IPASJ International Journal of Electronics & Communication (IIJEC)
Web Site: http://www.ipasj.org/IIJEC/IIJEC.htm
A Publisher for Research Motivation ..... Email:editoriijec@ipasj.org
Volume 5, Issue 8, August 2017 ISSN 2321-5984

Deployment and Intrusion Detection Approach in Heterogeneous WSN

Mr. Sumedha Parihar

SP Jain Institute of Management and Research, Mumbai

ABSTRACT

Intrusion detection could be a method of distinguishing and responding malicious activity. Wireless detector networks consisting of an oversized range of sensors square measure effective for gathering knowledge in form of setting. the fundamental sensors square measure straightforward and have restricted power provides. Heterogeneous wireless detector networks square measure higher ascendable and lower overall price than same detector networks. during this paper, we have a tendency to square measure rising the life of wireless network and that we gift a survey of assorted energy economical techniques in a very heterogeneous wireless detector network. it's necessary to rising wireless network as a result of detector nodes in wireless networks square measure forced by restricted energy.

1. INTRODUCTION

Wireless detector network (WSN) refers to a system that consists of range of low-priced, resource restricted detector nodes to sense necessary knowledge associated with setting and to transmit it to sink node that has entranceway practicality to a different network, or Associate in Nursing access purpose for human interface. WSN could be a apace growing space as new technologies square measure rising, new applications square measure being developed, like traffic, setting observance, healthcare, military applications, home automation. WSN is liable to varied attacks like ECM, battery evacuation, routing cycle, cloning. because of limitation of computation, memory and power resource of detector nodes, complicated security mechanism can't be enforced in WSN. thus energy-efficient security implementation is a vital demand for WSN.

On the opposite hand, in a very heterogeneous detector network, 2 or a lot of differing types of nodes with completely different battery energy and practicality square measure used. The motivation being that the a lot of complicated hardware and therefore the additional battery energy will be embedded in few cluster head nodes, thereby reducing the hardware price of the remainder of the network. therefore there square measure 2 fascinating characteristics of a detector network, viz. lower hardware price, and uniform energy evacuation. whereas heterogeneous networks reach the previous, the same networks reach the latter. but each options can't be incorporated within the same network. Associate in Nursing Intrusion Detection System (IDS) detects a security violation on a system by observance and analyzing network activity. There square measure 2 approaches: misuse detection and anomaly detection. Misuse detection identifies Associate in Nursing unauthorized use from signatures whereas anomaly detection identifies from analysis of an occasion. once each techniques sight violation; they raise Associate in Nursing alarm signal to warn the system. Intrusion detection is analyzed in 2 scenarios: single sensing detection and multiple sensing detection .In single sensing detection the trespasser is detected by one detector.

Therefore we've analyzed the multiple sensing detection too. we have a tendency to derive the expected intrusion distance and measure the detection likelihood in numerous application situations. we have a tendency to on paper capture the impact on the detection likelihood in terms of various network parameters, together with node density, sensing vary, and transmission vary.

2. HETROGENEOUS WSN

A typical heterogeneous wireless detector networks consists of an oversized range of traditional nodes and many heterogeneous nodes. the traditional node, whose main tasks square measure to sense and issue knowledge report, is cheap and source-constrained. The heterogeneous node, that provides knowledge filtering, fusion and transport, is costlier and a lot of capable. it should possess one or a lot of variety of heterogeneous resource, like for e.g. increased energy capability or communication capability. Their batteries is also replaced simply. Compared with the traditional

nodes, they will be designed with a lot of powerful microchip and a lot of memory. They conjointly could communicate with the sink node via high-bandwidth, long-distance network, like LAN. If heterogeneous node is gift in WSN then it will increase network dependableness and lifelong.

A. Deployment

In heterogeneous detector networks, the fundamental detectors will be deployed indiscriminately as in same sensor networks. The cluster heads, on the opposite hand, ought to be a lot of fastidiously deployed to create positive all basic sensors square measure lined, that is, every detector will hear from a minimum of one cluster head. However, since the quantity of cluster heads is tiny, their best locations will be found inside an affordable quantity of your time and that they will even increase their transmission.

The problem of causation packets from sensors to one sink node with energy constraints has been studied. However, the distinction between our work and people is profound. First, assume that knowledge ought to be gathered by a data-forwarding tree, that a tree isn't the simplest structure for knowledge gathering applications. the simplest structure will be found by running a network flow formula, that is what we'll adopt in our work. Second, in essence, specialize in traffic routing, whereas we have a tendency to take into account each traffic routing and media access management. during this paper, Associate in Nursing trespasser is outlined as any moving object that enters into the WSN space .It may enter from a random purpose, or through boundary of the preparation space. If born from the air then the entry purpose will be thought of as a random purpose. we have a tendency to gift the analysis of intrusion detection in a very heterogeneous WSN.

B. Styles Of Resource Heterogeneousness

1) procedure heterogeneity- A heterogeneous node has a lot of complicated processor and memory in order that they will perform refined tasks compared to a traditional node.
2) Link heterogeneity- A heterogeneous node possesses high information measure and long distant transceiver than a traditional node proving reliable transmission.
3) Energy heterogeneity- A heterogeneous node is line hopped-up (its battery is replaceable).Out of the higher than the energy heterogeneousness is that the most significant, since computation and link heterogeneousness consumes a lot of energy.

C. Impact of heterogeneousness on WSN inserting heterogeneous nodes within the detector network, decreases time interval and improve battery life time. As mentioned higher than, Computation and link heterogeneousness decreases the waiting time thereby, decreasing the time interval. the typical energy consumption are going to be less in heterogeneous detector networks for forwarding a packet from the traditional nodes to sink, therefore life time is inflated.

3. INTRUSION DETECTION SYSTEM

Event knowledge is that the network activities (for example range of success and failure of authentication). This set of knowledge is ready for additional analysis. Misuse Detection analyses event knowledge from signature record. just in case of event knowledge is matched with any rules, alert signal are going to be raised. Otherwise, event knowledge is forwarded to anomaly detection for additional analysis.

4. CONNECTED WORK

The analysis of heterogeneous wireless detector network isn't new. In Associate in Nursing application for home ground observance, Estrin et al. [1] planned a system design within which knowledge filtered by native process on means through larger, a lot of capable and costlier nodes. References [2] [3] offer different 2 samples of real detector networks with heterogeneous nodes for process and transport tasks. In higher than works, the requirement of heterogeneousness and therefore the mechanisms of packet forwarding and process square measure incontestable and represented. Sensing models square measure of 2 varieties. they're single sensing model and multi sensing model. Intrusion detection method in these 2 models is explored by Wang et al. [4]. In his work, the mix of detection likelihood and network parameters like transmission vary, sensing vary, and node density square measure thought of for experiments underneath single sensing models. Lee et al. [5] analyzed WSN in heterogeneous network setting underneath varied types of deployments for increasing life of network. Their studies discovered that life time of WSN will be maximized by exploitation sure mechanisms and particularly by adding small servers that have an effect on life time of network completely. Xi Peng et al [6] planned a security management model for self organizing wireless detector networks supported intrusion detection. It will stop most of attacks. Then Associate in Nursing analysis of every layer of networks in security model is mentioned and therefore the security management measures within the circuit layer and network layer square measure represented intimately particularly. Such a structure is constructed supported the prevailing coding and authentication protocols.

5. PURPOSED MODEL

Our objective is to sight all intrusions in heterogeneous WSN.In this section, we have a tendency to purposed single sensing model and multiple sensing sightion model in heterogeneous WSN to detect trespasser .The purposed system aims to manage on the market energy in economical manner to boost the network quantifiability, flexibility and lifelong. we have a tendency to divide detector network into clusters that square measure once more partitioned off into sectors. it'll minimize the energy consumption by avoiding all the nodes wanting to send knowledge to an overseas sink node. It uses anomaly detection technique in such the simplest way in order that phantom intrusion detection will be avoided logically.

REFERENCES

[1] A. Cerpa, J. Elson, D. Estrin, L. Girod, M. Hamilton, and J. Zhao,"Habitat monitoring: application driver for wireless communications technology," in Proc. ACM SIGCOMM Workshop on Data Communications in Latin America and the Caribbean, Costa Rica, April 2001

[2] A. Mainwaring, J. Polastre, R. Szewczyk, D. Culler, and J. Anderson, "Wireless Sensor Networks for Habitat Monitoring," Intl. Workshop on Wireless Sensor Networks and Applications (WSNA '02), Atlanta, GA, Sept. 2002.

[3] H. Wang, D. Estrin, and L. Girod, "Preprocessing in a Tiered Sensor network for Habitat Monitoring," in Proc. of the IEEE Conf. on Acoustics, Speech, and Signal Processing, Hong Kong, China, April 2003 .

[4] 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..

[5] Lee, J.J., Krishnamachari, B., Kuo, C.C.J.: Impact of Heterogeneous Deployment on Lifetime Sensing Coverage in Sensor Networks (IEEE SECON). (2004).

[6] 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.

[7] 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.

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

[9] 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.

[10] 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.