RESEARCH ARTICLE OPEN ACCESS

Various Approaches of Intrusion Detection in Heterogeneous WSN

Ms. Smita H.Karande[1], Mr. S.P.Kosbatwar[2]
Department of Computer Science and Engineering
SKNCOE
Savitribai Phule Pune University,
Pune - India

ABSTRACT

Wireless Sensor Networks (WSNs) are composed of sensor nodes and sinks. The intrusion detection is a mechanism for a Wireless Sensor Network to detect incorrect, improper moving attackers. WSN consumes lots of energy to identify an intruder. The main objective of this approach is to find the intrusion in WSN. Wireless sensor networks (WSNs) consist of small, little devices which having limited energy, limited power, transmission range, and memory. There are two sensing detection models: single-sensing detection and multiple-sensing detection.

Keywords:- Intrusion detection, sensor nodes, Wireless Sensor Network (WSN), Heterogeneous WSN.

I. INTRODUCTION

An Intrusion detection system (IDS) is basically aimed to detect unwanted attacks which attempts at accessing, deactivating of computer mainly through a network. Intrusion detection is very vital in WSN. Intrusion detection plays an very important role in the region of network security, so in an attempt to apply the same idea in WSNs it will makes a lot of sense. There are basically two approaches: misuse detection and anomaly detection. Misuse detection identifies an illegal use by signatures. Anomaly detection identifies from analysis of an event. There are two sensing approaches: Single sensing and multisensing. In single sensing detection approach, the intruder is detected by using one sensor only. Whereas in multisensing detection approach, multiple sensors are used to detect the intrusion

A wireless sensor network (WSN) is a type of wireless network consists of small nodes with capabilities of sensing physical or environmental situations, handling related data and send information wirelessly. WSN is a wireless network consisting of spatially distributed independent devices using sensors to monitor physical or environmental conditions, such as temperature, sound, trembling and force etc.

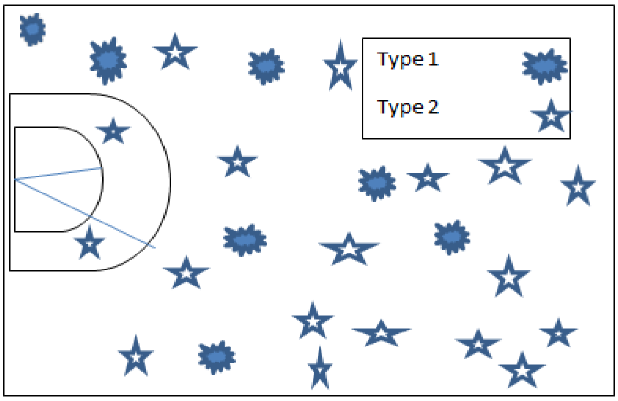

Fig 1 Single sensing detection

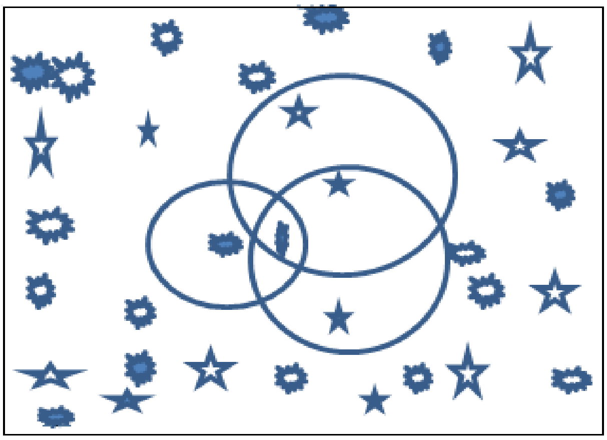

Fig.2 Multisensing Detection

There are number of security protocols used for sensor networks. For example
SPINS (Sensor protocol for information).
LEAP (Localized encryption and authentication protocol).

II. VARIOUS ATTACKS ON WSN

Wireless sensor network is susceptible to several security threats. There are many papers [2] that provide the security threats in details.

Following are network layer attacks:

*A.*Misdirection

Altering or repeating the routing data can cause the misdirection attack. Forwarding the message along with the incorrect path can cause this kind of attack. Misdirection attack is also calculated as routing layer attack.

*B.*Selective Forwarding

In this type of attack, attacker rejects to forward packets or fall them and act as a black hole.

*C.*Sinkhole Attack

In Sinkhole attack, attackers appeal all the traffic from a specific area to a compromise node. This kind of attack can also cause selective forwarding attack.

*D.*Sybil Attack

In Sybil attack, a malicious node can represent multiple identities to the network.

*E.*Wormhole Attack

The simplest form of this attack is an attacker be seated in between the two nodes and forward among them.

*F.*Hello Flood Attack

In Hello Flood Attack, Attacker sends hello packets to the networks to add himself as the neighbor to the other node.

Different DoS attacks and Defense Mechanisms in WSN are:

a. Physical Layer - In physical layer attack caused are jamming and tempering.
Defense mechanisms for this kind of attacks are spread spectrum, priority messages, Lower duty mapping and region mapping.

b. Link Layer- In physical layer attack caused is collision, exhaustion and unfairness.
Defense mechanisms for this kind of attacks are error correcting code, rate limitations and small frames.

c. Network and routing - In physical layer attack caused
are Neglect and Greed , Homing, Misdirection, Black holes. Defense mechanisms for this kind of attacks are Redundancy, probing, Encryption, Egress filtering, Authorization, Monitoring and Redundancy.

d. Transport Layer- In physical layer attack caused are
Flooding, D-Synchronization. Defense mechanisms for this kind of attacks are Client Puzzle, Authentication.

In a WSN, there are two ways for the detection of an intruder: single-sensing detection and multiple-sensing detection. The intruder can be successfully detected by only a single sensor, in the Single-sensing detection approach. On the other hand, in the multiple-sensing detection the intruder can only be detected by using multiple sensors. In some applications; the sensed information delivered by a single sensor is not be suitable for knowing the intruder, because Single sensor can only sense a portion of the intruder.
The intrusion detection can be studied according to the ability of sensors in terms of the broadcast range and sensing range. In a heterogeneous WSN some sensors have a large power to achieve a longer transmission range and large sensing range.

III. COMPARATIVE STUDY of HETEROGENEOUS WSN AND HOMOGENEOUS WSN

In homogeneous networks, all the sensor nodes are identical with respect to battery energy, power and hardware complication.. In homogeneous network, single platform is used by group and all nodes in the network that share the same functionality .In heterogeneous network all the nodes are treated as differently. In the real world, homogeneous network is not practically possible. Heterogeneous WSN consist of dissimilar types of sensor nodes which having different sensing and transmission range. So, when we have to select the sensor node for intrusion detection. We need to consider the difference of sensing and transmission range.

In order to enhance network reliability and extend network lifetime heterogeneous WSN is better. Also, if the sensors are prepared with same hardware, energy, power, they may not always have the same communication and sensing models. There is no guarantee that two sensors using the same platform have exactly the same physical properties. This categorization focuses on heterogeneity at the designing stage. In the heterogeneous wireless sensor network, the average energy consumption for sending a packet from the normal nodes to the sink in heterogeneous sensor networks will be much less than the energy spent in homogeneous sensor network.

IV. LITERATURE SURVEY

There exist several tools for security in wireless sensor networks. There are many solutions used in traditional network but they cannot be applied directly to WSN because the properties of sensor nodes have some restrictions. Ad-hoc and WSNs security has been studied in a number of proposals.

Zhang and Lee [5] are among the first to study the problem of intrusion detection in wireless Ad-hoc networks. They proposed design for a distributed and cooperative intrusion detection system for Ad-hoc networks; their scheme was based on numerical variance detection techniques. This scheme requires much more time, data and traffic for intrusion detection.

Detecting a moving intruder is very critical application in wireless sensor networks .Intrusion detection is defined as, first interaction time when the intruder knockouts the sensing range of a sensor belonging to the large sensor cluster. Up till now most of the present work highlighting on the problem of network configuration for strongly detecting the intruder within a pre-specified time, under the restrictions of less power and/or cost effectiveness.

Liu et al. [6] have discovered the effects of sensor mobility on sensing exposure and detection skill in a mobile WSN. It is proved that sensor mobility can improve the sensing coverage of the network, and provide fast detection of directed actions.

Wang et al. [7] have provided a joining approach in relating the intrusion detection probability with respect to the intrusion distance and the network factors (i.e., node density, sensing range and transmission range).

Byunggil Lee et al., [4] have developed management policy and security structure for WSN. The proposed structure has benefits as respect to secure link and intrusion detection.

Qi Wang et al., [8] have developed an intruder detection algorithm of low complexity for static wireless sensor network. The intrusion detection model includes features that determine the normal frequency of performance of order. A dispersed algorithm in which the sensor collects the information from the adjacent nodes to examines the irregularities if any from the neighbor's.

V. OUTCOME

In our survey we have studied about the intrusion detection, wireless sensor network and about the heterogeneous wireless sensor network as well as the homogeneous wireless sensor network.

We have studied about the WSN, Wireless sensor networks (WSN) consist of small or little devices. These small devices have limited power, limited energy, and memory. Networks are positioned mostly in open and unguarded environment. There are two types of WSN first, homogeneous WSN and second, heterogeneous WSN. We have selected heterogeneous WSN for our survey.

VI. CONCLUSIONS

This paper presents various approaches of intrusion detection mechanism that increases life of WSN.

Various attacks of WSN and protocols for WSN. Wireless sensor networks are helpless to some attacks because of their deployment in an open and unprotected environment. This paper describes the major security threats in heterogeneous WSN and also describes different intrusion detection techniques. The paper also describes several existing approaches to detect the intrusion in WSN.

REFERENCES

[1] Mohamed Mubarak T, Syed Abdul Sattar, G.Appa Rao, Sajitha M" Intrusion detection:

An Energy efficient approach in Heterogeneous WSN”.

[2] Anomaly Intrusion Detection System in Wireless Sensor Networks: Security Threats and Existing Approaches International Journal of Advanced Science and Technology Vol. 36, November, 2011

[3] Xi Peng, Wuhan Zheng Wu, Debao Xiao, Yang Yu," Study on Security Management Architecture for Sensor Network Based on Intrusion Detection "' IEEE, Volume: 2,25-26 April 2009.

[4] Byunggil Lee, Seungjo Bae and Dong Won Han, “Design of network management platform and security frame work for WSN”, IEEE International conference on signal image technology and internet based system, 2008.

[5] Y. Zhang and W. Lee. Intrusion Detection in Wireless Ad-Hoc Networks. In Proc. ACM MobiCom, pages 275-283, 2000.

[6] B. Liu, P. Brass, O. Dousse, P. Nain, and D. Towsley, “Mobility improves coverage of sensor networks,” in Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), 2005.

[7] Y. Wang, X. Wang, B. Xie, D. Wang, and D. P. Agrawal ,“Intrusion detection in homogeneous and heterogeneous wireless sensor networks,”IEEE Transactions on Mobile Computing, vol. 7, no. 6, pp. 698–711, 2008.

[8] Qi Wang, Shu Wang, “Applying an Intrusion detection algorithm to wireless sensor networks”, Second international workshop on Knowledge Discovery and Data Mining, 2009.

[9] A. Perrig, et al., “SPINS: Security Protocols for Sensor Networks”, Wireless Networks, 8(5):521- 534, Sep. 2002.

[10] S. Zhu, S. Setia, and S. Jajodia, “LEAP: Efficient Security Mechanisms for Large-scale Distributed Sensor Networks”, Proc. of the 10th ACM Conference on Computer and Communications Security (CCS '03), Oct. 2003.