Special Issue of Engineering and Scientific International Journal (ESIJ)
Technical Seminar & Report Writing - Master of Computer Applications - S. A. Engineering College (TSRW-MCA-SAEC) – May 2015

ISSN 2394-187(Online)
ISSN 2394-7179 (Print)

Attack Detection Using Intrusion Detection System in Wireless Sensor Network

U.Revathi

Department of Computer Applications, S.A Engineering College-Chennai
revathiu51@gmail.com

Abstract— Wireless Sensor Networking has its own importance in the area of communication technology because it has low installation cost and simple network operations. Wireless sensor Networks are growing very fast nowadays. Wireless sensor network consists of large number of nodes which will be distributed in nature. The wireless sensor networks applied in the areas include agriculture, healthcare, military, hospitality, etc. Now a day's networks are very important and security of the network is one of the major concerns. In Wireless Sensor Networks the various attacks are jamming attack, collision attack, sinkhole attack, Sybil attack, wormhole attack, etc. Stopping these attacks are detecting the attacks of the Wireless Sensor Networks system various Intrusion Detection policies are developed to detect the nodes that are not working properly and it is also used to detect the malicious or unexpected intruder. In this paper explained various attack of wireless sensor networks. Hybrid Intrusion Detection System(HIDS), Energy Prediction based Intrusion Detection System (EPIDS) and the Cross layer Detection System are implemented to assure the maximum possible security from the Intrusions .For wireless sensor network in secure manner many intrusion detection systems were proposed.

Keywords— *Intrusion detection system, Attacks, PPDM, WSN, Types of IDS, HIDS, Data privacy,*

1. Introduction

An intrusion is a set of actions that can lead to an unauthorized access .The intrusion detection system is used to monitor the computer networks and system; detecting possible intrusion in the network and altering users after intrusion had been detected, reconfiguring the network if this is possible. Intrusion is an illegal action in a system that is either statically or dynamically.

Wireless sensor network is a kind of networks that constitutes a large number of small mobile devices with sensor function . Sensor have responsibility to monitor the physical condition such as sound, pressure, temperature ,etc and provide facility to transfer the data over the network.

A WSN is made by grouping of several numbers of nodes. Each node is connected to one sensor for availing network facilities. Each sensor node of network has a radio transceiver, a microcontroller, a sensor and an energy source.

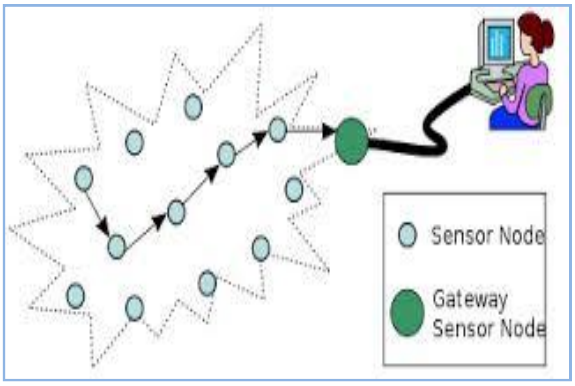

Fig.1: Wireless sensor network

The categorization of WSN in two types they are 1) Monitoring 2) Tracking. Each category can be divided in many sub categories. Many security mechanisms like authentication and key exchange and security routing have been proposed but they cannot deal with providing security towards many attacks.

2. Attacks on WSN

2.1 Jamming (Radio Interference) Attack

In this attack, the attacker transmits the signal to the receiving Antenna at the same frequency as the frequency used by the authorized transmitter, it causes radio Interferences. Jamming attacks involves at disrupting communication services and result in partial or entire degradation of the services.

This attack can be made by continuous radio signal or transmitting only when one channel is active rather than when without a gap between them. This attack can easily be carried out by laptop with high energy.

2.2 Collision Attack

In this attack, when attacker get the legal node is transmitting data, attacker sends its own signal for interferences .Even if one byte have a collision means it creates an error and cripple entire message . But this attack is better than jamming attack in terms of less power consumption and detection ability. This attack can makes degradation of network and exhausting communication channel.

2.3 Sinkhole Attack

In this attack, the attacker node is attractive to its neighbouring node in terms of routing metric like higher power transmission or the appearing of Base station. By using this routing metric more number of neighbouring nodes can be attracted and they choose the attacker or sinkhole node to route their data.

This attack creates a false sink and make non authentication of links and the result is that the data doesn't reach the exact BS. This attack makes the damages to the entire network services.

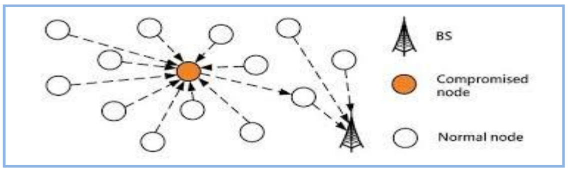

Fig. 2: Sinkhole attack

2.4 Sybil Attack

In this attack, the attacker node assumes multiple identities and try to fill neighbour nodes memory with useless information that come from the nonexistent neighbours and then the attacker nodes fills others memory with redundant Data. If the node has a limit on number of nodes keeps data. If results in removal of actual nodes information. Sybil attack is an identity attack that causes unfairness in the network by forging as multiple nodes and thus creates information redundancy. The aim of the attack is attacking data aggregation, voting, etc.

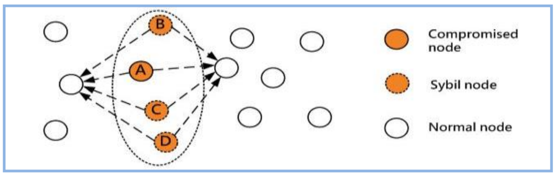

Fig. 3: Sybil attack in WSN

2.5 Wormhole Attack:

In this attack, the low latency or tunnel is created in between two nodes in the network which are then destroyed by the attacker. The aim of the attacker leaves dropping on data being transmitted, creation of false topology.

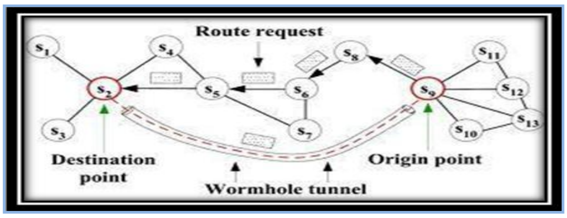

Fig. 4: Wormhole attack

2.6 Hello Flood Attack

In this attack**, t**he attacker node tries to satisfy all other nodes to choose it as parent node by using a powerful radio transmitter by flooding the whole network with hello message by giving false neighbour status. The false status the legal nodes can send the data to the attacking node even though it might be in out of range. It has the same characteristics as Sybil attack but need more powerful.

2.7 Selective Forwarding Attack

In this attack, the attacker may decrease to forward every messages it gets, acting as black hole or it can forward some messages to the illegal receiver and it simply drop other.

2. 8 Sleep Deprivation Attack

In this attack the attacker node forces authorized nodes to waste their energy by resisting the attacker nodes from going into low power sleep node. The aim of this attack is to maximize the energy consumption of the node by this the life of the battery.

3. Intrusion Detection in Wireless Sensor Network

There are two major types of intrusion detection systems (IDS) .There are Host intrusion detection systems (HIDS) and network intrusion detection systems (NIDS). Intrusion detection can be defined as Intrusion detection can be defined as the automatic detection and alarm makes generation to report that an intrusion has occurred in progress. IDS cannot take preventive action, IDS are passive in nature, and they can only detect intrusion and generate an alarm.

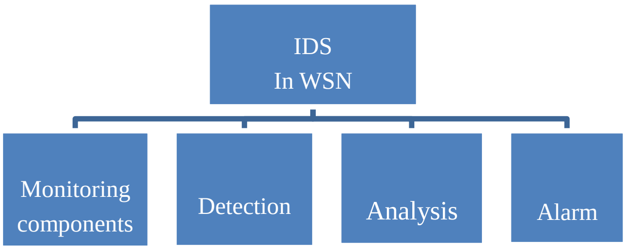

Fig. 5: Components of IDS

There are two distinct technologies of IDS are,

Network Intrusion Detection System (NIDS)

These systems are designed to intercept and analyse packets and analyse packets circulating in the network. All communication in the wireless network are conducted on the air and a node can hear the traffic passing from a neighbouring node.

Host intrusion detection systems (HIDS)

HIDS analyses only data on the node where the IDS is installed. Any decision is based on information collected at this node.

4. Existing Methodology

In the existing methodology they are using signature based IDS, Anomaly based IDS and Hybrid based IDS.

In signature based IDS it has some predefined rules for security attacks. When packets traffic incomes, it is compared with these pre known signatures and if any activity is found to be deviated from these rules, its termed as an attack.

Therefore this IDS are also called rule based IDS. But this IDS is only suitable for known intrusion and cannot detect attacks for which no rule has been defined. This IDS is basically used for detecting routing attacks and sinkhole attacks. Here every node monitors and cooperates with neighbours.

Anomaly based IDS or heuristic approach is used to classify any activity as malicious or normal. Generally some threshold are used in which if any activity is below that threshold, its termed as normal or else as an intrusion. So this IDS uses statistical behaviour modelling where audit data is taken for analysis by firstly transforming the data to format that is statistically comparable to user’s profile.

This user’s is dynamically generated by administrator and updated on based of user’s usage and if on analysis any deviation is found from threshold value, alarm of intrusion is raised. This IDS is capable of detecting new and unknown attacks.

Hybrid IDS is a combination of signature based and anomaly based IDS .This IDS consists of two detection modules, one for detecting well known attacks using rules or signatures and other module detect malicious patterns by detecting behaviour deviation from normal pattern.

This combination of two approaches makes hybrid IDS more accurate in terms of attack detection with less number of false positives. But this hybrid approach is usually not recommended in WSN as this consumes more energy and resources.

5. Proposed Methodology

The combination of Energy prediction based IDS, Hybrid IDs and Cross layer IDs are implemented. First we have to select the cluster head. It is one of the important procedures in IDS. The algorithm for node selection trying to select the high capacity nodes compared to other one. High capacity means large sensing range and transmission range.

Si–Set of type i sensors in the WSN area.

S-Set of all sensors in the network

N(a)-Set of neighbours of node a.

```
Repeat
For i=1 to N
Select node a with min N(a) in Set Si
If N(a)≠ ϕ
Select a
SN={ j/the distance between a and N(a)<(rsi/2) }
If SN>1
S=S-(SN U a)
Else
S=S-a
Until S is null set
```

When compared to the other sensor node, cluster head have the maximum amount of energy.

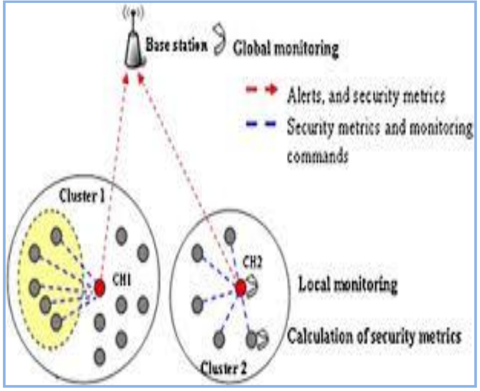
Base station
Global monitoring
Alerts, and security metrics
Security metrics and monitoring commands
Cluster 1
CH1
CH2
Local monitoring
Calculation of security metrics
Cluster 2

Fig.6: Cluster head

After the cluster head has been selected, the sensor node will be communicating with the cluster head. Then it can be communicate with each other node. After the attack as been done in the node the normal working condition is changed.

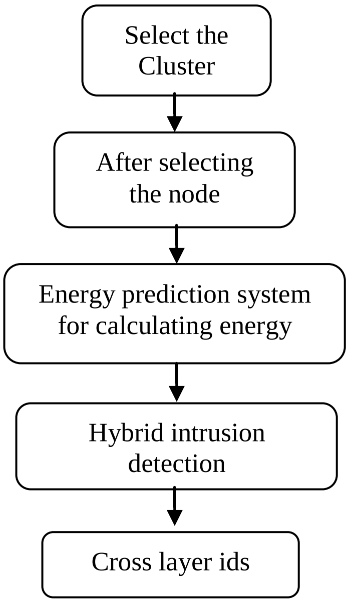
Select the Cluster
After selecting the node
Energy prediction system for calculating energy
Hybrid intrusion detection
Cross layer ids

Fig. 7: Combination of IDS

The attack consumes more energy from the node. So the power of the will be affected. For this we are using the energy prediction system for calculating the normal energy consumption rate will be calculated and compared with the present condition of the affected node. This shows that the node is affected. Then the hybrid IDS will be employed after the energy prediction system. Hybrid is a combination of signature based and anomaly based IDS. Signature based IDS will check the known attacks and Anomaly will check the new attack.

After the Hybrid IDS is Cross Layer IDS. If the node does not contain any fault means it will remove from the black list. It continues its normal working after being corrected. Suppose the node contains the fault it will remove from the node. The combination of three IDS's will detect all the possible intrusion. The cross layer is suitable for large network with large number of sensor node so we are using that IDS.

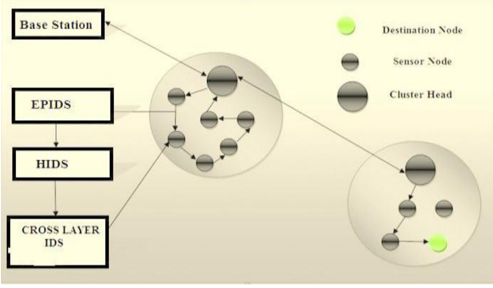

Fig. 8: Combination of three layers

There are two groups of node in bigger circles. Inside the circle there are sensor nodes are located. The bigger circles are called cluster heads.

6. Conclusion

Intrusion detection is used to monitor the networks and detect possible intrusions and alerting the user after the intrusion occurred. We know that security is the main criteria while designing a Wireless Sensor Network. Due to the Broadcast nature of the medium, they are more prone to security attacks. The attacker attacks the node so the energy consumption is reduced in the WSN. So, that the three combination of IDS (Hybrid Intrusion Detection System (HIDS), Energy Prediction based Intrusion Detection System (EPIDS) and the Cross layer Detection System) is used for energy efficiency and detection speed.

It gives a wide range of flexibility in detection of Intrusions compared to the other existing systems. Also the energy efficiency and the system life time is greatly improved.

References

[1] Rodrigo Roman, Jiang zhou and Javier Lopey Applying intrusion detection to wireless sensor network".

[2] Chandra Prakash ,Kunal Jain and PriyankaTripathi "A Comparative Study of Intrusion Detection System for Wireless Sensor Network" Volume 1, Issue 5.

[3] KeshavGoyal, NidhiGuptaandKeshawanand Singh "A Survey on Intrusion Detection in Wireless Sensor Networks" Volume 2 Issue2 pp 113-126 May 2013.

[4] Joseph RishSimenthyCEng , AMIE, K. Vijayan "Advanced Intrusion Detection System for Wireless Sensor Networks" Vol. 3, Special Issue 3, April 2014.

[5] Yassine MALEH and Abdellah Ezzati "A Review of Security and Attacks Intrusion Detection Schemes InWireless Sensor Network" Vol. 5, No. 6.

6] Ismail Butun, Salvatore D. Morgera, and Ravi Sankar" A Survey of Intrusion Detection Systems in Wireless Sensor Networks

[7] Manalisingh, Kushbhubabbar and KushumLata Jain "A survey on intrusion detection in wireless sensor network" vol3,no.3.

[8] Patel nakul" A survey on malicious node detection wireless Sensor networks".

[9] K.Venkatraman,J.VijayDaniel,G.Murugaboopathi "Various Attacks inWireless Sensor Network: Survey"Volume-3, Issue-1.

[10] K. Shanmugavalli, K.Fathima "Wireless Sensor Net Based Surveillance System to TrackEnemyIntrusion at Borders"Volume3, Issue1.

U.Revathi is holding a Under Graduation Degree in BCA from Soka Ikeda college of arts and science for women and pursuing Post-Graduation in master of computer applications from S.A Engineering College. This paper is a part of curriculum covered under in (MC7413) Technical Seminar and Report Writing.