International Journal Of Research In Advent Technology Vol.3 No.2, February 2015
E-ISSN: 2321-9637

A Survey on Hybrid Intrusion Detection of Cluster-Based Wireless Sensor Network

Miss R. khewale; Miss M. Ramteke; Miss D. Bawane;Miss S. Tathe, Miss T. padmagiriwar
Final Year B.E.(IT), Smt. Rajshree Mulak College Of Engineering For Women, Nagpur
Email:26shilpatathe@gmail.com

Abstract: Wireless Sensor Networks (WSNs) Play an important role in unprotected environment there will be a large number of distributed nodes for that security are very important. It is mostly used in military and civil etc. Intrusion Detection System in Wireless Sensor Networks is used to detect those malicious node or intruders. In this paper, we propose an Intrusion detection system (IDS) created in cluster- based Wireless sensor network (CWSNs). The capability of cluster head (CH) is better than Sensor Nodes (SNs) in CWSN. Therefore, a Hybrid Intrusion Detection System (HIDS) is designed in this research CH is used to detect intruders that decreases the consumption of energy. Many protocols of CWSN have been proposed, such as LEACH [4], TEEN [9], APTEEN [10], and PEGASIS [8] however, the lifetime of network can be extend by the intended HIDS.

Keywords: WSN, Cluster, Intrusion detection, Hybrid IDS, Anomaly detection, Misuse detection.

1. INTRODUCTION

Wireless Sensor Networks (WSNs) is a new technology which is mostly used in military and civil areas therefore WSNs is very popular research subjects because of Advancements in wireless communication. The function of WSN is to collect and monitor the information in specific environment. The SNs detect the given target and deliver the data to the sink using wireless communication and analyzed that data to find out the state of the target. However, due to the design of their hardware, WSNs have certain resource constraints such as low computation capability, small memory and limited energy.

There are various types of attacks. For example when WSN is applied to the battlefield, SNs are invaded by the enemy and destroyed. Similarly, IDS can help to develop the prevention system through acquired natures of attack. An Intrusion Detection System is used to detect the packets in a network which determine their possibility of being attackers. IDS prevent destruction of the system by raising an alarm before the intruder starts to attack. There are two modules of intrusion detection that is anomaly detection and misuse detection [1]. Anomaly detection has a high detection rate but the false positive rate is also high. Anomaly detection builds a model of normal behavior and compares the model with detected behavior. The misuse detection detects the attack type by comparing the past attack behavior and the current attack behavior. The misuse detection has high accuracy but low detection rate. By using those modules the Hybrid Intrusion Detection System is developed. The module of hybrid detection to gain both the advantages of anomaly detection and misuse detection [2].

The Hybrid Intrusion Detection System (HIDS) achieves the goals of high detection rate and low false positive rate. In this work, a HIDS is discussed in a Cluster based Wireless Sensor Network (CWSN). CH is used to detect the intruders in this proposed HIDS because it is one of SNs in the CWSN but the capability of CH is better than other SNs. It decreases not only the consumption of energy but also efficiently reduces the amount of information and the lifetime of WSN can be extended by the intend HIDS.

2. LITERATURE SURVEY

2.1 Background Study

2.1.1. Intrusion Detection System (IDS)

Intrusion Detection is a technique which is used to identify the attempt to disturbance the integrity, confidentiality, or availability of a resource. Intrusion Detection System (IDS) can be access in open and wireless environment to protect them against the attack by monitoring it. There is not any specific technique for detecting the attack .we need to monitor each and every node in the network if any intrusion has occurred. Intrusion detection consists of anomaly detection and misuse detection technique. It is also divided into host based and network based approaches. Because today we use modern technology that is mobile and laptop. The mobile is wireless communication device which is used everywhere. There is not any specific technique for detecting the attack .we need to monitor each and every node in the network if any

intrusion has occurred. Intrusion detection consists of anomaly detection and misuse detection technique. It is also divided into host based and network based approaches.

Host-based vs. Network-base Intrusion Detection

Detecting an intrusion most of most of intrusion detection system takes either network-based or host-based approach. When the system checks for the pattern which usually indicate malicious packet .IDS is a network based when it check the pattern in network traffic and it is host based when it check the pattern in log file.

Network based system (NIDS) observe the each packet passing through the network. It means they use raw packets as data sources. They typically utilize a network adapter running in promiscuous mode for monitoring and analyzing all the traffic in real-time as it travels across the network. They are able to look at the payload within a packet, to see which particular host application is being accessed, and to raise alerts when attack occurs on a code. NIDS are host-independent but can also be a software package installed on specific workstation.

Host-based systems (HIDS) are concerned with each individual packets and host. They are able to detect actions such as repeated failed access attempts or changes to critical system files, and normally operate by accessing log files or monitoring real-time system usage. In order for a HIDS to function, clients have to be installed on every host in the network. These clients reside on the hosts as processes and perform analysis on the audit data gathered locally, at the expense of the already limited resources of the hosts. Depend on detection techniques, IDS can also be divided into three categories as follows:

- Misuse detection systems
- Anomaly detection systems
- Specification-based detection

Misuse detection is also called as signature based intrusion detection. In misuse detection, the data is matched against known attack characteristics thus limiting the technique largely to known attacks even it exclude the variant of known attacks. Some reason to give the incoming packet is not perfect and does not match the data to the original present data. Legal or illegal behavior can be defined and observed behavior can be compared accordingly. Such a system tries to detect proof of intrusive activity irrespective of any knowledge regarding the background traffic, i.e. the normal behavior of the system [5].

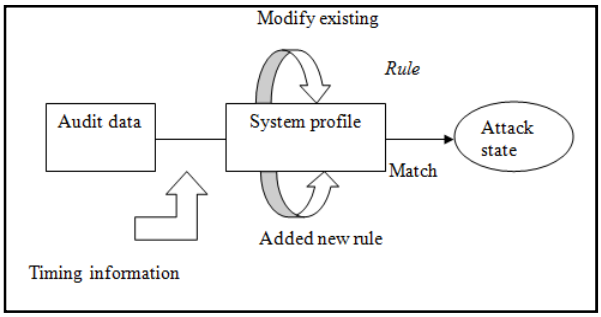

Figure 2.1 Misuse Detection Systems

In anomaly detection, shows side view of normal behavior of systems and also established through automated training. Anomaly detection are compared with the actual activity of the system to flag any significant deviation. A training phase in anomaly-based intrusion detection determines characteristics of normal activity; in operation, unknown activity, which is usually statistically significantly different from what was determined to be normal. Anomaly detection can detect unknown attacks, but often gives high false alarm rate [5]. One disadvantage of anomaly detection module computing is that the normal profile must be periodically updated and the deviations from the normal profile must be computed.

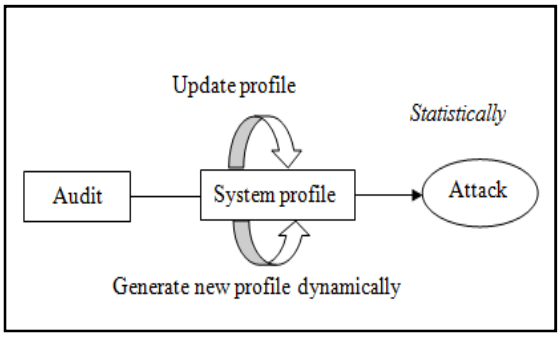

Figure 2.2 Anomaly Detection Systems

The periodic calculations can impose a heavy load on some resource constrained mobile devices, light-weight approach may involve comparatively less compute but it might be well suited.

Specification-based detection defines a set of compulsion that describes operation of a program or protocol, and monitors the execution of the program with respect to the defined compulsion. This technique provides the capability to detect previously unknown attacks, while displaying a low false positive rate. The detector operates by detecting the intrusion against the background of the normal traffic in the system. The detectors have good chance of detecting truly interesting events in the supervised system, since

they both know the patterns of intrusive behavior. It can relate to the normal behavior of the system.

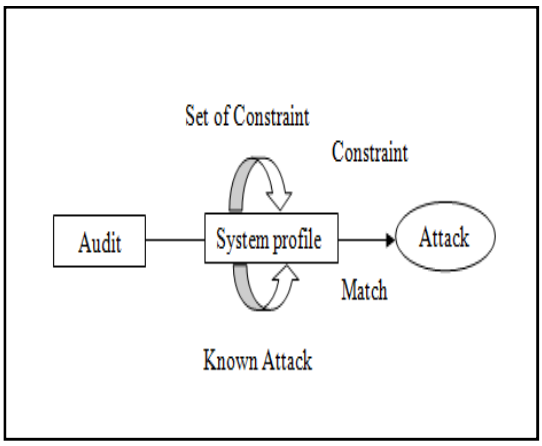

Figure 2.3 Specification based detection

3. CONCLUSION

In this paper, we propose the Hybrid Intrusion Detection scheme for cluster- based Wireless sensor network (CWSNs). In which we detect the malicious nodes. Result show that the Hybrid Intrusion Detection scheme detecting many attacks like black hole, wormhole, sync flood etc. It has been observed that these intrusion detection systems are not adequate for protecting WSN from intruders efficiently. The IDS is the need of the day for detecting intrusions accurately in an energy-efficient manner. It is exhausting the battery life very quickly. The aim of this proposed mode is to extend the lifetime of the WSN. Simulation proves the effectiveness of proposed model. At present work is on for more detailed analysis of HIDS in a simulated environment

REFERENCES

[1] O. Depren, M. Topallar, E.narim and M.K. Ciliz, "An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks," Expert Systems with Applications, 29(4), 2005, pp. 713-722.

[2] X. Du and F. Lin, "Improving routing in sensor networks with heterogeneous sensor nodes," Proceedings of IEEE 61st Vehicular Technology Conference, 4, 2005, pp. 2528-2532.

[3] W.R. Heinzelman, J. Kulik and H. Balakrishnan, "Adaptive protocols for information dissemination in wireless sensor networks," Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking, 1999, pp. 174-185.

[4] W.R. Heinzelman, A. Chandrakasan and H. Balakrishnan, "Energy-efficient communication protocols for wireless microsensor networks," Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, 2000, pp. 1-10.

[5] K. Jong, E. Marchiori, M. Sebag and A. van der Vaart, "Feature selection in proteomic pattern data with support vector machines," Proceedings of the Computational Intelligence in Bioinformatics and Computational Biology (CIBCB'04), 2004, pp. 41-48.

[6] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," Ad Hoc Networks, 1(2-3), 2003, pp. 293-315.

[7] R.A. Kemmerer and G. Vigna, "Intrusion detection a brief history and overview," Computer, 35(4), 2002, pp. 27-30.

[8] S. Lindsey and C.S. Raghavendra, "PEGASIS: Power-efficient gathering in
sensor information systems," IEEE Aerospace Conference Proceedings, 3, 20025, pp. 3-1125.

[9] A. Manjeshwar and D.P. Agrawal, "TEEN: a routing protocol for enhanced efficiency in wireless sensor networks," Proceedings of 15th International Parallel and Distributed Processing Symposium, 2007, pp. 2009-2015.

[10] A. Manjeshwar and D.P. Agrawal, "APTEEN: a hybrid protocol for efficient routing and comprehensive information retrieval in wireless sensor networks," Proceedings of the International Parallel and Distributed Processing Symposium, 2002, pp. 195-202.

[11] A. Murali and M. Rao, "A survey on intrusion detection approaches," Proceedings of the First International Conference on Information and Communication Technologies, 2005, pp. 233-240.

[12] Y. Qiao and X. Weixin, "A network IDS with low false positive rate," Proceedings of the 2002 Congress on Evolutionary Computation, 2, 2002, pp. 1121-1126.

[13]D.E. Philippe, Neural network models: theory and projects, London ; New York : Springer, 1997

[14] W.T. Su, K.M. Chang and Y.H. Kuo, "eHIP: An energy-efficient hybrid intrusion prohibition system for cluster-based wireless sensor networks," Computer Networks, 51(4), 2007, pp. 1151-1168.

[15] Y. Wang, G. Attebury and B. Ramamurthy, "A survey of security issues in wireless sensor networks," IEEE Communications Surveys & Tutorials, 8(2), 2006, pp. 2-23.

[16] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," Computer, 35(10), 2002, pp. 54-62.

[17]http://kdd.ics.uci.edu/databases/kddcup99/kddcup Proceedings of the International MultiConference of Engineers and Computer Scientists 2009 Vol I IMECS 2009, March 18 - 20, 2009, Hong Kong