HCTL Open International Journal of Technology Innovations and Research (IJTIR)
http://ijtir.hctl.org
Volume 14, April 2015
e-ISSN: 2321-1814, ISBN (Print): 978-1-62951-946-3

Cooperative OCEAN Based Technique for Isolating Attack in Wireless Sensor Network

M. Samundeeswari[1], **R. Gowri**[2]

sam.it.mit@gmail.com, gowrithirumurugan@gmail.com

Abstract

The Intrusion Detection in the ad hoc networks is used to detect or identify the unwanted or unauthorized access in the Wireless Sensor Network. WSN contains wide range of applications which are exposed to some security issues. WSN consumes plenty of energy to note an intruder. Wireless Sensor Network (WSN) usually contains a little devices with restricted energy, and process power, transmission vary, and memory. Due to the distributed nature of denial of service attack, it is difficult to identify the malicious behavior using the traditional intrusion detection method. The proposed technique will improve the detection accuracy and made defense rate performance against attacks and this method is compared against other existing methods. To evaluate the proposed model performance, energy, drop rate the technique OCEAN is an Observation-based Cooperation Enforcement in Ad hoc Network is used with Ad- hoc On Demand Distance Vector (AODV) protocol and simulated using a network simulator.

Keywords

Intrusion Detection, OCEAN, Wireless Sensor Network (WSN), AODV, etc...

[1]M.Tech Networking, Sri Manakula Vinayagar Engineering College, Pondicherry, sam.it.mit@gmail.com
[2]Associate Professor, Sri Manakula Vinayagar Engineering College, Pondicherry, gowrithirumurugan@gmail.com

Introduction

An intrusion detection system (IDS) [1] is designed to identify the unwanted or unauthorized access in a network. The unauthorized access or login can also be happen within the network or external from the network. Monitor the network activity in order to detect any malicious action or intruder. Intrusion Detection plays a significant role in network security so, applying the idea in WSN makes a lot of sense. There are two approaches in intrusion detection: misuse or signature detection IDS with signature based detection compares the current state of the nodes with the stored nodes profile and it will generate an alarm based on that profile; anomaly detection [2] compares system normal profile with the current activity. In cluster based routing the network is divided into cluster head (CH) and member nodes (MNs) The Member Nodes send their knowledge to the Cluster Head that aggregates the information before sending it out of the cluster toward the base station

Wireless Sensor Network (WSN) is taken under consideration as one of the most important research area in recent years. The number of applications which are growing on wireless Sensor Networks are environment science, health service, military, and etc.WSN has recently tremendously developed in education and in industry sector. In Wireless Ad Hoc Networks (WAHN) uses multi-hop routing to communicate with other nodes. The Wireless Ad-Hoc Network (WANET) is divided into three sub-categories namely Wireless mesh networks (WMN), Wireless sensor
Networks (WSN) and Mobile Ad-Hoc Networks (MANETs). The Wireless Sensor Network has the Broad-Area of WANET

The WSN has classified into two types: structured and unstructured. The sensors are to be preplanned and then deployed is structured and in unstructured WSN all the nodes are to be deployed wireless manner.

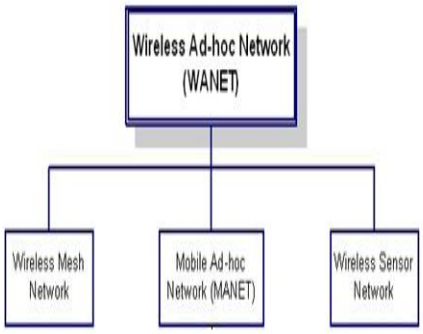

Figure 1: Classification of WANET

WSN uses a vast number of self capable devices, device nodes, to create a network. The sensor in WSN which are small, limited processing and with limited computing resources, and they are inexpensive when compared to traditional sensors. Each node in WSN is capable of sensing the phenomena, it locally process the data and sends those data to at least one or a lot of variety of destinations through a wireless link. WSN which are tiny devices with limited energy, limited memory, limited transmission range, and limited computation power.

Problem Statement

The existing system is based on the fuzzy immune system for detecting intrusion (attacks). Here, a fuzzy misuse detector module (FMDM) has been included to detect the attack node in the cluster network. But still these model lags in detecting the attack in the large-scale networks. When the network size increases the module lags to detect the attack node. Still the network needed an experience to detect the attack node in accurate. These model will mostly work when the source node as attack node. But these model lags when the attack node as intermediate in the cluster. The performance of the network lags when the size of the network increases. To overcome this problem going to propose a protocol called OCEAN (Observation-based Cooperation Enforcement in Ad hoc Networks) which is an extension of the AODV protocol. OCEAN like previous techniques uses a monitoring and a reputation system.

The LEACH (Low Energy Adaptive Clustering Hierarchy) [3] which is the first hierarchical cluster based routing protocol the sensor nodes which forms themselves into a group of cluster. Each cluster group contains a cluster head and some cluster members. The cluster head monitors all other cluster members and performs aggregation the number of information strolling back from the nodes that belong to the varied clusters and transmit that mixture of data to the Base Station (BS). The information from the member nodes is directly sent to the cluster head in LEACH and the sink node uses single –hop routing which is not applicable for large scale networks. And ahs the disadvantage that lot's or too many cluster heads are selected in a particular area. For cluster head exchanges, advertisement the dynamic clustering routing is implemented which consumes more energy.

Related Works

Regarding security, there are many tools which are used to provide security in intrusion detection system. The IDS are an important tool to detect an intrusion in the network. Intrusion detection is an important aspect in network security. Many solutions are proposed in traditional network however it can't be applied on to WSN as a result of the resources of sensor nodes restricted. Ad hoc and WSN security has been studied in a variety of proposals.

[4] Presents two kinds of intrusion detection: anomaly based and signature based. This paper explains several attacks on Wireless Sensor Network and focused only on the anomaly based intrusion detection system. Finally discussed about the several existing approaches and briefly explained various attacks on WSN. And also described some of the existing approaches for anomaly intrusion detection technique which are based on (OSI layer, sliding window, rules, delta grouping algorithm, black hole attack).

This paper [5] evaluates and compares the foremost distinguished anomaly-based IDS systems for hierarchical WSNs and distinguishing their strength and weakness. For every IDS , the architecture and therefore the connected practicality area unit in short introduced, discussed and compared, focusing on each the operational strengths and weakness. Additionally, a comparison of the studied IDSs is carried out employing a set of vital analysis metrics that area unit divided into 2 groups: the primary one related to

performance and therefore the second associated with security finally supported the carried analysis and comparison, a group of style principles area unit terminated, that need to be self-addressed and happy in future analysis of coming up with and implementing IDS for WSNs..

The first to review the problem of intrusion detection in wireless ad-hoc networks [6] they designed the architecture for intrusion detection system in ad-hoc networks. Their theme was based on anomaly detection techniques. However the theme want abundant time, knowledge and traffic to find intrusion. To date most of the present works specialize in the matter of network configuration for expeditiously detecting the intruder among a pre- specified time threshold below the constraints of tight power saving or value potency.

[7] Introduces the intrusion detection formula of low quality for static wireless detector network. The intrusion detection model includes characteristics that verify the typical frequency of execution of order. A distributed formula within which the detector collects the data from the neighboring nodes to analyses the anomalies if any from the neighbors. The intrusion detection formula on identifying anomalies packets received from its neighbors basic alarms to report the anomaly.

The authors of [8] projected ANDES, a centralized frame work for finding devices inflicting anomalies (selective forwarding, sinkhole, flooding attack) within the WSN. In ANDES the Base station correlates the information traffic and routing data to find and localize a male functioning node. ANDES uses straightforward threshold for the number of application packets received, and encompasses a high false positive rate.

Proposed Work

The Wireless Sensor model which consists of a distributed network with a group of nodes consists of clusters of nodes cluster head (CH) and a cluster member (CM). The cluster head which is also called as sink nodes (SN) in a cluster. The cluster head monitors the behaviour of the entire cluster member in the cluster group and transmit the status information to the base station (BS).

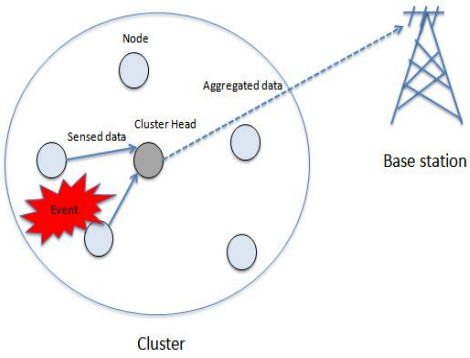

Figure 2: Cluster head and cluster member

According to fig .2 if any attacks are occurred in the cluster member, the cluster head notices the behaviour of the member node and sends the attack information to the base station through the adjacent sink nodes.

In AODV (Ad hoc On Demand Distance Vector) [9] is a routing protocol designed for ad hoc networks. The AODV which performs both unicast and multicast routing. This protocol connects the neighbour routes with the request/reply query. The source node creates a route path to its destination to send the packet. If the source node doesn't have the route it sends the route request (RREQ) packet to the neighbours. The node which knows the destination address which send the RREP message to the source which contains the source ip , broadcast id .The observation based co-operation enforcement which is an extension of the AODV protocol. OCEAN protocol is used to detect the misbehaviour nodes like selfish and malicious node within the proactive routing protocol.

OCEAN

Ocean is a protocol which helps nodes builds intelligent routing and forwarding Selections. OCEAN is designed on top of the AODV. OCEAN protocol focuses on the error free packet forwarding and individual bad behaviour of the nodes. OCEAN classified routing misbehaviour into two classes: misleading and selfish

If a node participate in routes finding however doesn't forward a packet is called misleading node and misleads alternative nodes however if a node doesn't participate in routes finding it's thought of as a selfish node. So as to find misleading routing behaviors, once a node forwards its packet to neighbors, it stores the packet in buffer and monitors other nodes. Then indicates positive or negative value as its watching leads to order to update the rating of neighboring node. If the rating is under faulty threshold, then the neighbor node is considered as misbehavior node and additionally added to RRQ as an avoid list. This node is given a selected time to come to the network because this particular node is wrong suspect of misbehaving or if it's a misbehaving node.
OCEAN [10] consists of five parts to identify the malicious nodes.

1. NeighborWatch: observes or monitors the behaviour of the neighbour's node. When forwarding a packet the packet checksum is stored in the buffer if the neighbour does not forward the packet within a given time period. The default timeout value is 1ms. NeighborWatch enters negative value for that neighbour node and remove its checksum from the buffer. Each forwarding packet compared with the checksum in the buffer if it matches registers a positive event and removes the checksum in the buffer. if it does not matches the packet is not forwarded.

2. RouteRanker: each and every node maintains the rating for their neighbours. The ratings are to be increment and decrement according to the event value as positive or negative.

3. Rank-based Routing: it selects the route based on the information observed from the Neighbor Watch

4. Malicious Traffic Rejection: it rejects all the nodes from which it considered misleading.

5. Second Chance Mechanism: if the node is considered misleading wrongly then the node can became useful again with a second chance.

If the node is said to be the selfish node then by punishing all the traffic from the node is rejected. OCEAN depends solely on direct observations and not second hand reputation. Each and every node maintains a chip count earns chip for forwarding function and loses chip for every request. For incrementing and decrementing the chips there are two categories: optimistic and pessimistic. The optimistic approach increments the chips count only if the neighbour accepts that packet. It doesn't check whether or not the neighbour node within the route actually forwarded the packets or not. The pessimistic approach increments the chip count only if the neighbour node is discovered to forward the packet. In existing the bio inspired artificial immune system is used to detect the DDoS attack by using the Fuzzy Misuse detector Module here, we are proposed a protocol called OCEAN to monitor and observe the nodes which is misleading. This will helpful when the attack node act as intermediate node. By using AODV the number of packets transferred from the source to destination are calculated. And OCEAN uses the direct observations of monitoring neighbour node than second hand reputation method.

Conclusion

Deploying Wireless Sensor Network in an open environment is exposed to some security issues. This paper explains OCAN techniques to find the misleading nodes in the Wireless Sensor Network. The AODV (Ad–hoc On Demand Distance Vector) is used efficiently to find the number of packets sends and received to find the attack node even the node acts as an intermediate node. And the proposed method will improve the detection accuracy than the existing technique. The simulation result shows the comparison of AODV protocol and adding OCEAN technique. The future work of this project is to improve the second chance mechanism of adding nodes back to the list.

References

[1] Peyman Kabiri and Ali A. Ghorbani "Research on Intrusion Detection and Response: A Survey" International Journal of Network Security, Vol.1, No.2, PP.84–102, Sep. [Online] Available at http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.129.698

[2] Md. Safiqul Islam Syed AshiqurRahman, "Anomaly Intrusion Detection System in Wireless Sensor Networks: Security Threats and Existing Approaches", International Journal of Advanced Science and Technology Vol. 36, November,2011 [Online] Available at http://www.sersc.org/journals/IJAST/vol36/1.pdf

[3] H.H. Soliman , Noha A. Hikal , Nehal A. Sakr "A comparative performance evaluation of intrusion detection techniques for hierarchical wireless sensor networks" Egyptian Informatics Journal (2012) 13, 225–238. [Online] Available at http://www.sciencedirect.com/science/article/pii/S1110866512000412

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

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

[6] Gupta, R. Zheng, and A.M.K. Cheng, "ANDES: An anomaly detection system for wireless sensor networks," in Proceedings of the IEEE International Conference on Mobile Ad Hoc and Sensor Systems (MASS 2007), pp.1-9, 2007. [Online] Available at http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=4428636&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D4428636

[7] Wendi Rabiner Heinzelman, Anantha Chandrakasan, Hari Balakrishnan, "Energy-Efficient Communication Protocol for Wireless Microsensor Networks" , Proceedings of the 33rd Hawaii International Conference on System science, , January 4-7, 2000, Maui Hawaii.[Online]Availableat: http://www.gta.ufrj.br/wsns/Routing/leach.pdf

[8] Prashant Kumar Maurya, Gaurav Sharma, Vaishali Sahu, Ashish Roberts, Mahendra Srivastava "An overview of AODV Routing Protocol" , International Journal of Modern Engineering Research (IJMER), Vol.2, Issue.3, May-June 2012 pp-728-732 ISSN: 2249-6645. [Online] Available at:http://ijmer.com/papers/vol2_issue3/AC23728732.pdf

[9] Sorav Bansal Mary Baker, "Observation-based Cooperation Enforcement in Ad hoc Networks", arXiv:cs/0307012v2 [cs.NI] 6 Jul 2003 [Online] Available at http://arxiv.org/pdf/cs/0307012.pdf

[10] Abeer Ghandar, Eman Shabaan, Zakey Fayed, "Performance Analysis of Observation Based Cooperation Enforcement in Ad Hoc Networks", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 6, No 2, November 2011 ISSN (Online): 1694-0814. [Online] Available at http://ijcsi.org/papers/IJCSI-Vol-8-Issue-6-No-2.pdf