An Effective Hierarchical IDS for Wireless Sensor Networks

Amar Saraswat
Assistant Professor
Dronacharya College Of Engineering, Gurgaon

Vishal Bharti
Head of Department, CSE
Dronacharya College Of Engineering, Gurgaon

ABSTRACT
This paper emphasizes on safeguarding the hierarchical structure in wireless sensor network by presenting an Intrusion Detection Technique, which is very useful, simple and works effectively in improving and enhancing the security in wireless sensor Network. This IDS works on the combination of anomaly detection algorithm and intrusion detection nodes. Here all the features and numerous architectures of popular IDS(s) along with their confines and benefits are also being described.

Keywords
Anomaly Detection; Intrusion Detection; Wireless Sensor Network

1. INTRODUCTION
Wireless sensor network (WSN) usually consists of a large number of tiny sensor nodes (SNs) which are deployed in an operational area for sensing the data, aggregating and processing. Applications of WSN benefits includes Structural Monitoring, Bio-habitat monitoring, Industrial monitoring, Disaster management, Military surveillance, Home/building security, Object tracking, Underwater Research, Health Monitoring and various other fields are also benefited by the services of the WSN. Due to such services provided by the WSN, there is the rapid growth in the research field and it use [4]. WSN comprises of large no of small SNs having limited computational and communication capabilities

The exposure to natural environments and the inherent unreliability of wireless transmission make a WSN vulnerable to many attacks [1]. Securing WSN is the major concern. As there are certain limitations with the SN, such as constraints of energy, memory and computational power the traditional energy-consuming defense mechanisms like public key infrastructure [2] and host-based intrusion detection techniques [3] may not be feasible. Also, the problem may arise that Sensing Nodes that are deployed in hostile environments for military applications are prone to be captured and can become malicious. According to the research being done, there come the three broader Views [5] such as

• Key Management: Key is used for encryption, decryption and authentication

• Authentication and Secure Routing [12]: Making information confidential

• Security Service: This includes the various security programs that are being used to lessen the conflicts that have aroused, not eliminating the consequences. Such services comprise security integration, safety orientation, etc.

Intrusion detection can be defined as a security technology that attempts to identify those who are trying to break into and misuse a system without authorization and those who have legitimate access to the system but are abusing their privileges. An IDS dynamically monitors a system and user's actions in the system to detect intrusions [18]. IDS, by analyzing the system and users' operations, in search of undesirable, mistrustful and suspicious activities, may effectively monitor and protect against threats [6].

2. ARCHITECTURE

2.1 Defining the Architecture for Hierarchical Intrusion Detection System for WSN
For the detection of the various Distributed attacks, It is essential to have a Distributed Architecture which has a well-defined hierarchy, distributed properties, and is very useful in providing the scalability, robustness in different ways [7]. With the use of distributed architecture, the process of intrusion detection can be dispersed to numerous nodes in the network. The major advantage is that if, by chance, the node crashes or is being removed; it can still work and can be termed as fault tolerant [17].

Figure 1 illustrates the Intrusion Detection Hierarchy for the Wireless Sensor Network. And its structure shown above refers to the hardware architecture of the wireless Sensor Network [15]. In the first level, SN is accountable for assembling the data, observing the deeds of a neighbor node, and also collecting the information of the activities of the local response to the invasion that can be by isolating the relevant node [7]. Then comes the Layer 2 i.e. Coordination layer which is mainly responsible for the data integration, monitoring all the activities that are performed in the network such as individual node activity monitored by the neighboring SN. The second major work of the layer 2 is to analyze the aggregated data collected and forwarded by the layer 1 though which it can conclude about activities related to invasion. Now to identify that whether any attack or invasion has occurred, the base layer is used, whose responsibilities are similar to that of coordination layer, to recognize and observe all the engines.

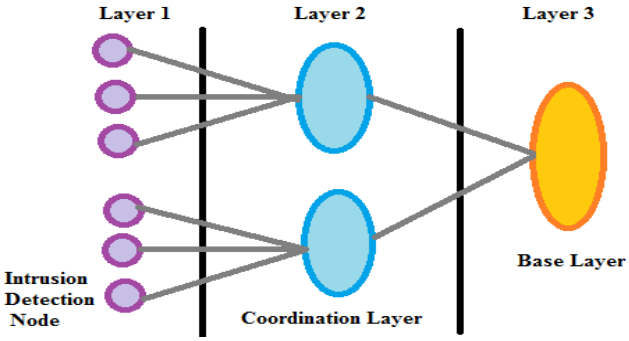

Fig.1 Architecture of Intrusion detection system model for WSN

2.2 Working of IDS Model for WSN

In Fig. 2 an Intrusion Detection System model is shown [8] for WSN. Due to the constraint of the SN i.e. computing power and the storage capacity is limited, therefore a model is designed which works with the joint collaboration of each node and consists of multiple nodes [15]. These nodes achieve Data Collection (DC), Intrusion Detection (ID), Result Response (RR), Track and Node Choose (NC) .DC nodes not only collect information from each node, but also forms a warehouse of information about each node; ID nodes with DC information, detection intrusion information by using anomaly detection [16] algorithm; the RR node is responsible to identify the node in which the invasion has occurred in abnormal conditions by triggering the track node. Due to the reason that DC node has more power consumption, NC is mainly responsible for making large energy node act as DC node. The working of the model further in the form of a flow chart.

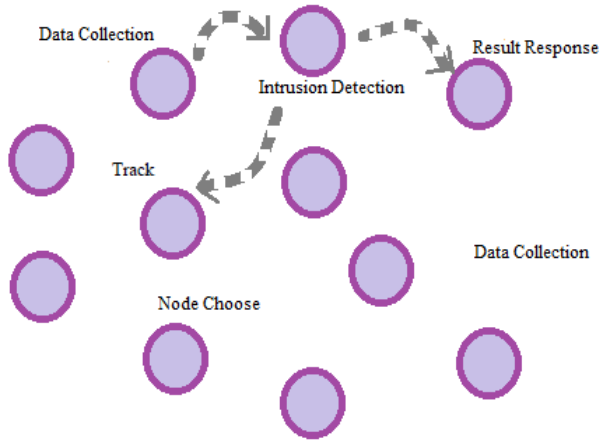

Fig.2 An IDS model for WSN

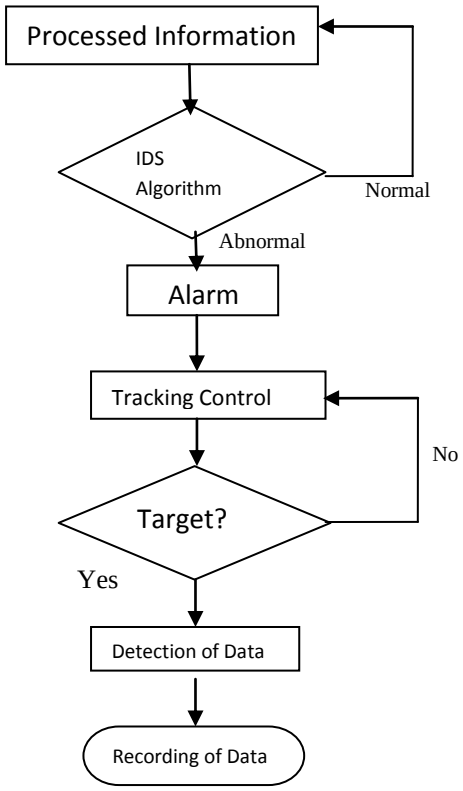

Fig.3 An IDS Flow graph

According to the[15], an experiment was done on NS-2 as a simulation platform in which the area with 10m ×10m, 50 nodes were distributed including DC,ID,RR,NC and Track. It was found that detection rates were consistently 55% to 60% for wandering and each node has a stable initial energy with similar communication range. In the network, packet transport at the speed of 19.5kB per second.

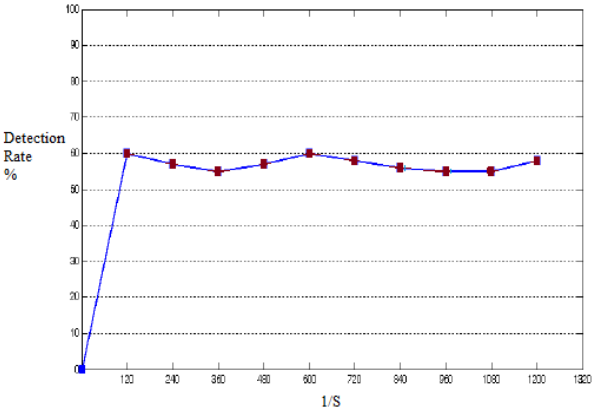

Fig.4 A Graph showing the percentage detection rate

(Source: Intrusion detection model based on hierarchical structure in Wireless sensor networks by Lei Li, Yan-hui Li, Dong-yang Fu, Ming Wan in "2010 International Conference on Electrical and Control Engineering")

3. NUMEROUS IDS SCHEMES FOR WIRELESS SENSOR NETWORK

3.1 Energy Proficient Hybrid Intrusion Detection System

Su et al. proposed eHIP – energy efficient hybrid intrusion prohibition system [9] to improve this crudity of cluster-based sensor networks. The system consists of AIP (Authentication-based Intrusion Prevention) and CID (Collaboration-based Intrusion Detection) which provides heterogeneous mechanisms for securing levels in cluster based wireless sensor networks to improve energy efficiency[19].

In two different detection methods, the scheme for cluster-heads and Ordinary members was used. Cluster-heads are responsible for monitoring member node within the same cluster; and the other members are being used to observe the cluster-heads in their cluster [15]. The Cluster-head's safety is important because, they bear the main communication tasks. The authors emphasize on numerous energy flaws that occur while designing of the package, for an instance, addressing the monitoring of cluster-heads by using the method of ordinary members group-working in turns. However this also brings the group into a more intricate mechanism, increases the system complexity and difficult to implement.

3.2 Markov Model based IDS

Agah et al proposed a new game theory as per the paper referenced as [10]. According to [15], the use of Markov decision process and the issue of offensive and defensive structure works essentially to predict the node, which has the higher probability to get attacked [14].and this works by creating two type of participants, in offensive as well as defensive issues, with other two models i.e. Zero-sum game model as well as the non-cooperative game model, between the intruder and wireless sensor network [7]. In this, the attacker or participants emphasizes to maximize their own gains, but if the strength of participants is increased, it may lead to reduction in other participants proceeds. If Markov decision Policy process is adopted, the prediction of the node which is more vulnerable to attack can be done. This model has proved to be the Nash equilibrium.

In [7][10], Doumit et al. suggested a self-organized criticality and stochastic learning based intrusion detection scheme that uses the advantage of self-organized criticality for a certain location which is dependable on an environment variable along with hidden Markov model to detect future irregularities [13]

3.3 Immune based IDS Algorithm

The mechanism of intrusion detection based on immune algorithm was proposed by Zeng et al in [11], in which the reference to the biological mechanism is given as the author mapped the human immune system to the IDS. The Double layer intrusion prevention measures are provided by the algorithm, which states [15]:

1. Determining whether the network behavior is matching the known invasion pattern to activate specific immune-layer. Each node in the network is composed of the testing knowledge base and its corresponding detector. The major work of the detectors to define thee network intrusion and to take the appropriate response strategies by analyzing the extracted features and query testing knowledge base.

2. For responding the unknown priori invasion, the nonspecific immune layer is responsible. The major work of the Non-specific immune layer is to simulate organism's adaptive immune system with the capacity to study and identify unknown invasive methods which comprises normal set and its corresponding detector. If it is found that there is the chance for the attack due to any abnormal condition in network then the layer is activated, to locate and isolate the abnormal nodes by seeking multi-node collaboration, while including the various features such as intrusion detection into the knowledge base. Also, the multi-detector collaborative with information processing mechanism can also be used jointly to improve the capability of detection of intrusion as well as reducing the rate of false alarm.

4. CONCLUSION

Every Security mechanism has some loop holes which are to be filled to provide the greater security and reliability. The research work on Intrusion Detection System is has been conducted for over 20 years, but need to be further enhanced for using it for Wireless Sensor Network In Present scenario, the focus should be given to lot of research work in improving the IDS Solutions for securing the Wireless Sensor Network which depends upon distribution and collaboration to reduce the ill effects of the invasion. Still, there is the need at present, to study about the new methods for the intrusion detection in wireless sensor networks.

5. ACKNOWLEDGMENTS

Sincere thanks to Mr. Vishal Bharti, for providing his valuable guidance in this field.

6. REFERENCES

[1] X. Chen, K. Makki, K. Yen, and N. Pissinou, "Sensor network security: a survey," IEEE Communication Surveys & Tutorials, vol. 11, no. 2, June 2009, pp. 52-73.

[2] Y. Zhang, W. Liu, W. Lou, Y. Fang, and Y. Kwon, "AC-PKI: anonymous and certificateless public-key infrastructure for mobile adhoc networks," 40th IEEE International Conference on Communications, May 2005, pp. 3515-3519.

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

[4] Jing Deng, Richard Han, Shivakant Mishra, INSENS: Intrusion-tolerant routing for wireless sensor networks, Computer Communications, July 2005,pp.216-217

[5] ZENG Xia-ling,LIANG Yan-zhao,PENG Ya-li,YU Min,Cluster-Based Intrusion Detection System for Wireless Sensor Network,Microelectronics and Computer,June 2008,156-163.

[6] Bo Sun And Lawrence Osborne, Lamar University Yang Xiao, The University Of Alabama Sghaier Guizani, University Of Quebec At Trois-Rivieres "Intrusion Detection Techniques In Mobile Ad Hoc And Wireless Sensor Networks"

[7] Li Gang, Study on intrusion detection for wireless sensor network,China computer&Network,2009,pp.535.

[8] Liu ning,FAN Xin-li,ZHAO Jian-hua, An Intrusion Detection System Model for Wireless Sensor, Journal of SouthwestUniversity of Science

[9] Zhou Xian-wei, Wireless sensor network and security,Bei jing, National Defense Industry Press,2007,pp.178-188

[10] WANG Ying, LI Guorui, A Group-Based Intrusion Detection Scheme in Wireless Sensor Networks, CHINESE JOURNAL OF SENSORS AND ACTUATORS, Jun. 2009,pp.879-881

[11] YANG L i-bin, MU De-jun, CAI Xiao-yan, Study on intrusion detection for wireless sensor network, Nov. 2008,pp.3204-3207.

[12] Chong Eik Loo, Mun Yong Ng, Christopher Leckie, Marimuthu Palaniswami. Intrusion Detection for Routing Attacks in Sensor Networks, International Journal of Distributed Sensor Networks, Volume 2, Issue 4 December 2006 , pages 313 - 332 DOI: 10.1080/15501320600692044

[13] S. Doumit and D.P. Agrawal,"Self-organized criticality & stochastic learning based intrusion detection system for wireless sensor network", MILCOM 2003 - IEEE Military Communications Conference, vol. 22, no. 1, pp. 609-614, 2003

[14] A. Agah, S. Das, K. Basu, and M. Asadi, "Intrusion detection in sensor networks: A noncooperative game approach", in 3rd IEEE International Symposium on Network Computing and Applications, (NCA 2004), Boston, MA, August 2004, pp. 343346.

[15] Lei Li, Yan-hui Li, Dong-yang Fu, Ming Wan,"Intrusion detection model based on hierarchical structure in Wireless sensor networks" 2010 International Conference on Electrical and Control Engineering.

[16] V. Bhuse, A. Gupta, "Anomaly intrusion detection in wireless sensor network" Journal of High Speed Networks, Volume 15, Issue 1, pp 33-51, Jan 2006

[17] FZhang, Y. and Lee W "Intrusion detection in Wireless Ad hoc Networks", The 6th annual international conference on Mobile computing and networking, Boston MA, Aug 2000. PP:275-283

[18] Rodrigo Roman, Jianying Zhou , Javier Lopez, "Applying Intrusion Detection Systems to wireless sensor networks ",Consumer Communications and Networking Conference, 2006. CCNC 2006. 3rd IEEE, 8-10 Jan. 2006 Volume: 1, On page(s): 640- 644 ISBN: 1-4244-0085-6

[19] OTran Hoang Hai, Faraz Khan, and Eui-Nam Huh, "Hybrid Intrusion Detection System for Wireless Sensor Network", ICCSA 2007, LNCS 4706, Part II, pp. 383–396, 2007. Springer-Verlag Berlin Heidelberg 2007