Engineering Sciences International Research Journal
ISSN (Print) : 2330 – 4338 ; Volume 1 Issue 1 ‖ February. 2013 ‖

Architecture for Intrusion Detection on IP Based Sensor Networks

V. Sowjanya[1], J. Sirisha[2], G. Lalitha Kumari[3], Y. Surekha[4]

Abstract: In this paper, we present architecture for intruder detection system that uses a wireless sensor network. The sensor network uses an unsupervised fuzzy Adaptive Resonance Theory (ART) neural network to learn and detect intruders in a previously unknown environment. Networks protection against different types of attacks is one of most important issue into the network and information security domains. This problem on Wireless Sensor Networks (WSNs), in attention to their special properties, has more importance. There are some of proposed solutions to protect Wireless Sensor Networks (WSNs) against different types of intrusions; but the proposed architecture in this paper has been a comprehensive view to this issue by presenting a complete Intrusion Detection Architecture (IDA). The main contribution of this architecture is its hierarchical structure; i.e. it is designed and applicable, in one, two or three levels, consistent to the application domain and its required security level. We have also learned that the software development process is very time consuming unless support for over-the-air reprogramming is implemented, and that the unpredictability of radio conditions make sensor node placement hard.

Keywords: Adaptive Resonance Theory (ART), Wireless Sensor Networks (WSN), Detection Architecture (IDA).

1. INTRODUCTION

Wireless sensor networks[1] have received a lot of attention from the research community during the last years. In WSNs there are two other compo-nents, called “aggregation points” (*i.e.* cluster-heads and CIDSs’ deployment locations) and “base station” (*i.e.* the central server and the WSNIDS’s deployment location), which have more powerful resources and capabilities than normal sensor nodes [2, 3]. As shown in **Figure 1**, aggregation points collect information from their nearby sensor nodes, aggregate and forward them to the base station to process gathered data [4].

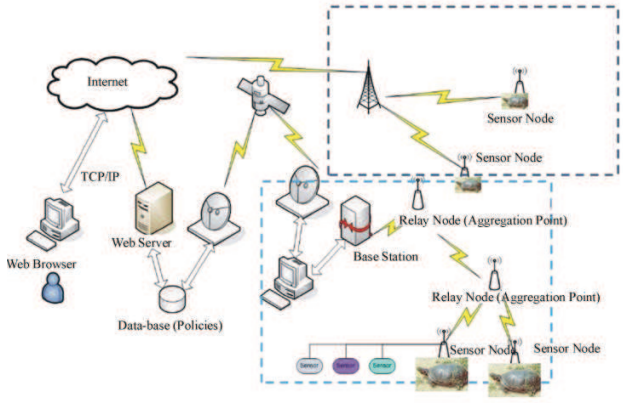

Fig. 1. WSNs’ communication architecture

To make it possible to bridge the sensor network over IP-based channels, such as GPRS or LANs, communication between the sensors within the sensor network. The TCP/IP support is provided by uIP [5], a complete TCP/IP implementation with a code size of only a few kilobytes requiring only few hundred bytes of RAM. This network is the _rst actual deployment of a fully IPbased wireless sensor network made of small and computationally constrained sensor nodes. This work points towards the possibilities with using TCP/IP for wireless sensor networks.

2. THE CONTIKI OPERATING SYSTEM

The sensor nodes run the Contiki operating system [6] developed at SICS. Contiki is lightweight system for communication oriented, memory-constrained devices such as tiny sensor devices. Contiki includes our uIP TCP/IP stack [5] and therefore has full TCP/IP support.

In order to ease software development and deployment, Contiki allows individual programs and services to be dynamically loaded and unloaded in a running system. We found that the simple protocol worked well in small networks, but we intend to implement more complex distribution methods (e.g. the Trickle protocol [7]) for larger network deployments.

3. INTRUSION DETECTION SYSTEM (IDS)

Intrusion, *i.e.* unauthorized access or login (to the system, or the network or other resources) [8]; intrusion is a set of actions from internal or external of the network, which violate security aspects (including integrity, confidentiality, availability and authenticity) of a network’s resource [9.10]. Intrusion detection is a process which detecting contradictory

activities with security policies to unauthorized access or performance reduction of a system or network [8]; the purpose of intrusion detection process is reviewing, controlling, analyzing and representing reports from the system and network activities. Intrusion Detection System (IDS), *i.e.*:

- A hardware or software or combinational system, with aggressive-defensive approach to protect information, systems and networks ;
- Usable on host, network and application levels;
- Informing and warning to the security manager (sometimes disconnect suspicious communications and block malicious traffic);
- Determining identity of attacker and tracking him/ her/it;

3.1 IDS Categorization

3.1.1. Host-Based Intrusion Detection System (HIDS)

HIDS installs on a computer system [11, 12]; it uses processor and memory of that system and protects only the hosting system. It has an abnormal detector part which using statistical methods to detect abnormal behavior of users in comparison to their behavioral records [13, 14].

3.1.2. Network-Based Intrusion Detection System (NIDS)

NIDS is a software process which installs on a special hardware system in many cases, it operates as a sniffer and controls passing packets and active communications, and then it analyzes network traffic in sophisticated, to find attacks. NIDS can identify at-tacks, on network level; thus, it includes following steps:

- Setting up the Network Interface Card (NIC) on promiscuous mode and eavesdropping total network traffic [15];
- Capturing the transmitting network packets
- Extracting requirement information and properties from them (the packets);
- Analyzing properties and detecting statistical deviation from normal behavior and known patterns (using pattern matching);
- Producing and logging proper events;

4. INTRUSION DETECTION ON WIRELESS SENSOR NETWORKS (WSNS)

Intrusion detection in WSNs has many challenges, mainly due to lack or weak of resources [16, 17]. Besides, the existent methods and protocols of traditional net-works can not be enforced to the WSN, directly; because they need to the resources which attending to the WSNs' limitations and constraints are inaccessible. In general, WSNs are application-oriented *i.e.* they are de-signed as cover the very special properties according to the target application domain. Intrusion detection process is supposing that the behavior of normal system is differentiating than the behavior of attacked system.

4.1. Main Challenges in Designing IDS for WSNs

There are a lot of challenges in designing IDS for WSNs; as follows described:

- Designing efficient software to store and install on the sensor nodes, cluster-heads and the central server, to saving existent energy consumption; as a result, leading to increase the network lifetime;
- Limited resources;
- Repeated failures and unreliable sensor nodes;
- Application-oriented networks;
- Requiring to the monitoring, detecting, decision making and responding to the intrusions, in real-time and fast; then leading to minimum damages;
- It is difficult to time synchronizing nodes into the WSNs; so, it is difficult to using protocols that are relying on time synchronization;
- Databases challenges: the volume of sensed data in the dynamic and mobile WSNs; proper storage medium; supporting different queries from sensor nodes, cluster-heads and the central server in network wide level;

5. NETWORK PROTOCOLS

One of the aims of our network was to make a first test of the viability of using the TCP/IP protocols for wireless sensor networking. The advantage of using IP in the sensor network is the issue of connectivity: with IP running within the sensor network, we can easily connect the sensor network to any other IP network, without protocol converters or proxies.

A. IP address assignment

Spatial IP address assignment uses the node's location to construct its address, unlike ordinary IP address assignment where IP addresses are assigned based on the network topology. Spatial IP address assignment assumes that sensors know their own location. This assumption is valid in many type of sensor networks, as sensor information may be useless unless it can be connected to a physical location. In our network, each sensor is configured with a location as the sensor is deployed.

ISBN: 978-93-81583-90-6

B. Event propagation using an overlay network

The network consists of two separate parts: a set of backbone nodes make up a backbone network, and a set of **sensor nodes** that send alarm events to the backbone. The backbone network replicates and transports alarm event information so that all backbone nodes will have a log of all recent events from the entire network. Backbone nodes periodically try to find each other by using broadcast messages.

6. THE PROPOSED INTRUSION DETECTION ARCHITECTURE (IDA) FOR WSNS

As **Figure 5** is showing, the suggested architecture has a combinational (distributed, in two low levels and centralized, in highest level) and hierarchical structure; thus, the proposed approach can be used in 1, 2 or 3 levels of IDSs, including SIDSs (on sensor nodes), CIDSs (on cluster-heads) and the WSNIDS (on the central server).

5.1. Sensor-Based Intrusion Detection System (SIDS: Sensor Node Level IDS)

In low level of the proposed architecture (sensor nodes), there is a simple IDS or Sensor-based IDS (SIDS/HIDS) per each sensor node. In each sensor node, there is a small policy-base that is including most common attacks in this domain along with special and limited preprocessing capabilities such as extracting the required data fields from the network packet. This IDS is signature-based; if an attack be detected, according to the determined response into the corresponding policy and security rule, it be responded (autonomous and independent decision making).

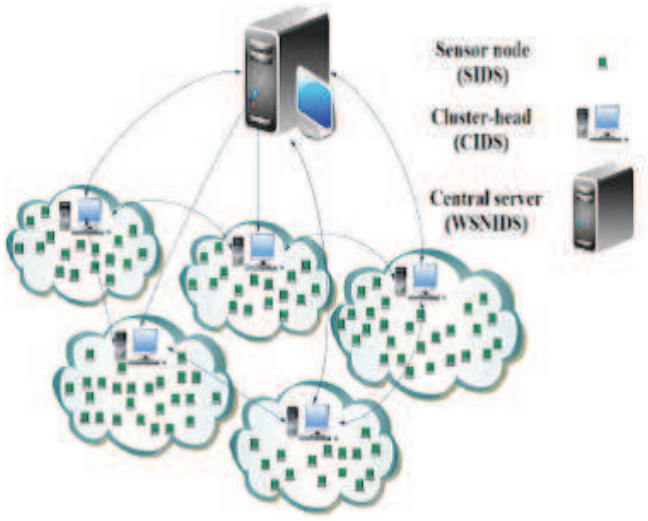

Fig. 5. The proposed Intrusion Detection Architecture (IDA) for WSNs.

5.2. Cluster-Based Intrusion Detection System (CIDS: Cluster-Level IDS)

CIDSs place on the medium level of the proposed architecture; *i.e.* they install and deploy on the heterogeneous cluster-heads. There is a cluster-head per each cluster of sensor nodes which it covers its radio range sensor nodes; so, the intrusion detection process does by cluster-heads. There is a small and low-size policy-base (Cluster-Based Policy Base: CBPB) on each cluster-head that includes the most common patterns of attacks on this domain, along with some preprocessing capabilities such as requirement data field extraction from the network packets and packets filtering. If an attack detects, according to the predefined actions into the policy-base and the corresponding security rule-base, the IDS is responding to it. In this level, decision is making in combinational; so, if the current traffic be from the internal of the cluster, the proper decision takes autonomously and independently.

7. CONCLUSION

The purpose of this paper is discussing the intrusion detection problem on WSNs and designing an Intrusion Detection Architecture (IDA) for these networks, of course by attending to their constraints. The suggested system depends on situations, the WSN's application area, the requirement security level and other things such as its cost, can be used and implemented in 1, 2 or 3 levels; including: SIDSs (monitoring the local host) on the sensor nodes, CIDSs (surveillance, monitoring and control in cluster-level) on the central management system.

Some of research areas in this domain to improve and extend the proposed model capabilities are:

- Improving response scheduling, priority responses and having more control on response production mechanism;
- Providing higher level of security, fault tolerant and robustness for suggested architecture;
- Centralizing more detailed information about system activities for forensic analysis;
- Efficient data management;

8. REFERENCES

[1] A. Mainwaring, J. Polastre, R. Szewczyk, D. Culler, and J. Anderson. Wireless sensor networks for habitat monitoring. In *First ACM Workshop on Wireless Sensor Networks and Applications (WSNA 2002)*, Atlanta, GA, USA, September 2002.

[2] S. Mohammadi, R. A. Ebrahimi and H. Jadidoleslamy, "A Comparison of Routing Attacks on Wireless Sensor Networks," *International Journal of Information Assurance and Security*, Vol. 6, No. 3, 2011, pp. 195-215.

[3] S. Mohammadi and H. Jadidoleslamy, "A Comparison of Transport and Application Layers Attacks on Wireless Sensor Networks," *International Journal of Information Assurance and Security*, Vol. 6, 2011, pp. 331-345.

[4] B. Krishnamachari, D. Estrin and S. Wicker, "The Im pact of Data Aggregation in Wireless Sensor Networks," *International Workshop on Distributed Event-Based Sys-tems*, Vienna, July 2002, pp. 457-458.

[5] A. Dunkels. Full TCP/IP for 8-bit architectures. In *MOBISYS`03*, San Francisco, California, May 2003.

[6] A. Dunkels, B. Gr¨onvall, and T. Voigt. Contiki - a Lightweight and Flexible Operating System for Tiny Networked Sensors. In *First IEEE Workshop on Embedded Networked Sensors*, 2004.

[7] P. Levis, N. Patel, D. Culler, and S. Shenker. Trickle: A self-regulating algorithm for code propagation and maintenance in wireless sensor networks. In *Proc. NSDI'04*, March 2004.

[8] R. A. Kemmerer and G. Vigna, "Intrusion Detection: A Brief History and Overview," *Computer Society*, Vol. 35, No. 4, 2002, pp. 27-30. Do I : ieeecomputersociety.org /10.1109 / MC.2002.10036.

[9] Ch. Krügel and Th. Toth, "A Survey on Intrusion Detec-tion Systems," TU Vienna, Austria, 2000.

[10] A. K. Jones and R. S. Sielken, "Computer System Intru-sion Detection: A Survey," University of Virginia, 1999.

[11] Ch. Krügel and Th. Toth, "A Survey on Intrusion Detec-tion Systems," TU Vienna, Austria, 2000.

[12] G. Maselli, L. Deri and S. Suin, "Design and Implemen-tation of an Anomaly Detection System: an Empirical Approach," University of Pisa, Italy, 2002.

[13] J. Molina and M. Cukier, "Evaluating Attack Resiliency for Host Intrusion Detection Systems," *Information As-surance and Security Journal*, Vol. 4, 2009. pp. 1-9.

[14] S. Zanero and S. M. Savaresi, "Unsupervised Learning Techniques for an Intrusion Detection System," *Proceed-ings of ACM Symposium on Applied Computing*, New York, 2004, pp. 412-419. doi:10.1145/967900.967988.

[15] A. K. Jones and R. S. Sielken, "Computer System Intrusion Detection: A Survey," University of Virginia, 1999.

[16] M. Saxena, "Security in Wireless Sensor Networks: A Layer-based Classification," Department of Computer Science, Purdue University, 2011. https://www.cerias.purdue.edu/apps/reports _HYPERLINKhttps://www.cerias.purdue.edu/apps/reports_and "and_papers/view/3106 .

[17] K. Scarfone and P. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)," NIST 800-94, Feb 2007.

[1]*Asst. Professor, Department of CSE, Prasad V Potluri Siddhatha Institute of Technology, Kanuru, Vijayawada.*
[2]*Asst. Professor, Department of IT, Prasad V Potluri Siddhatha Institute of Technology, Kanuru, Vijayawada.*
[3]*Sr.Asst.Professor, Department of CSE, Prasad V Potluri Siddhatha Institute of Technology, Kanuru, Vijayawada.*
[4]*Asst.Professor, Department of CSE, Prasad V Potluri Siddhatha Institute of Technology, Kanuru, Vijayawada.*