International Journal of Innovative Research in Technology and Management (IJIRTM), Volume-2, Issue-3, 2018.
www.ijirtm.com *ISSN: 2581-3404 (Online)*

A Review on Malicious Attack Detection in Wireless Sensor Network

Vivek Kirar[1], Prof. Jitendra Mishra[2]
[1]M. Tech Scholar, Department of EC, PCST, Bhopal (India)
[2]Head & Professor, Department of EC, PCST, Bhopal (India)
[1]kirar.vivek@gmail.com, [2]jitendra.mishra260@gmail.com

ABSTRACT
This paper presents an overview of the technologies and the methodologies used in Intrusion Detection Systems (IDS). Intrusion Detection System (IDS) technologies are differentiated by types of events that IDSs can recognize, by types of devices that IDSs monitor and by activity. Intrusion Detection is the process of monitoring the information systems by sensors or agents and analyzing the collected information to detect and to attempt to stop the attacks in real time, identifying vulnerabilities, the violation of security policies or standard security practices

Keywords: Attack detection, Wireless Sensor Network, Intrusion detection system, firewall, anomaly detection.

INTRODUCTION
Current state of the art in Wireless Sensor Networks (WSNs) includes a substantial number of security mechanisms [3]. Nevertheless, an adversary can still compromise sensor nodes by exploiting software vulnerabilities or through physical attacks. Compromised sensors pose a severe threat to data integrity as they can report arbitrary data instead of real measurements. Such threat also propagates to IoT applications that build on top of compromised WSNs, such as emergency management, network security, health monitoring, and Vehicle control [3]. Along with growing reliance on wireless networking technology in recent years, the challenges of wireless network security have been increasing [5]. One of the pivotal elements in wireless network security is the wireless intrusion detection system (WIDS) that is considered as a second line of defense for detecting any leaked attacks form the first line of defense such as firewall and encryption. Characteristics of WIDSs do not deviate much more from the wired intrusion detection systems (IDSs); just the RF (radio frequency) sensors, wireless communication features and wireless attack features are taken into account for WIDSs.

The chance of detecting malicious data injections depends on the ability to exploit correlation as well as

on the attack's sophistication. We envisage that malicious measurements can be injected with any sophisticated strategy that maximizes the damage to the WSN and minimizes the risk of being detected. This is possible if compromised nodes collude, i.e., act in concert towards a common goal [1].

There are two principal approaches for detection, intrusion: Misuse detection based on rules, these rules will look for signatures on the network and then system operations try to catch known attack that should be considered as Misuse [14]. Anomaly detection [14], which based on the normal behavior of a system, it compares normal activities against observed events to identify significant deviations. The main scope of this paper is to improve that random forest technique is an efficient anomaly detection technique for IDS in WSN, with a comparative evaluation study for the most recent and performants anomaly detection technique used in IDS for WSN. If the malicious behavior of the user falls under the accepted behavior, then it goes unnoticed. An activity such as directory traversal on a targeted vulnerable server, which complies with network protocol, easily goes unnoticed as it does not trigger any out-of-protocol, payload or bandwidth limitation flags [6].

Sensors can be broadly classified as either passive or active based on the source of energy being sensed. Passive sensors measure ambient energy. For example, temperature sensors like those found in thermostats are considered passive, because they measure heat energy

in the ambient environment. By contrast, active sensors probe some physical entity with self-generated energy. This energy is partially reflected back to the sensor where it is measured and used to infer properties about some physical phenomenon [2].

The boundary is an important feature, since we assume that the first line of defense in most systems - the perimeter does not apply to an insider. The boundary may be a national boundary, the physical limits of a place of work, a logical boundary defined by electronic technology, or the combination of physical and logical boundaries that define an organization [8].

The rest of this paper is organized as follows in the first section we describe an introduction of about the wireless sensor network attack detection. In section II we discuss about the support vector machine classifier. In section III we discuss about the rich literature for attack detection. In section IV we discuss about the problem formulation and statement as we getting from the rich literature survey, finally in section V we conclude the about our paper which is based on the literature survey and specify the future scope.

II SUPPORT VECTOR MACHINE CLASSIFIER

Support Vector Machines (SVMs) are supervised learning algorithms, which have been applied increasingly to anomaly detection in the last decade. One of the primary benefits of SVMs is that they learn very effectively from high dimensional data [14]. In WSN SVM is used to investigate spatial and temporal correlations of data for detecting suspect behavior of a node. Many researchers have tried to find possible methods to apply SVM classification for large data sets. Sequential Minimal Optimization (SMO) is a fast method to train SVM, which breaks the large Quadratic Programming (QP) problem into a series of smallest possible QP problems. One-class quarter-sphere SVM, as a representative algorithm of SVM, is also suited to distribute anomaly detection [28]. First, the local quarter-sphere is computed at each common sensor node. Second, the cluster heads collects these locally computed radii to work out a global radius. Detection is then launched at each common sensor node with the global normal profile.

III RELATED WORK

In this section we discuss about the rich literature survey for the malicious attack detection in a network.

[1] In this paper they have focused on detecting malicious data injections in WSNs, in particular when one or more events can occur and collusion between compromised sensors exploits the loss in correlation brought in by them. They have proposed a novel methodology to detect malicious data injections, based on the measurements cross-scale relationship. In addition, they have provided an approach to characterize malicious colluding nodes, by partitioning the sensor nodes based on the correlation between their measurements.

[2] This work presents PyCRA, a physical challenge-response authentication scheme designed to protect active sensing systems against physical attacks occurring in the analog domain. PyCRA provides secure active sensing by continually challenging the surrounding environment via random but deliberate physical probes. By analyzing the responses to these probes, the system is able to ensure that the underlying physics involved are not violated, providing an authentication mechanism that not only detects malicious attacks but provides resilience against them.

[3] In this paper they compare the benefits and drawbacks of both techniques and seek to determine how to best combine them. However, our study shows that no single solution exists, as each choice introduces changes in the measurements collection process, affects the attestation protocol, and gives a different balance between the high detection rate of attestation and the low power overhead of measurements inspection. .therefore, we propose three strategies that combine measurements inspection and attestation in different ways, and a way to choose between them based on the requirements of different applications.

[4] This paper will focus on digital vulnerabilities within the smart grid and how they may be exploited to form fully fledged attacks on the system. A number of countermeasures and solutions from the literature will also be reported, to give an overview of the options for dealing with such problems. This paper serves as a triggering point for future research into smart grid cyber security. Multiple issues of importance to smart grid cyber security were studied and discussed. These include the smart metering infrastructure, power line communication, distributed energy resources, and network systems.

[5] This paper developed a holistic taxonomy of wireless attacks from the perspective of the WIDS evaluator. This proposed taxonomy helps in generating all possible attack test cases and extracting the valid representative ones. Their proposed taxonomy respects the requirements of the satisfactory taxonomy, taking into account all the sufficient and necessary dimensions for wireless attacks classification. They have followed

our taxonomy to generate and extract some representative attack test cases in wireless networks.

[6] This paper elaborates the foundations of the main anomaly based network intrusion detection technologies along with their operational architectures and also presents a classification based on the type of processing that is related to the "behavioral" model for the target system. This study also describes the main features of several ID˝s systems/platforms that are currently available in a concise manner. The most significant open issues regarding Anomaly based Network Intrusion Detection systems are identified, among which assessment is given particular emphasis.

[7] This paper presents an overview of the technologies and the methodologies used in Network Intrusion Detection and Prevention Systems (NIDPS). Intrusion Detection and Prevention System (IDPS) technologies are differentiated by types of events that IDPSs can recognize, by types of devices that IDPSs monitor and by activity. NIDPSs monitor and analyze the streams of network packets in order to detect security incidents. The main methodology used by NIDPSs is protocol analysis. Protocol analysis requires good knowledge of the theory of the main protocols, their definition, how each protocol works.

[8] This paper proposes a scalable solution to this problem by maintaining long-term estimates that individuals or nodes are attackers, rather than retaining event data for post-facto analysis. These estimates are then used as triggers for more detailed investigation. They identify essential attributes of event data, allowing the use of a wide range of indicators, and show how to apply Bayesian statistics to maintain incremental estimates without global updating. The paper provides a theoretical account of the process, a worked example, and a discussion of its practical implications.

[9] This paper review some of the existing en-route filtering schemes and analyses the performance of those en-route filtering schemes based on their filtering efficiency. Finally a case study about some of the en-route filtering scheme is provided and this provided the aspects for the designers to implement suitable scheme to defend against false data injection attack. Wireless sensor networks are vulnerable to security attacks due to their unattended nature and deployment in hostile environment. Security attacks include false data injection, data forgery and eavesdropping. Adversaries can inject false data reports into the WSN through compromised nodes.

[11] In this article, how WSN differs from wired network and other wireless network and also basic information about the WSN and its security issues compared with wired network and other wireless networks is discoursed. Summarization of typical attacks on sensor networks and survey about the literatures on several important security issues relevant to the sensor networks are also dissertated. Security concerns constitute a potential stumbling block to the impending wide deployment of sensor networks.

[12] This paper review some of the existing en-route filtering schemes and analyses the performance of those en-route filtering schemes based on their filtering efficiency. Finally a case study about some of the en-route filtering scheme is provided and this provided the aspects for the designers to implement suitable scheme to defend against false data injection attack. In addition a review about possible attacks on communication in WSN is described. En-route Filtering is an efficient way of dealing with false data injection attacks.

IV PROBLEM STATEMENT

Sensor networks are used in a number of domains that handle sensitive information. Due to this, there are many considerations that should be investigated and are related with protecting sensitive information traveling between nodes (which are either sensor nodes or the base station) from been disclosure to unauthorized third parties [10]. The idea of using primary tests or indicators to identify suspects who then warrant further investigation is an established financial management practice. Standard texts on fraud management specify tests that can be used to trigger further investigation, based on the likelihood that fraudsters' behaviour is sufficiently different from that of normal employees to be statistically significant [8]. The key concept is to move away from maintaining models of the behaviour or sequencing of individual attacks, since this in principle requires a hypothesis to be initiated for each event.

V CONCLUSIONS AND FUTURE WORK

The key challenge of evolving intrusion detection system in WSN is to identify attacks with high accuracy, and satisfied the required constraints and challenges, to prolong the lifetime of the entire network. In this paper we have focused on to present's vast survey to detecting malicious data injections in wireless sensor networks. In the future, we plan to implement the threat model to consider malicious attack. Wireless sensor networks are vulnerable to security attacks due to their unattended nature and deployment in hostile environment. Security attacks include false data injection, data forgery and eavesdropping.

REFERENCES:-

[1] Vittorio P. Illiano, Luis Mu~noz-Gonz_alez, Emil C. Lupu, "Don't fool Me!: Detection, Characterisation and Diagnosis of Spoofed and Masked Events in Wireless Sensor Networks", IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 14, NO. 3, MAY/JUNE 2017. Pp 279-293.

[2] Yasser Shoukry, Paul Martin, Yair Yona, Suhas Diggavi, Mani Srivastava, "PyCRA: Physical Challenge-Response Authentication For Active Sensors Under Spoofing Attacks", COMPUTER-COMMUNICATIONNETWORKS, 2015. Pp 1-12.

[3] Vittorio P.Illiano, Rodrigo V. Steiner, Emil C. Lupu, "Unity is strength! Combining Attestation and Measurements Inspection to handle Malicious Data Injections in WSNs", wisec, 2017. Pp 134-145.

[4] Carlos Lopez, Arman Sargolzaei, Hugo Santana, Carlos Huerta, "Smart Grid Cyber Security: An Overview of Threats and Countermeasures", Journal of Energy and Power Engineering, 2016. Pp 1-13.

[5] Khalid Nasr, Anas Abou El Kalam, Christian Fraboul, "generating representative attack test cases for evaluating and testing wireless intrusion detection systems", International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.3, May 2012, Pp 1-20.

[6] V. Jyothsna, V. V. Rama Prasad, K. Munivara Prasad, "A Review of Anomaly based Intrusion Detection Systems", International Journal of Computer Applications, 2011. Pp 26-35.

[7] Nicoleta STANCIU, " Technologies, Methodologies and Challenges in Network Intrusion Detection and Prevention Systems", Informatica Economica, 2013. Pp 144-152.

[8] Howard Chivers, John A. Clark, Philip Nobles, Siraj A. Shaikh, Hao Chen, "Knowing Who to Watch: Identifying attackers whose actions are hidden within false alarms and background noise", 2010. Pp 1-16.

[9] S.V. Annlin Jeba, B. Paramasivan, "False Data Injection Attack and its Countermeasures in Wireless Sensor Networks", European Journal of Scientific Research, 2012. Pp 248-257.

[10] Sunil Gupta, Harsh K Verma, A L Sangal, "Security Attacks & Prerequisite for Wireless Sensor Networks", International Journal of Engineering and Advanced Technology, 2013. Pp 558-567.

[11] T.Kavitha, D.Sridharan, "Security Vulnerabilities In Wireless Sensor Networks: A Survey", Security Vulnerabilities In Wireless Sensor Networks: A Survey, 2010. Pp 31-45.

[12] S.V.Annlin Jeba, B. Paramasivan, "an evaluation of en-route filtering schemes on wireless sensor networks", international journal of computer engineering & technology, 2012. Pp 62-73.

[13] Deepali Virmani, Ankita Soni, Shringarica Chandel, Manas Hemrajani, " Routing Attacks in Wireless Sensor Networks: A Survey", 2015. Pp 1-8.

[14] YOUSEF EL MOURABIT, ANOUAR BOUIRDEN, AHMED TOUMANARI, NADYA EL MOUSSAID, " Intrusion Detection Techniques in Wireless Sensor Network using Data Mining Algorithms: Comparative Evaluation Based on Attacks Detection", International Journal of Advanced Computer Science and Applications, 2015. Pp 164-170.

Vivek Kirar received his Bachelor`s degree in Electronics & comunication Engineering, in 2013. Currently he is pursuing Master of Technology Degree in Electronics & comunication (Digital communication) from PCST, (RGPV), Bhopal, Madhya Pradesh India. His research area include Wireless sesnor networks.

Mr. **Jitendra Kumar Mishra** he is Associate Professor and Head of the Department of Electronics and communication Engineering in PCST, Bhopal (RGPV). His received Master of Technology and Bachelor's of engineering

respectively in Digital communication from BUIT, Bhopal and from RGPV, Bhopal. He has more than 10 years of teaching experience and publish 25+ papers in International journals, conferences etc. His areas of Interests are Antenna & Wave Propagation, Digital Signal Processing, Wireless Communication, Image Processing etc.