IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 26-28

Analysis of Intrusion Detection Models for Wireless Sensor Networks

Vaidehi.V. Bhatt
(Assistant Professor, K.J Somaiya Institute of Management Studies and Research, India)

Abstract: *With increase in the utility of Wireless Sensor Networks in various mission critical fields like environmental monitoring, traffic control, military, medical and healthcare, inventory tracking and smart spaces; secure and reliable sensor networks are a necessity. Majority of sensor networks are deployed in hostile areas making them difficult to maintain. With limited energy of sensor nodes deploying an efficient Intrusion Detection System which does not consume more resources than the primary function of the network is of paramount importance. The Intrusion Detection System should detect and recover from internal and external attacks. In this paper, analysis of different methodologies is performed to identify their advantages and disadvantages.*

Keywords: *WSN, IDS, TPIDS, HIDS, EPID, Cognitive networks*

I. Introduction

WSNs consist of sensor nodes in a scattered manner. Mostly sensors are deployed in hostile environments. These scattered sensor nodes communicate with central sink node delivering the data collected from the environment. The major challenge of WSNs is limited capabilities of sensor nodes. The lack of infrastructure compels sensor nodes to perform the task of routing which consume a lot of energy of the sensor nodes. Additional challenge is maintaining the security of WSNs in hostile environments. Due to the vulnerable nature of WSNs the security solutions designed for Intrusion Detection should keep in consideration the limited capabilities of sensor nodes. Thus the Intrusion Detection Systems deployed on WSNs should be light weight and flexible. IDS should comprise of monitoring component, analysis component, detection algorithm and alarm component. All the components should be efficient enough to be able to perform their individual tasks keeping the consumption of resources minimal. The IDS should not hinder the primary function of the wireless sensor network. IDS apply different techniques, but there is no clear indication which technique is efficient for growing requirement of sensor networks in various fields. This paper will analyze the existing IDS, evaluate them on various parameters and identify different advantages and disadvantages for each of them.

II. Existing Ids Models

2.1 Intrusion Detection for Wireless Sensor Network Based on Traffic Prediction Model

Han and Wang [1] have proposed a traffic prediction technique for large scale tiled wireless sensor networks. This technique is based on anomaly detection which detects selective forwarding attacks and Denial of Service attacks. Along with known attacks it can detect unknown attacks. Each node builds Markov model of traffic prediction and analyzes characteristics of nodes which have similar network traffic. Being light weight is the advantage of the algorithm. The nodes are not capable of addressing vulnerabilities precisely. Considering the sensor node capabilities the detection algorithm should be improved. Also each mode building the Markov model can be considered as an overhead.

2.2 Advanced Intrusion Detection System

Joseph et al [2] suggests that one Intrusion Detection System is not sufficient, combination of two or more IDS are found to be efficient. It is stated Hybrid intrusion detection is the amalgamation of signature and anomaly based detection identifies only few attacks. Whereas Energy prediction intrusion detection model takes into account the initial energy and then calculates the rate at which energy is consumed for normal functioning. Any abnormal consumption is detected as an attack. The issue with such an approach is that sometimes energy consumption may differ due to other parameters. Cross Layer Intrusion Detection system suggests forming of clusters. The proposed model combines the Hybrid Intrusion Detection, Energy Prediction Based Intrusion Detection and Cross Layer Intrusion Detection system. The model is said to be useful for small, medium and large sensor networks. The results shown convey that Advanced Intrusion Detection system detects intrusions more efficiently than individual Intrusion Detection systems. The issue that can be highlighted here is deploying

this model on small and medium sized networks may consume a lot of energy as the complexity of the Intrusion Detection system increases.

2.3 Abnormal Node Detection in Wireless Sensor Networks by Pair Based Approach using IDS Secure Routing Methodology

Khandakar et al [3] propose a pair-based abnormal node detection combining prevention and detection based techniques. This model requires deploying a centralized knowledgebase. Pairs of sensor nodes are created to keep a check on each other for abnormalities. This method reduces the problem space. Along with centralized knowledgebase for anomaly based detection, each node maintains a local knowledgebase and local detection engine. Local knowledgebase contains information of the adjacent node. Abnormalities in the adjacent node are indicated by the local detection engine utilizing the local knowledgebase. Central knowledgebase is updated with new information from local knowledgebase. Central knowledgebase contains information of each pair in all groups. Central knowledgebase is continuously updated from the local knowledgebase and local detection engines are updated with abnormal behavior of all groups. If any anomaly is detected, local knowledgebase is approached and if the attempt fails then central knowledgebase is approached to detect the anomaly. The issue with this model is high energy consumption as local knowledgebase has to be maintained and the centralized knowledgebase has to be updated. If the centralized knowledgebase is not updated on proper intervals, detection can become difficult. Also if one of the nodes in the pair is compromised the formation of a new pair consumes more energy as the local knowledgebase of both the nodes have to update.

2.4 Cognitive Approach Based User Node Activity Monitoring for Intrusion Detection in Wireless Networks

Sunilkumar et al [4] propose cognitive approach based node activity monitoring. Network statistics and repeating trail of network messages provide input for decision making and the ways to rectify network issues. In this proposed model user node activity is monitored and preventive measures are taken if user node messages are malicious. The monitored behavior section stores the prediction after the peer nodes are observed. This task is accomplished by using self-organizing maps. Zones are formed by grouping nodes, each representing a feature and have a lattice. Each node is assigned zero weight. The lattice of each zone is assigned a vector randomly from the training data. On receiving the input vector, each node weight is compared to the input vector. If both of them match then the node is declared as the winning node and is identified as best matching unit. Mexican hat learning function and Gaussian learning function are used for unsupervised adjacent node learning. The issue to be addressed for this approach is the unsupervised self-organizing maps.

2.5 Decentralized Intrusion Detection

Paula et al [5] propose Decentralized Intrusion Detection which has three phases. In the data acquisition phase data stored in various important message fields are stored in an array. In the rule application phase rules are defined for various types of message types. According to the order of complexity of rules, they are applied to the data stored.If a message of specific type does not satisfy a rule defined for that message type the failure counter is incremented and the message is discarded. This strategy is adopted as WSNs have severe resource restrictions. As the first failure indicates abnormal behavior there is no requirement to further process the rules, which reduces detection latency. Phase three distinguishes between network failures occurring occasionally from actual attack instances. The idea of deviation tolerance is subjected by the following approach. The monitor node detects an attack after considering all network failures. This task is carried out by analyzing the messages which are transmitted to the neighborhood. The IDS is deployed on common nodes. The important issues to be addressed here is the formation and updating of rules, selection of nodes for deploying IDS.

III. Analysis of Intrusion Detection Models

Lot of approaches have been researched for development of Intrusion Detection Systems for WSNs, but none of the approaches mention the applications or type of applications for which the model can be utilized. With the help of important parameters identified one can select a specific model. TABLE 1 displays the comparative study of the above discussed models to make the selection efficient. Looking at different parameters like the power consumption, memory consumption, attacks identified one can take decision as to which model would be most suitable for the chosen application. The parameters which are of at most importance for an application should be identified and matched with the comparative study which will enable the selection of the suitable IDS for the application.

Table 1 Analysis of Intrusion Detection Models

Model Observed [Paper Ref.]	**TPM [1]**	**AIDS [2]**	**ANDWSNPBA [3]**	**CABUNAM [4]**	**DID [5]**
IDS Model	Traffic Prediction Model	Hybrid, Energy and Cross Layer	Pair Based Model	Cognitive Model	Decentralized Model
Processing power utilization	Enormous	Enormous	Enormous	Enormous	Limited
Memory Utilization	Limited	Limited	Extensive(Highest)	Enormous	Enormous
Attacks Identified	Selective Forwarding, Denial of Service and unknown attacks.	Selective Forwarding, Worm Hole, Sybil, Sink Hole, DoS	Malicious Node Identification	Not Specified	Malicious Node Identification
Advantages	Low complexity	Multiple Intrusion Detection Systems combined.	Availability of local knowledgebase makes identification of malicious activities faster.	Intelligent Engine	Less computation
	Less computation and communication cost.	Useful for small, medium and large networks	Centralized knowledgebase helpful in identifying different attacks.	High detection rate	Differentiates between occasional network failures and attack instances.
Drawbacks	Overhead of building Markov model on each node.	High resource consumption.	Local and Centralized knowledgebase have to be maintained.	High resource Requirement	Rules to be formed for various message types.
	Attacks identified and place of deployment of IDS for the model are not specified.	Place of IDS deployment not identified.	Synchronization of local and centralize knowledgebase should be scheduled at proper intervals.	Time taken to calculate best matching unit.	Selection of nodes for deploying the IDS.

IV. Conclusion

Wireless Sensor Networks work on limited constraints. Thus Intrusion Detection System designed for WSNs should utilize constrained resources. The analysis performed helps in choosing which model of Intrusion Detection can be used for the desired application. Some of the models are complex in nature but do not specify the king of attacks addressed. Such models should be avoided in mission critical applications. Processing power consumption and energy consumption are critical requirements for WSNs, the models which consume high processing power and energy should not be considered for applications to be deployed in uncontrolled and hostile environments. Most of the models observed deploy different mechanisms for intrusion detection but fail to address the issue of unknown attacks. Thus the need of the hour is to design Intrusion Detection Models for Wireless Sensor network keeping the above factors in consideration.

References

[1]. Han Zhijie, Wang Ruchuang, Intrusion Detection for Wireless Sensor Network Based on Traffic Prediction Model, *International Conference on Solid State Devices and Materials Science, 2012.*

[2]. Joseph Rish Simenthy CEng , AMIE, K. Vijayan, Advanced Intrusion Detection System for Wireless Sensor Networks, *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, 2014.*

[3]. Khandakar Rashed Ahmed , A.S.M Shihavuddin, Kabir Ahmed, Md. Shirajum Munir and Md Anwar Asad, Abnormal Node Detection in Wireless Sensor Network by Pair Based Approach using IDS Secure Routing Methodology, *IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.12, December 2008.*

[4]. G Sunilkumar , Thriveni J , K R Venugopal , L M Patnaik, Cognitive Approach Based User Node Activity Monitoring for Intrusion Detection in Wireless Networks, *IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 3, March 2012.*

[5]. Ana Paula R. da Silva, Marcelo H.T. Martins, Bruno P.S. Rocha, Antonio A.F. Loureiro, Linnyer B. Ruiz, Hao Chi Wong, Decentralized Intrusion Detection in Wireless Sensor Networks, *Proceedings of the First ACM Workshop on Q2S and Security for Wireless and Mobile Networks, Montreal, Quebec, Canada, October 13, 2005.*