliers caused by errors may occur frequently, while outliers caused by events tend to have extremely smaller probability of occurrence. Erroneous data is normally represented as an arbitrary change and is extremely different from the rest of the data.

2) Events

An event is defined as particular phenomena that change the real-world state, e.g., forest fire, chemical spill, air pollution, etc [10]. This sort of outlier normally lasts for a relatively long period of time and changes historical pattern of sensor data. However, faulty sensors may also generate similar long segmental outliers as events and therefore it is hard to distinguish the two different outlier sources only by examining one sensing series of a node itself.

3) Malicious attacks

Attacks can be classified into two major categories, according the interruption of communication act, namely passive attacks and active attacks. For the first category, the attack obtains data exchanged in the network without interrupting the communication. For the second category referred to an active attack it can be affirmed that the attack implies the disruption of the normal functionality of the network, meaning information interruption, modification, or fabrication. Examples of passive attacks are eavesdropping,traffic analysis, and traffic monitoring. Examples of active attacks include jamming, impersonating, modification and message replay.

C. Need of outlier detection in WSN

Outlier is used for finding errors, noise, missing values, inconsistent data, or duplicate data. This abnormal value may affect the quality of data and reduces the system performance. The use of Outlier detection technique is very important in several real life applications, such as, environmental monitoring, health and medical monitoring, industrial monitoring, surveillance monitors and target tracking [3].In wireless sensor networks, the sensors have low cost and low energy, so to improve the quality and performance, the better solution is to use outlier detection technique.

D. Problems in outlier detection in WSN

We can summarize many problems in detection of outliers in WSNs as follows:

a. High communication cost

b. Modeling normal objects and outliers effectively

c. Application specific outlier detection

d. Identifying outlier source

e. Distributed data

f. Communication failures frequently

g. Dynamic network topology

INTRUSION DETECTION

Intrusion Detection was developed to recognize and report the attack in the late 1990s, as hacker’s attacks and network worms began to affect the internet, it detected hostile traffic and sent alerts but did nothing to stop the attacks . It has been a long road for Intrusion Detection System (IDS), almost two decades since it has become a major issue [1]. In other words, Intrusion Detection is passive rather than active. It is not able to detect all malicious programmes and activities most of the time and incompatible to integrate with control restriction to restrict traffic inbound-outbound from attacking; which means it was only capable to detect attack actions, without prevention action. Intrusion Prevention System (IPS) is primarily a network-based defence system, with rising global network connectivity and combines the technique firewall with that of IDS properly with proactive techniques. When an attack is identified, intrusion prevention blocks and logs down the offending data. Currently, requirement for a system to provide early detection / warning from intrusion security violation with databases knowledge based has become a necessity.

This mechanism is activated to stop or allow packet data to process associated with the event. It prevents attack before it enters the network by examining various data records and prevents the demeanour of pattern recognition. Currently, requirement for a system to provide early detection / warning from intrusion security violation with knowledge based has become a vital necessity. Therefore, the system must be active and smart in classifying and distinguish the packet data, if curious or mischievous data are detected, alert is triggered and event alert response is executed

RELATED WORK OF IPS

Based on the previous section, in order for places to counter security threat, this current needed an integrated solution that is renewable and not avoidable. The roadmap for development of detection, early detection and prevention system are represented in Figure 1. It started earlier in the IDS solution by [4], presenting the taxonomy and existing tools used of IDS. Furthermore, previous work by [5], proposes automatic early warning system to make prediction and advice regarding malware based on database and repository of threat. These early detection concepts has been introduced by [6], which describes differentiate types of operation mode IDS, IPS and Intrusion Response System (IRS), they compare it on the basis of literature product with features such as proactive, reactive and passive. The trend of behaviour analysis to efficient data collection is describe to improve the performance of sensors in the real-traffic network, due to the network traffic captured on high speed links is always a challenge to capacity issues. This means that early detection, protection and response system act as an elementary of IPS.

It is expanded on the functionality provided by IDS by enabling to prevent attack against of network. As mentioned previously, early detection and intrusion response has the fundamental part of intrusion prevention mechanism in recent network security challenge, this was confirmed performed. Responding to this issue, some researchers have proposed several different detections and response mechanisms to complement the existing prevention mechanism [10] they were declared intrusion response as having similar function as IDS and part of it, by maintaining detection, alerting and response to security operator. IPS functions as radar to monitor stream network traffic; detecting, identifying, and recognising any signal that could be regarded a security violation.

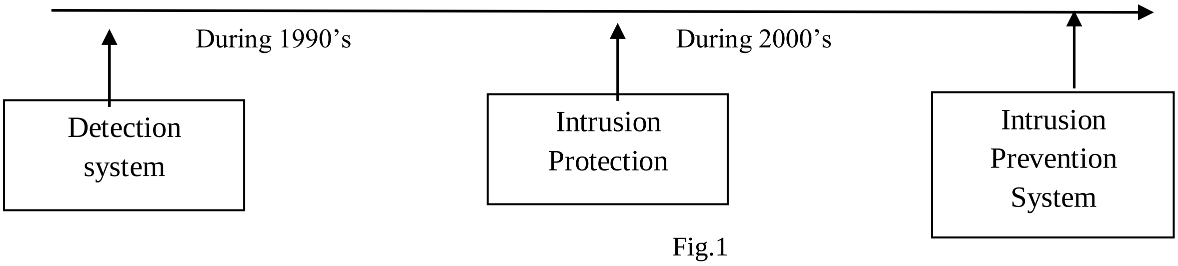

Fig.1

INTRUSION PREVENTION SYSTEMS: Traditionally, firewalls and anti-virus programs try to block attacks but IDS tries to identify attacks as it occurs. Such techniques are critical to defence in depth approach to security, but have some limitations. A firewall can restrict services by blocking certain ports but it does very little to evaluate traffic that uses allowed ports. IDS can evaluate traffic that travels through these open ports but cannot restrict it. IPS can proactively block the attacks. Signature based approaches focuses on how an attack works, trying to detect certain strings in them. If an attacker makes minor changes by using the IDS evasion techniques discussed above, then previously written signatures no longer can detect the attack. IPS focuses prevention, instead on what an attack does, which does not change. IPS popular Approaches Some of the approaches being used are as follows 1. Software based heuristic approach - This approach is very similar to IDS anomaly detection using neural networks with additional ability to act against intrusions and block them. 2. *Sandbox* approach - Mobile code like ActiveX, Java applets and various other scripting languages are quarantined in a *sandbox* - an area with restricted access to rest of the system resources. The system runs the code in this *sandbox* and monitors it's activities. If the code violates a predefined policy it is stopped and prevented from executing, thwarting the attack. 3. Hybrid approach –On network-based IPS (NIPS), various detection methods, some of the proprietary including protocol anomaly, traffic anomaly, and signature detection work together to determine an imminent attack and block traffic coming from an inline router. 4. Kernel based protection approach – It is used on host-based IPS (HIPS). Most operating systems restrict access to the kernel by a user application. The kernel controls the access to system resources like memory, I/O devices, and CPU, thus preventing direct user access. In order to use resources user applications send requests or system calls to the kernel, which then carry out the operation. Any of the exploited code will execute at least one system call to gain access to privileged resources or services. Kernel based IPS prevents execution of malicious system calls in the system.

CONCLUSION: It is obvious that we need protection against wireless threats. However, a real-time wireless intrusion detection tool for detection/ removal of rogue access points is vital for any organization. The development of new wireless standards and security protocols is expected to improve the WLANs' security, but we also estimate that wireless intrusion prevention systems will continue to play a vital and important role in assuring the organization's security for the next generations. In this paper, we address the problem of anomaly detection in WSNs. We also provide information about anomalies in WSNs, desirable properties of any anomaly detection techniques designed for WSNs.In this paper we discussed the problem of outliers in wireless sensor networks. We also discussed a classification of outlier detection techniques based on some criterion.

REFERENCES :

[1.]Sandeep B. Vanjale; P. B. Mane; Sandip V. Patil," Wireless LAN Intrusion Detection and Prevention system for Malicious Access Point",Computing for Sustainable Global Development (INDIACom), 2015 2nd International Conference,pp 487 – 490,2015

[2.]S V Athawale; D N Chaudhari," Towards effective client-server based advent intrusion prevention systemfor WLAN ", Computer, Communication and Control (IC4), 2015 International Conference on Year: 2015,pp 1 - 5, 2015.

[3.]Zhang, Y.; Meratnia, N.; Havinga, P.J.M. Outlier detection techniques for wireless sensor networks: A survey. *IEEE Commun. Surv. Tutorials* **2010**, *12*, 159–170.

[4.]K. Kapitanova, S.H. Son, and K. D. Kang. Event Detection in Wireless Sensor Networks. Second International Conference,ADHOCNETS 2010, Victoria, BC, Canada, August 18-20,2010.

[5.]Yujia Zhang; et al. ," An overview of wireless intrusion prevention systems, Communication Systems, Networks and Applications (ICCSNA), pp 147-150,2010.

[6.]Yaqing Zhang,Srinivas Sampalli,"Client-based Intrusion Prevention System for 802.11 Wireless LANs",2010 IEEE 6th Intemational Conference on Wireless and Mobile Computing. Networking and Communications, pp 100-107,2010.

[7.]Boulis, A. Castalia: Revealing Pitfalls in Designing Distributed Algorithms in WSN. In *Proceedings of the 5th International Conference on Embedded Networked Sensor Systems (SenSys)*, Sydney, Australia, 6–9 November 2007.

[8.]Hai, T.H.; Khan, F.I.; Huh, E. Hybrid Intrusion Detection System for Wireless Sensor Networks.In *Proceedings of International Conference on Computer Science and Applications*, San Francisco,CA, USA, October 2007.

[9.]S. Rajasegarar, C. Leckie, M. Palaniswami, J. C., Bezdek."Distributed anomaly detection in wireless sensor networks",Proceedings of IEEE ICCS, 2006.

[10.]I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci,"Wireless sensor networks: a survey," Computer Networks, vol.38, no. 4, pp. 393- 422, March, 2002.