Scientific Journal Impact Factor (SJIF): 1.711

International Journal of Modern Trends in Engineering and Research

IJMTER

ISSN (ONLINE) : 2349 - 9745

ISSN (PRINT) : 2393 - 8161

An Implementation of a Technique to Detect and Avoid Denial of Service Attacks in Wireless Sensor Networks

Ashwini M R[1], B S Aparna Rao[2], Kavitha N[3], Neha N Patkar[4], Dr. K Raghuveer[5]

[1,2,3,4,5]Department of Information Science and Engineering ,NIE Mysore.

Abstract-A wireless sensor network (WSN) is a network of spatially distributed autonomous sensors to monitor physical or environmental conditions and passage of data through the network to a base station. The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors.DoS attacks disrupt the entire or a part of WSN network. Detection and avoidance of DoS attacks is necessary. We provide a technique for the same.Nodes are grouped into clusters which have a cluster head which has information about the nodes under it. This paper intends to implement common key authentication mechanism by which cluster head as well as any other sensor nodes in network can identify the communicating node as an attacker node or not. Authentication server will send common key to all nodes and cluster heads. For successful communication, hash codes of the requesting sensor node and cluster head need to match. If they don't then node is said to be attacker. A new key will then be generated and distributed across the all nodes except attacker node. Aim is to make system efficient.

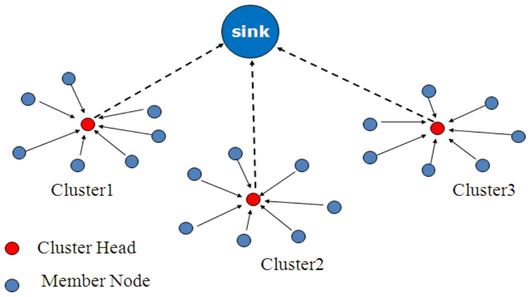
I. INTRODUCTION

A wireless sensor network (WSN) is a network of cheap and simple processing devices (sensor nodes) that are equipped with environmental sensors for temperature, humidity, etc. and can communicate with each other using a wireless radio device. Sensed data collected by sink or base station nodes which have accessed to the infrastructure like internet finally end user can fetch the data by accessing the infrastructure networks.

- The Sensor nodes that form the sensor network. Their main objectives are making discrete, local measurement about phenomenon surrounding these sensors, forming a wireless network by communicating over a wireless medium, and collect data and rout data back to the user via sink (Base Station).

- The sink (Base Station) communicates with the user via internet or satellite communication. It is located near the sensor field or well-equipped nodes of the sensor network. Collected data from the sensor field routed back to the sink by a multi-hop infrastructure less architecture through the sink.

- The user who is interested in obtaining information about specific phenomenon to measure/monitor its behaviour.



Wireless Sensor Networks (WSNs) have being used in many application areas like ocean and wildlife monitoring, manufacturing machinery performance monitoring, building safety and earthquake monitoring, military applications and health related applications. The harsh and unattended deployment of these networks along with that in wireless sensor networks each node has limited energy, computation and storage space makes they are more vulnerable to attacks than wired networks. The simplest form of such attacks is Denial ofService Attack(DoS)which can block any current legitimate communication. However, theadversaries can compromise some sensors and launch the DOS attack by replaying redundant messages or making overdose of fake messages . The DOS is an attempt to make a machine or network resource unavailable to its intended users. Due to the severe security attacks in the wireless media, the network faces various difficulties. Prevention of DOS attack has become a very serious problem in network security. The main aim of this project is to secure the network by build the secure cluster head in each clusters.

II. LITERATURE SURVEY

1. Denial of Services

Awful action or casual failure of nodes generates Denial of Service[1]. The easiest denial of service invasions tries to exhaust the availability of sources to the victim node, by forwarding extra not useful packets and stop user legal network from accessing sources or services to which they are empowered. Denial of service invasion is meant not only for the intruder's attempt to invert, destruct or disrupt network, but also for any event that reduces the ability of network to give a service. In WSN,different types of denial of service invasions in several layers may be executed. The denial of service invasions can be tampering & hindering at physical layer. Collision & hindering at link layer. Dropping packet, fictitious routing information & tunnel at network layer. Inject wrong message & energy exit attacks at the transport layer. The mechanisms to stop denial of service invasions involve payment for sources of network, strong traffic's identification & authentication.

2. Detection of DoS Attack

Initially, network administrators will first detect symptoms such as uniform degradation of network or device performance. Uniformly degraded performance could be due to resource consumption of bandwidth attack. Point-to-point attack can also occur to specific devices in the network, causing the CPU utilization to run up and failure of the host to serve other users. Investigating Denial of Service Attacks[2] often require the use of sniffers or logging at the router to determine the extent of the attack, whether it is propagating to other hosts in the network, and to identify the pattern or signature of the attack. Analysing router and host logs may or may not show the real nature of the attack or may cause false reporting. In some experience with organizations installing commercial network Intruder Detection System, misconfigured attack signature, provided wrong alert indicators. A sniffer at this point helps to identify the real threat. Based on experience, misconfiguration of devices such as hubs and routers can also cause DoS effect. Thus, it is advisable not to eliminate any possibility until the packets are thoroughly examined.

III. PROPOSED SYSTEM

Network is divided in to clusters and each cluster has its respective cluster head that maintains details of each and every node in its cluster. The nodes should be communicate only via their respective cluster heads. The authentication server is responsible for the generation and distribution of common keys for all nodes in the network including cluster heads. It also maintains the attacker node details for future reference and precaution . After receiving the common key, nodes generate the hash code for the the same using various hash functions. Communication requires that they send data along with hash code. After receiving the data, receiver node must compare and match the received hash code with its own . If they match then assume that sender node is the legitimate node and starts communication with it, else it is dropped.

Also threshold value is set by the server for all the nodes in the network. After start of communication , the receiving node increments the count by one for each transaction with that sender node and compared with the threshold value. If it crosses the limit then the sender is assumed to be the attacker. After detecting the attacker node, cluster head sends attacker node details to the authentication server which will then updates the attacker node details ,generate and distributes new keys to all the nodes in the network except the attacker node. When the attacker node tries to re-communicate using old key with any nodes in the network , the network nodes verify the authentication and when it fails the attacker is blocked to communicate with other nodes in the network.

Algorithm:

Detection Algorithm :

Step 1 : Cluster head receives a request message from a node which seeks a communication from another node in a network

Step 2 : Cluster head checks whether the message is normal or not

Step 3 : If it is abnormal , consider the sender as attacker node

Step 4 : If it is normal , compare count with threshold value.

Step 5: If the count is greater than threshold, consider sender as attacker node.

Step 5 : Go to step 1

Avoidance algorithm :

Step 1 : Details of attacker node sent to server as per cluster head's notification

Step 2 : Received attacker node details are stored by server as history record. Generate and send new common key to all nodes except attacker node.

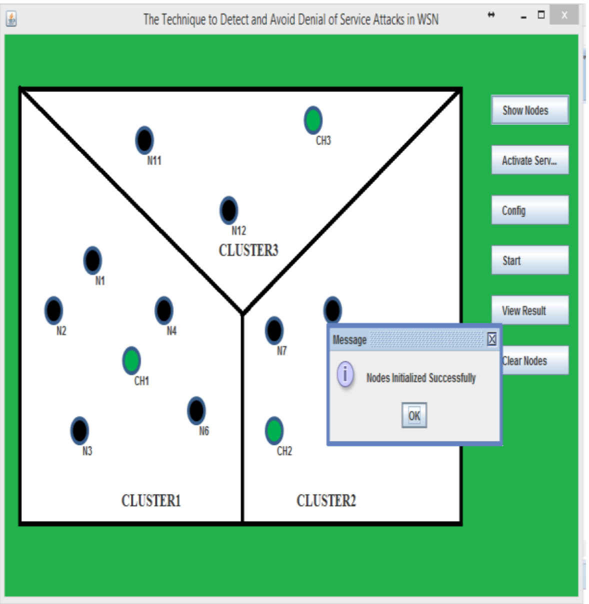
IV. IMPLEMENTATION

The system is divided into 7 modules:

1. **Attacker Module :** This module generates random requests in large numbers in order to attack the system. It tries to guess the authentication key.
2. **Authentication server:** This module generates keys for the sensor nodes and cluster heads. It keeps track of the information of the network elements and also maintains the details of attacker node.
3. **Cluster Head:** This module monitors and mediates communications between sensor nodes of the same clusters or those in other clusters.

4. **Dbcon module:** This module consists of all the databases in the system.
5. **GUI:** This module is implemented using java and gives the outer interface of the system.
6. **Hashing module:** This module is responsible for hashing the generated keys. It produces hash codes that can be used for comparison during communication authentication.
7. **Cluster nodes:** this module is responsible for maintaining the details of all the sensor nodes in their respective clusters.

The implementation is done in eclipse using java with swings.
A snapshot of the implemented interface is below:


The Technique to Detect and Avoid Denial of Service Attacks in WSN

Message

Nodes Initialized Successfully

OK

V. CONCLUSION

This method effectively detects and eliminates DOS attacks in wireless sensor networks using common key mechanism.

DoS attack is a threat for wireless sensor networks . We have used common key authentication mechanism by which cluster head is able to identify an attacker node and inform authentication server. Authentication server keeps the record of attacker node details which helps to avoid further attacks. As an attacker node is identified , a new common key is generated and distributed to all nodes except the attacker node by the authentication server, thus blocks the attacker node to communicate with other nodes in the network. This mechanism helps to detect and avoid DoS attack.

REFERENCES

[1]Security Issues in Wireless Sensor Network: A ReviewPooja Gupta, Dr.NaveenHemrajani ISSN: 2277-9655 , [Gupta, 2(5): May, 2013].

[2]Understanding the Various Types of Denial of Service Attack By Raja Azrina Raja Othman.

[3]. “Denial of service attacks in wireless sensor networks: issues and challenges” Al-Sakib Khan Pathan1 Department of Computer Engineering, Kyung Hee University1 Seocheon, Giheung, Yongin 446-701, South Korea .

[4]. ”Chaudhari H.C. and Kadam L.U.S wami Vivekanand Mahavidyalaya “Wireless sensor networks: security attacks and challenges”.

[5]. DevuManikantanShila, Yu cheng, and Tricha Anjali, “Mitigating selective forwarding attacks with a channel-aware approach in WMNs”,IEEE transactions on wireless communications, vol. 9, no. 5 , may 2010.

[6]. G.Lin and G.Noubir . “On link layer Denial of service in data wireless LANs”. Wireless communications and MobileComputing, 5(3):273-284, May 2004.

[7]. SudipMisra, Sanjay K. Dhurandher, AvanishRayankula and DeepanshAgrawal, “Using honey nodes for defense against jamming attacks in wireless infrastructure-based networks”, computers and electrical engineering, may 2009.

[8]. Deng J, Han R, Mishra S. “Defending against path-based DoS attacks in wireless sensor networks”. SASN’05, ACM New York, NY, USA, 3rd ACM workshop on Security of Ad Hoc and Sensor Networks Table of Contents Alexandria, VA, USA, Nov 7, 2005: 89−96.