IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 3 Issue 7, July 2016
ISSN (Online) 2348 – 7968 | Impact Factor (2015) - 4.332
www.ijiset.com

Intrusion Detection in Heterogeneous Wireless Sensor Networks

Salman Siddiq, Mr.Srinivasulu M

M.Tech, Dept. of CSE Visvesvaraya Institute of Advance Technology,, Bengaluru, India.
Asst. Professor M.Tech, Dept. of MCA, Visvesvaraya Institute of Advanced Technology, Bengaluru, India.

***Abstract*---Intrusions in heterogeneous WSNs can be detected by using multi-sensors in between sender hosts and receiver hosts. These multi-sensors can operate at same time and monitor the activity of data packets transformation between the two hosts the sender and receiver hosts are registered with sensor if any anomalous sender try to send modified date packet then the sensor detects the anomalous sender with their port numbers and block the data packet which is sent by anomalous sender. The main objective the paper. Transfer information in a secured manner and provide security by using multiple sensors that detects the intrusion during data transformation in connectionless sensor networks.**

Keywords—Intrusion detection, anomalous sender, heterogeneous system.

1. INTRODUCTION

The intrusion also called as encroachment it is consider as the technique for connectionless sensor networks to identify the presence of in-appropriate, false, or inconsistent attackers those are in moving stage. in this paper, intrusions in heterogeneous WSNs can be identified by using multi-sensors in between one host(sender) and another host(receiver) in WSN. These multi-sensors can operate at same time and monitor the activity of data packets transformation between the two hosts the sender and receiver hosts are registered with sensor if any anomalous sender try to send modified date packet then the sensor detects the anomalous sender with their port numbers and block the data packet which is sent by anomalous sender.

Intrusions in heterogeneous WSNs can be detected by using multi-sensors in between sender hosts and receiver hosts. These multi-sensors can operate at same time and monitor the activity of data packets transformation between the two hosts the sender and receiver hosts are registered with sensor if any anomalous sender try to send modified date packet then the sensor detects the anomalous sender with their port numbers and block the data packet which is sent by anomalous sender.

A. Statement of problem

The system needs to utilize all the network resources efficiently and provide most effective technique to identify intrusion even if the detector host fails to detect further the system has to consider all network parameters.

B. Objective

The main objective is to utilize all the network resources effectively and to get maximum utilization of network resource and to provide multiple sensors which are active at same time. During data transmission all detector hosts try to identify intruder node and block that host system.

The multiple sensor technique helps to track the intruder with registered port numbers then block the malicious host in the network which tries to send data.

II. BACKGROUND

The detector system works with single sensor at a time if one sensor fails then another sensor activate and start sensing

for the intrusions, this leads to poor utilization of network resources and performance degradation,

IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 3 Issue 7, July 2016
ISSN (Online) 2348 – 7968 | Impact Factor (2015) - 4.332
www.ijiset.com

III. LITERATURE SURVEY

D.P. Agrawal and Q.-A. Zeng, et all [1] Provides security to data packets while transmitting in ad-hoc network by using CRC algorithms. it provides security to only the data present in a data packet and not during data transmission, many algorithms have been proposed to provide security in connectionless sensor networks and in Ad-Hoc systems during this security techniques the performance can be decreased and network utilize maximum number of network resources this results in more cost and implementation will be difficult because of the more network resources that has to be manage.

Seyedeh yasaman rashida [2] By using homogeneous system better security can be provided and in heterogeneous system security to data packet can be provided with the help of sensors, this paper provides an effective way of defiance against attackers in computer networks and this paper also proposes the attacks are most common in data transmissions it tries to overcome bottom level element for the information aggregation and analysis this allow to results in better scalability.

This paper mainly depends upon following parameters in intrusion detection system,

- Tracker
- Monitor
- Misuse detector
- Anomaly detectors

X. Chen, and X. Zhang et All [3] The security can be achieved in both homogeneous and heterogeneous system with the help of sensors which detects the intrusions, this paper focus on accurate traffic monitoring to avoiding the intrusion detection, it classifies the intrusion detection based on network systems and network based monitoring system. In these host based monitoring system the host or the hosts which are connected in a network for communication individually monitor the unauthorized senders based on port numbers and in network based system the network contains some of the hostss or host systems which verify the number of system present in network and the sender address and receiver address by using IP address.

IV. PROPOSED SOLUTION

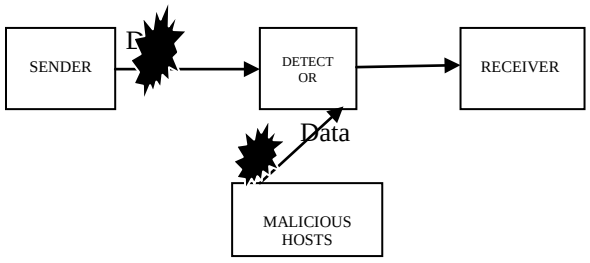

Fig 3.1.1: working of IDS

The figure 3.1.1 shows the architectural representation of for intrusion detection system the sender node tries to send data with registered port number with the detector node, detector node identifies the valid and invalid port numbers through which the sender send the data. if the data packet is from valid sender then data packet is forwarded to receiver otherwise the data packet is discarded at detector node

The method proposes that all the sensors present in the network tries to identify the intrusion that will occur due to unauthorized access in heterogeneous connectionless sensor networks,

Further all the detector hosts verify all the sender's port numbers to identify whether the sender is authorized, if the send is unauthorized then the data packet is discarded detector hosts allows only authorized sender can send data packets to the receiver hosts.

For the implementation it contains the following modules which provides better performance and reliable intrusion detection system.

- Designing (Detector) Sensor Network
- Data packet selection
- Find valid and invalid ports
- Transfer of data packets
- Receiving valid packets and discarding invalid packets

A. Designing (detector) sensor network:

In this Designing sensor network can be constructed by interconnecting all the host systems to its neighbor host system to form the network.

B .Data Packet Selection

In this the browse button is used to select the data packets and if the packet size larger then it is breakdown into small sized packets with packet numbers mention for those packets

C. Find Valid And Invalid Ports

By this the detector node finds the valid and invalid host system in a network, to perform this activity the detectors get the information about valid and invalid port numbers registered previously with that detector for communication starts.

D. Transfer of Data Packets

During this stage when sender clicks on send button by selecting and registered port number the data packet which is already selected in previous operation is transferred on a network to receiver host during this transformation the detectors at intermediate checks for valid and invalid port numbers.

E. Receiving Valid Packets And Discarding Invalid Packets

During this the detector nodes transmit only the valid packets to receiver host and discard the data packets which send by unauthorized port number. These modules designed in such a way that every user can easily understand the functionality of end product.

VI. RELATED WORKS

This technique can be extended in web services with their application and also in parallel computing concepts in interconnection network; by considering all the network parameters the more efficient and high performance oriented intrusion detection technique can be implemented.

Further, Multiple sensors uses more network resources at same time the performance of network reduces, performance can be increased by considering all the network parameters like hosts density, sensing range, and transmission range. this paper can also be extended for Ad-Hoc networks.

The method proposes that all the sensors present in the network tries to identify the intrusion that will occur due to unauthorized access in heterogeneous connectionless sensor networks,

Further all the detector hosts verify all the sender's port numbers to identify whether the sender is authorized, if the send is unauthorized then the data packet is discarded detector hosts allows only authorized sender can send data packets to the receiver hosts.

VI. CONCLUSION

This system provides the solution to intrusion detection problem in heterogeneous WSN related to the distance parameter "D" from sender to detector host with following set of parameters like hosts density, sensing range, and transmission range.This multi-sensor technique allows us to effectively monitor the detector system by providing multiple detectors to detect intrusion at same time.

Further by this technique provide better security mechanism can be achieved for intruders and make use of available resources effectively, since multiple sensors can actively participate to detect intrusion, then there is no chance of entering an intruder during communication between sender hosts and receiver hosts.

This paper provides an efficient use of network resources hence multi-sensor networks can be implemented in least cost security mechanism than compared to other WSN security mechanism.

Finally this paper work helps to develop a secure communication mechanism in WSN networks in less cost, effective utilization of network resources.

Acknowledgment

I sincerely thanks to my guide Mr. Srinivasulu M, Assistant Professor, Dept. of MCA, VTU-CPGS, Bengaluru Region, VIAT, Muddenahalli, for his valuable guidance throughout this research work.

REFERENCES

[1] D.PAgrawaland Q.-A.Zeng, Introduction to connectionless MobileSystems.Brooks/Cole Publishing,

[2] Seyedeh yasaman rashida," Proc.IEEE Int'l Conf. Network Security and its applications (IJNSA),vol.5,no.3, May. 2013.

[

[3] S. Ren, Q. Li, H. Wang, X. Chen, and X. Zhang, " IEEE Trans. Parallel and Distributed Systems, vol. 18, no. 3, pp. 334-350, Mar. 2013.

[4] S.Banerjee, C. Grosan, A. Abraham, and P. Mahanti," Int'l J. Applied Science and Computations,vol. 12, no. 3, pp. 152-173, 2005.

[5] R. Hemenway, R. Grzybowski, C. Minkenberg, and R.Luijten, "Optical-packet-switched interconnect for supercomputer applications,"*OSA J.Opt. Netw.*, vol. 3, no. 12, pp. 900–913, Dec. 2014.

[6] MohammadSaifulIslam amun,hierarchical design based intrusion detection system for connectionless ad hoc sensor network,International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.3, July 2012.

[7] IEEE paper on "The Role of Intrusion Detection System" by John McHugh, Alan Christie, and Julia Allen.

[8] H. Jadidoleslamy A Hierarchical Intrusion Detection Architecture for Wireless Sensor International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.5, Sep 2011.

[9] Ani Taggu, Amar Taggu, (2011) "TraceGray: An Application layer scheme for intrusion detection in MANET using Mobile agents" in Third International Conference on Communication Systems and Networks, pp.1-4.

[10] Yinan Li, Zhihong Qian, (2010) "Mobile agents based intrusion detection system for mobile Ad-hoc network" in International Conference on Innovative Computing and Communication,pp.145-148
.
[11] O. Oriola, (2012). Distributed Intrusion Detection System Using P2P Agent Mining Scheme",African Journal of Computing & ICT, Vol 5. No. 2, pp. 3-10.

[12] Kotagiri Ramamohanarao, Kapil Kumar Gupta, Tao Peng, and Christopher Leckie. The Curse of Ease of Access to the Internet. In Proceedings of the 3 rd International Conference on Information Systems Security (ICISS), pages 234–249. Lecture Notes.in Computer Science, Springer Verlag, Vol (4812), 2008.

[13] Overview of Attack Trends, 2002. Last accessed: November30,2008.http://www.cert.org/archive/pdf/attack_trends.pdf.

[14]KapilKumarGupta, Baikunth Nath, Kotagiri Ramamohanarao, and Ashraf Kazi. Attacking Confidentiality: An Agent Based Approach. In Proceedings of IEEE International Conference on Intelligence and Security Informatics, pages 285–296.Lecture Notes in Computer Science, Springer Verlag, Vol (3975), 2006.

[15] The ISC Domain Survey. Last accessed: Novmeber 30, 2008. https://www.isc.org/solutions/survey/.
[16] Peter Lyman, Hal R. Varian, Peter Charles, Nathan Good, Laheem Lamar Jordan,Joyojeet Pal, and Kirsten Swearingen. How much Information. Last accessed:Novmeber 30, 2008. http://www2.sims.berkeley.edu/research/papers/how-much-info-2003.

[17] Animesh Patcha and Jung-Min Park. An Overview of Anomaly Detection Techniques:Existing Solutions and Latest Technological Trends. Computer Networks, 51(12):3448–3470, 2007.

[18] CERT/CC Statistics. Last accessed: Novmeber 30, 2008. http://www.cert.org/stats/.