ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 10, October 2013

Analytical Study on Hybrid Approach towards Intrusion Detection System for Wireless Sensor Network

Mr. Ansar I. Sheikh[1], Mr. Pankaj Kewadkar[2], Mr. Hitesh Gupta[3]
M.Tech. Scholar, Department of CSE, PCST, Bhopal, India[1]
Assistance Professor, Department of CSE, PIES, Bhopal, India[2]
Assistance Professor, Department of CSE, PCST, Bhopal, India[3]

Abstract: Wireless Sensor Networks (WSNs) are playing primary role in rising invasive platforms for various applications such as military & banking sector. It may have various malicious attacks on sensor network. It is necessary to prevent sensor network from these attacks for security purpose. This paper shows overview of WSN, intrusion detection in WSN, type of intrusion detection methodology and comparative scrutiny of existing method. This paper proposed hybrid intrusion detection system (HIDS) for cluster WSN.

Keywords: WSN, Intrusion detection, cluster, rule-based detection

I. INTRODUCTION

Security is a major issue for various protocol designers of WSN because of the broad security-critical applications of Wireless Sensor Networks (WSNs). Wireless Sensor Network is a type of network that places by a large number of small mobile devices with sensor functions. It is mainly used to collect, disseminate and process sensor information. Its features: large-scale, wireless, self-organizing, multi-hop, no-partition, no infrastructure support, its nodes are isomorphic, lower cost, smaller size.

To protect a network, there are usually several security related requirements, which should be considered in the design of a security protocol, including confidentiality, integrity and authenticity. An effective security protocol should provide services to meet these requirements. In many cases, no matter how carefully, a security infrastructure for a network is design, attackers may still find a way to break into it and launch attacks from the inside of the network. If they just keep quiet to eavesdrop on traffic flows, they can stay safe without being detected. If they behave more actively to disrupt the network communications, there will be some anomalies, indicating the existence of malicious intrusion or attacks. An intrusion can be defined as a set of actions that can lead to an unauthorized access or alteration of the wireless network system. Intrusion detection mechanisms can detect malicious intruders based on those anomalies. Intrusion detection system (IDS) attempts to monitor computer networks and systems, detecting possible intrusions in the network and alerting users after intrusions had been detected, reconfiguring the network if this is possible [18], [9]. Usually, the neighbors of a malicious node are the first entities learning those abnormal behaviors. Therefore, it is convenient to let each node monitor its neighbors such that intrusion detection mechanisms can be triggered as soon as possible.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 10, October 2013

Intrusion detection systems must be able to distinguish between normal and abnormal activities in order to discover malicious attempts in time. There are three main techniques that an intrusion detection system can use to classify actions [7]; misuse detection, anomaly detection and specification-based detection. In misuse detection or signature-based detection systems, the observed behavior is compared with known attack patterns (signatures). Action patterns that may pose a security threat must be defined and stored to the system. Then, the misuse detection system tries to recognize any "bad" behavior according to these patterns. It is already concluded from research in ad hoc networks that severe memory constraints make ID systems that need to store attack signatures relatively difficult to build and less likely to be effective [6]. It looks for behavior that matches the known attack scenario by analyzing the information in the network, comparing it to a large database for known attacks. Any new attack which is not in the database cannot be detected so the database must keep up to date, which is not easy to do in sensor networks.

Anomaly detection systems focus on normal behaviors, rather than attack behaviors. First these systems describe what constitutes a "normal" behavior (usually established by automated training) and then flag as intrusion attempts any activities that differ from this behavior by a statistically significant amount. Anomaly detection techniques look for the behavior that deviates from normal system activities. These techniques do not require knowledge of known attacks and can detect new type of intrusion which is considered more suitable for sensor network.

Finally, specification-based detection systems are also based on deviations from normal behavior in order to detect attacks, but they are based on manually defined specifications that describe what a correct operation is and monitor any behavior with respect to these constraints. This is the technique we use in our approach. It is easier to apply in sensor networks, since normal behavior cannot easily be defined by machine learning techniques and training.

The remainder of this paper is organized as follows:

Section II introduces the security issues and object to be detected in Wireless Sensor Networks. The existing methods of Intrusion Detection in Wireless Sensor Networks are discussed in Section III. In Section IV, existing methods are analyzed. The proposed model has discussed in Section V and concluded in Section VI.

II. INTRUSION DETECTION IN WIRELESS SENSOR NETWORK

A. Issues Related to security

Apart from other traditional networks, Wireless Sensor Network faced many security problems like active attacks, passive attacks, internal attacks, external attacks etc. Attacks can be divided into layers corresponding to the different protocols. Therefore there is a great demand for the Wireless Sensor Network security technologies.

The intrusion detection framework should be distributed and cooperative to suite the requirements of WSN. The framework includes the following layers:

• The network layer refers to the network topology of the WSN. Sensor nodes are the major participants of intrusion detection.

• The semantic layer refers to security ontology. We use ontology to represent formal semantics for WSN activities.

• The model layer refers to the intrusion detection model for single sensor node. The model determines the behaviors of sensor nodes. The major component of the model is a collection of rules for intrusion detection. The rules are pre-defined for target WSNs.

• The cooperative layer refers to the policy that how sensor nodes cooperate with each other for intrusion detection. Here we use a multi-agent system (MAS) to achieve the cooperation.

B. Object Detection

The objects of the WSN for intrusion detection mainly include the following:

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 10, October 2013

• Natural events: Environmental variables (temperature, humidity), based on statistical methods of the data [8], or using Hidden Model [13].

• System parameters: Carrier sense time, signal strength, and packets delivery ratio.

• Network data: Network status information, such as routing table information, changing in neighbor nodes.

• Custom parameters: Malicious node, key etc.

III. EXISTING METHODS OF INTRUSION DETECTION

A. Rule-based

Rule-based intrusion detection [11] is the collection and classification of data, the data is placed in a queue, using the FIFO principle. While monitoring the network this rules are selected appropriately and applied to the monitored data. If the rules defining an anomalous condition are satisfied, an intrusion is declared. The algorithm has three phases for detecting intrusions. In the first phase monitor nodes monitors the data. In the second phase the detection rules, are applied, in increasing order of complexity, to the collected information to flag failure. The third phase is the intrusion detection phase, where the number of failure flagged is compared to the expected number of the occasional failures in the network. Occasional failures include data alteration, message loss and message collision. An intrusion alarm is raised if the number of failures flagged exceeds the expected number of occasional failures. The rule base methods are fast, simple and require less data.

B. Multi-Agent Based

In WSN, Multi-Agent Distributed IDS (MAIDS) use the independent and autonomy characteristics of agent to increase system scalability and improve the problems caused by failure of single point, improve the system's fault tolerance. Utilizing the flexible programming of Agent, it save the cost of the system, it is easy to implement and it is dynamically start or stop [12]. The MAIDS utilizes multiple agents to achieve different modules of each intrusion detection unit. Each agent can communicate with each other, mutual cooperation as shown in Figure 1.

C. Data-mining based

Data mining techniques clustering algorithm, association rules mining, time series forecasting, are deeply used to monitor and fusion data for the WSN and provide tools for the analytical topology control, battery replacement strategies [15]. Nuclear clustering based anomaly detection program to detect routing attacks caused by traffic abnormalities. Through the use of Mercer nuclear, in order to better complete the cluster, to improve the detection accurate rate, extend the time dimension, so that better reflect the recent network traffic conditions, reducing the historical error rate.

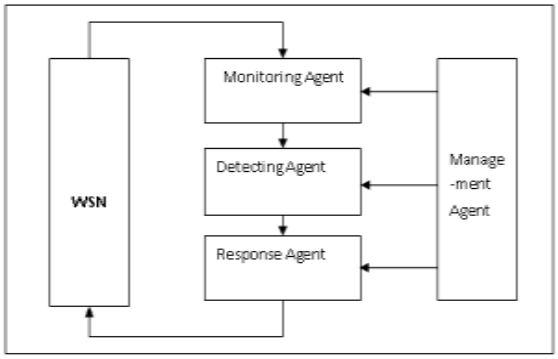

Fig 1. The Structure of Multi-agent based

D. Clusters-Based

Clustering is known as hierarchical of WSN [16]. To divide the network nodes into head cluster and members of nodes is the basic idea. Cluster head is the center of a cluster. Through cluster head's information fusion and forwarding to the member node of cluster, other members of nodes transmit to the base station.

E. Artificial Immune Based

In the traditional internet network, Paul K. Harmer [10] proposed artificial immune system architecture. This method gives a good artificial immune system model of WSN. Firstly, according to collect "clean" data set under the normal conditions, to extract data features and encode to the string set S which defined as "itself"; Then generates a random string collection, constitute the most original "Detector" R0 . Under the effect of negative selection, it

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 10, October 2013

compares the "detector" collection R0 with S and then clears the matched string and you will get the mature "detector" set R. When the network data appears the data which matches the string of set R, the "Detector" is activated. When the activation frequency exceeds a set threshold and then considers it intrusion behaviors. If "Detector" has not been matched in a period of time, the "detector" will be eliminated.

F. Hybrid Approach

In the Hybrid Approach [19], [17], the two techniques i.e. Cluster-Based and Rule-Based techniques are merged to form Hybrid detection technique. Hybrid detection used to gain the advantages of both Cluster-Based approach and Rule-Based approach. This combination provides simplicity, easy to operate, low consumption of energy and provide high safety. The Hybrid Intrusion Detection System (HIDS) achieves the goals of high detection rate and low false positive rate.

IV. ANALYSIS

Comparing analysis, for the advantages and disadvantages of different methods:

- Rule-Based: The Rule-Based method is simple, clear levels, easy to operate. But disadvantages are- low security level, need to establish an algorithm to solve security issues.
- Multi-Agent Based: This method reduces the network load, overcome network latency and good scalability, high security. This method requires large energy consumption, collision problem and low accuracy rate.
- Data Mining based: It can detect unknown complex attacks. It has high computational complexity, requires large amount of data samples and large energy-consuming.
- Cluster-Based: The cluster-based method requires low consumption, has high safety. Clustering is more complex algorithms, an increase of nodes' energy consumption. Cluster head node invasion, or encountered Sybil attack detection method is its failure, and its threshold settings affects the current network is a difficult problem.
- Artificial Immune Based: Has memory function ,but has high false alarm rate.
- Hybrid Based Approach: Decrease the amount of information in the network, increases detection rate, decreases false negative rate. It has high energy consumption, not accuracy rate up to the mark

V. PROPOSED MODEL – HIDS FOR CLUSTER BASED WIRELESS SENSOR NETWORK

The proposed HIDS consists of an intrusion detection module and decision making module. Intrusion detection module filters a large number of packet records using the rule base techniques. Decision making module is used to take an administrative action on the false node with the help of base station.

A. Proposed System Architecture

Here, the new Hybrid Intrusion Detection Model (HIDS) is proposed for Cluster Based Wireless Sensor Network (CWSN). This consists of two modules as shown in Figure 2**.** First, the Intrusion Detection Engine is used to filter the incoming packets and classify is as normal or abnormal. The packets identified as an abnormal are passed to the decision making module. The decision-making module is used to determine whether the intrusion occurs and the type of intrusion. Finally, returns to the base station to follow-up treatment.

In this proposed model, we used a hierarchical topology that divide the sensor network into clusters, each one having a cluster head (CH). Here the sensors nodes are fixed and

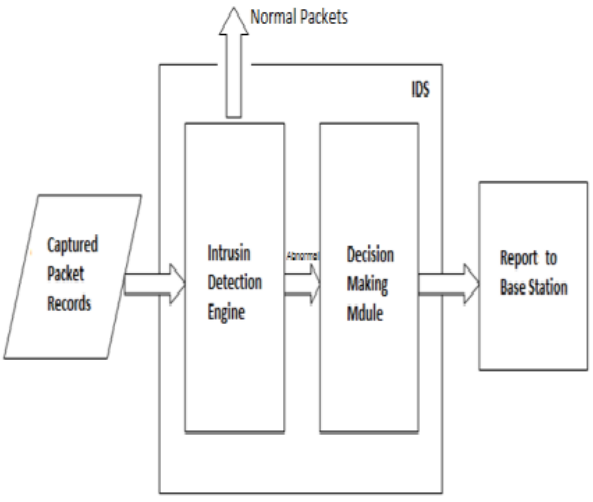

Fig 2. The proposed system architecture

assuming that the cluster heads having the more energy than the other sensor nodes. The objective of this architecture is to save the energy that allows the network life time prolongation and reduce the amount of

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 10, October 2013

information in the network. Some of the Cluster-based routing protocols founded in the literature are: LEACH [15], PEGASIS [16], and HEED [17].

B. Algorithm

Wireless Sensor Networks present a vast challenge in terms of implementation. Clustering algorithms play a vital role in achieving the targeted design goals for a given implementation. There are several key attributes that have been carefully considered, which are of particular importance in wireless sensor networks. It includes Cost of Clustering, Selection of Cluster heads and Clusters, Real-Time Operation, Synchronization, Data Aggregation, Repair Mechanisms, Quality of Service (QoS) etc.

In this proposed architecture, the wireless sensor network is divided into the small clusters. The hierarchical clustering is used to divide the sensor nodes. After the clustering process finished, the cluster head have been selected dynamically according to the current status of the nodes and formed the Cluster based WSN.

Generally, the node having highest energy left elected as a cluster head. Some form of clustering is almost always required for scalability in large-scale ad-hoc WSN deployments. Clustering reduces network contention by de-conflicting inter-cluster interference through lower transmit power, separate channels, or other spread-spectrum techniques, thereby improving spatial reuse. Reducing contention conserves energy and reduces latency in the network.

Clustering can also conserve energy by aggregating and fusing data at cluster heads for transmission to a base station.

In a CWSN, it is necessary for the packets to establish normal patterns of behavior for monitoring the status of packets. Therefore, in this, the rules-based analysis method is used to build intrusion detection module and the corresponding rules are defined by experts. The flow of construction can be divided into three steps, as follows.

Step 1: Analysis of network packets sent by the history. In CWSN, the packets, which pass through CH, are sent from: (1) The members of the cluster nodes; (2) The neighbor of CH, which chooses this CH as the transmission path. Therefore, the past packets that communicate on CH are collected to analyze and the packet is divided into two types, normal and intruder.

Step 2: Feature selection. Looking for identification of key features issued to distinguish between normal or abnormal packet.

Step 3: The establishment of anomaly detection rules.

VI. CONCLUSION

This paper has discussed various existing methods of intrusion detection of Wireless Sensor Network. The methods like Rule-based, Multi-agent based, Data Mining based etc. are worked up to the mark. But still intrusion detection in Wireless Sensor Network does not solved problems like low energy consumption, high detection rate, and improvement in detection of fault tolerance; protect inspection nodes safety and so on. With respect to the above problems, the new Hybrid Intrusion Detection Model is proposed which would solve existing IDS's system problem. It will be future work.

REFERENCES

[1] Hichem Sedjelmaci and Mohammed Feham ,"Novel Hybrid Intrusion Detection System for Clustered Wireless Sensor Network", IJNSA,Vol 3, No 4, July 2011.

[2] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications, Alaska, 11 May 2003, pp. 113-127.

[3] O. Younis, and S. Fahmy, "Heed: A hybrid, Energy-Efficient Distributed Clustering Approach for Ad Hoc Sensor Networks", IEEE Transactions on Mobile Computing, vol.3, No.4, 2004, pp.366-379

[4] S. Lindsey, and C. Raghavendra, "PEGASIS: Power Efficient Gathering in Sensor Information System", In Proc.IEEE Aerospace conference, vol.3, 2002, pp.1125-1130.

[5] W. R. Heinzelman, A. Chandrakasan , and H. Balakrishnan, "Energy Efficient Communication Protocol for Wireless Microsensor Networks", Proceeding of the 33rd Hawaii International Conference on System Sciences, IEEE, 2000, pp.1-10.

[6] A. Mishra, K. Nadkarni, and A. Patcha, "Intrusion detection in wireless ad hoc networks," IEEE Wireless Communications, vol. 11, no. 1, February 2004, pp. 48–60.

[7] S. Axelsson, "Intrusion detection systems: A survey and taxonomy," Department of Computer Engineering, Chalmers University of Technology, Tech. Rep. 99-15, March 2000.

[8] Shuai Liu, Jun-Jia Zhu and Ma Zhenyan, "wireless Sensor Network intrusion detection based on statistical anomalies(In Chinese)".

[9] R. Bace, "Intrusion Detection", MacMillan Technical Publishing, 2000.

[10] P. Harmer, P. Williams, G. Gunsch and G. Lamont, "AN artificial Immune System Architecture for Computer Security Applications", IEEE Transactions on Evolutionary Computation, Volume 6 issue 3, 2002, pp. 252-280.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 10, October 2013

[11] R.A. Kemmerer and G. Vigna, "Intrusion detection a brief history and overview," Computer, 35(4), 2002, pp. 27-30.
[12] O. Kachirski and R. Guha, "Intrusion Detection Using Mobile Agents in Wireless Ad Hoc Networks", IEEE Workshop on Knowledge Media Networking (KMN'02), Kyoto, JAPAN, 2002, pp 153-158.
[13] S. Doumit and D. P. Agrawal, "Self-organized Critically & stochastic learning based intrusion detection system for wireless sensor network", MILCOM2003-IEEE/ACM transactions on Networking, Vol. 11(1), 2003, pp 2-16.
[14] A. Paula, R. Da Silva, M. Martins and B. Roeha, "Decentralized Intrusion Detection in Wireless Sensor Networks", International Workshop on Modeling Analysis and Simulation of Wireless and Mobile Systems Proceedings of First ACM International Workshop on Quality of Services and Security in Wireless and Mobile Networks, 2005, pp 16-23.
[15] Z. Jun, " Study on Several Issues in Wireless Sensor Networks Based on Data Mining", Shanghai Jiao tong University master thesis 2007(In Chinese).
[16] R. Chen, C. Hsieh and Y. Huang, "A new Method for Intrusion Detection on Hierarchical Wireless Sensor Networks", ACM ICUIMC-09, Suwon, S. Korea, 2009.
[17] K. Q. Yan, S. C. Wang, S. S. Wang and C. W. Liu, "Hybrid Intrusion Detection of Cluster-based Wireless Sensor Network", Proceedings of International Multi-Conference of Engineers and Computer Scientists , Hong Kong, Vol. 1, 2009.
[18] J. Zheng and A. Jamalipour, "Wireless Sensor Networks: A Networking Perspective", a book published by A John & Sons, Inc, and IEEE, 2009.
[19] K. Q. Yan, S. C. Wang, S. S. Wang and C. W. Liu, "Hybrid Intrusion Detection System for Enhancing the Security of a Cluster-based Wireless Sensor Network", Chayang University of Technology, Taiwan, IEEE 2010, pp. 114-118

BIOGRAPHY

Ansar Sheikh is currently M.Tech. Student of Computer Science & Engineering, Department, PCST, Bhopal, India.