Intrusion Detection System In Wireless Sensor Network

Divyashree G, Durgabhavani A, KavyaM, Anushree Gudoor, Madhukar B Shetty

Abstract: The constant growth in network industry has put forward some queries regarding vulnerability and security of a computer network. Intrusion detection is the mechanism of identifying the unauthorized packets that enter an organization’s network. It acts as a shield and informs the system administrator when some unwanted traffic is seen to flow inside. The intrusion detection system has a lot of challenges; it must look up the event log and try to classify the packets that are malicious. A wireless sensor network (WSN) is one which consists of many low-cost nodes, whose position are not fixed in a network and are subjected to change. The main aim of this paper is to simulate intrusion in a WSN and perform a comparative analysis between DHCP(Delegation of Hosts), packet drop ratio and overhead. Hence, NetSim is used to identify intrusions in standalone devices or hosts in a computer network. This system monitors the incoming and outgoing traffic of standalone devices and will notify the executor if some malicious activities are identified. It captures a screenshot of the current system and compares it with the previously captured screenshot. On deletion or modification of any system files a notification will be received by the administrators of the system to handle the suspicious activity. The different types are Misuse and anomaly detection

Keywords: Intrusion Detection System (IDS), Wireless Sensor Network (WSN), Probe attacks, Network Simulation Tool (NS2), DoS (Denial of Service) attacks, Network Security.

I. INTRODUCTION

Despite the number of firewalls and widespread use of automated attack tools, network intrusion has posed a common problem. There are large numbers of malicious packets or viruses that have the capability of causing mass damages in the network. Hence Network Security places an important role in any organisation. While mechanisms like encryption, authentication, policy management and firewall have been proposed they still cannot rule out network attacks completely. The intruders still find many ways to tackle down these measures. Hence, we need a second layer of defence which is the intrusion detection system. Several types of IDS exist due to variation in network configurations.

1. Classification of IDS
A. Network based Intrusion Detection System (NIDS).

The system is located at specific points to analyze the difference in the behavior of network traffic. It evaluates the moving subnet traffic and maps this traffic to a set of already identified attacks. Once the attack is identified, the system users are notified. These systems can also compare the signatures of similar packets to analyze and drop packets which are found to be harmful based on their signatures which match up against the records of NIDS. There are two types of NIDS. They are Online NIDS (which works on real-time data) and Offline NIDS (which works on stored data).

B. Host based Intrusion Detection System (HIDS).

This system is used to identify intrusions in standalone devices or hosts in a computer network. This system monitors the incoming and outgoing traffic of standalone devices and will notify the executor if some malicious activities are identified. It captures a screenshot of the current system and compares it with the previously captured screenshot. On deletion or modification of any system files a notification will be received by the administrators of the system to handle the suspicious activity. The different types are Misuse and anomaly detection.

II. WIRELESS SENSOR NETWORKS

This is a type of computer network which contains many nodes which are mobile and do not have a static positioning in the network. WSNs involve deploying of hundreds of small nodes and are hence in trend for the past few years. Predetermination of the position of sensor nodes is not required. This feature enables us to use these networks in regions which are not accessible or in the relief operations during disasters. The limited power and shorter range compel the sensor nodes to work together in multi-hop wireless communication architectures to transmit the data sensed and collected to the closest base station. In wired networks the physical wiring helps to prevent intervention of a malicious user but in the case of wireless networks many security challenges come into picture that acts as prerequisites in the effective deployment of WSNs specifically in military. The resource-starved nature of sensor nodes poses a problem in the aspects of security. When security is maximized at each node, the system resources get exhausted very quickly and hence the nodes’ lifetime will be affected. WSN are vulnerable due to two major reasons: 1) They use broadcasting for data transmission and due to this reason are more susceptible to various types of security attacks. 2) The nodes sometimes are placed in non-safe environments where much protection is not available to them. The four elementary components of a WSN are: (1) many distributed mobile sensor nodes; (2) a wireless interconnecting network; (3) an information-gathering base station (Sink); (4) a set of devices to process, analyze and interpret the data received at the base station.

2. Media Access Control Layer (MAC)

This is a sub layer of the Data Link Layer. The other sub part being the Logical Link Layer. The MAC Layer is important especially in LAN’s, nearly all of which use multi-access channel as basis of their networks.
A MAC address is a unique address referred as the physical address since it is associated with the network Interface card (NIC). This MAC address helps in uniquely identifying each host on a network. This makes sure that each device shall have different and unique MAC address. There are several protocols that come under this layer, such as Random-access protocols, Controlled access Protocols and Channelization Protocols. Generally, for a network, we need high throughput, high data rate, high packet-drop ratio, low end-to-end delay, low overhead. When we have an intruder in the network, these parameters are worsened that decreases the efficiency of network. To retain the same working and efficiency we have designed two algorithms called Node Deployment Algorithm and Routing Table Formation.

III. LITERATURE SURVEY

[1] This paper proposes modern techniques and methodology for identifying intrusion in a network. It puts forward, the various advantages and limitations of modern IDS. The issues of false positives and the consequences of such actions in IDS are explained. Various methods are used in today’s world for securing information like software, hardware, and hardware-software and organizational. The major purpose of all these techniques is to enhance information security. IDS in general are either a hardware or software complex whose major aim is to detect intrusion in a network. [2] In this paper, the individual data packets are duplicated in the Internet Protocol layer (IP). The number of times duplication is to be done is estimated by route entries of the destination. Each packet being sent is identified distinctly with a tree-id which is made available by NS2 and the excess unnecessary packets are eliminated in the receiver’s IP layer. The Watchdog algorithms are used to identify the malicious nodes and the Path rater, to identify and react to the attacks by separating the malicious nodes from the original network. After the Watchdog module identifies misbehaving node, the Path rater module removes that specific path from the route cache and strives to find an alternative route to the destination. This technique identifies packet replication attacks and reduces the packet replication. [3] MANETS usually use the watchdog method for implementing IDS which has several disadvantages. Hence this paper proposes an alternate technique which is the Adaptive Acknowledgment (AACK). The TWOACK scheme was generally used but the detection overhead was high, and the efficiency was a bit low. This proposed technique is an advancement of this TWOACK and ensures better efficiency and lesser overhead. The implementation of this was done through an NS2 simulation to evaluate the system. Adaptive Acknowledgment is built over the AODV (Ad-hoc Distance vector) routing protocol as it provides an efficient and easy method for routing packets. The AACK solves two problems faced with watchdog technique 1. Receiver Collision and 2. Limited power transmission. [4] This paper aims to identify the location where a specific event which emits a signal that can travel over a larger area using wireless sensor networks. This technique uses sensor binary beliefs, a likelihood matrix whose highest value implies to the event’s location. The importance of this is that it Subtracts on Negative Add on Positive (SNAP), an algorithm that allows us to create a likelihood matrix in an efficient way by adding pm 1 contribution from the sensor nodes based on their alarm state (positive or negative). This proposed technique ensures production of good accurate results with ample amount of fault tolerance. [5] This paper describes an intrusion detection framework for WSN. It tries to solve the problem using semantic and multi-agent techniques. The framework includes layers such as the network layer, (specifying the topology), the semantic layer (refers to security ontology), the model layer and the co-operative layer (refers to how the nodes co-operate between each other for intrusion detection). They have described agent node and common nodes in which only the former has the intrusion detection model. They define a co-operative intrusion detection algorithm in which the sensor nodes collect the data and pass it onto the agent node for the detection. The result is then passed on to another algorithm called detect Intrusion which qualifies the result for intrusion detection based on the security ontology items. [6] WSN are facing threats due to different types of attacks. When we apply intrusion detection and prevention methods together it results in communication overhead and excessive energy consumption by the nodes. Hence this paper proposes an energy efficient routing method to solve this issue. The method consists of three main stages namely, initial construction phase, a sensing data transmission phase, and a re-construction phase. In the first phase, therouting and topology of network is constructed. In sensing data phase, the node creates an event and forwards it. In the reconstruction phase the network topology and routing table is reconstructed which decreases the overhead of communication and the energy consumption.

IV. IMPLEMENTATION

A normal network consists of many nodes trying to interact with each other. A simple architecture would consist of a Source(S), malicious node-Intruder(M) and the Destination(D). While passing information from Source to Destination, we need to connect them through the network which might have malicious nodes. In a normal system, we see that the data is divided into packets and move from Source to Destination through the network. The respective acknowledgements are received by the Sender. In case of the intruder being a part of this network, the packets might pass through this node before it reaches the Destination. While these packets go through the intruder, we experience packet loss and heavy delays in acknowledgement. Since our System is a NIDS, traffic will be analyzed in the network to find the malicious activity. As soon as it identifies the node as malicious on basis of the signatures or type of traffic moving it informs the system administrator to block the node and tries to find a different path to the Destination. Such a system already exists.

A. Proposed architecture for Intrusion Detection System.
We use the MAC layer of OSI model. The OSI have 7 layers of which the Data Link layer has been divided into two layers. They are: MAC Layer and the Logical Link Control Layer(LLC). The MAC Layer controls the hardware responsible for interaction with media whereas the LLC is mainly designed for flow control,error management and multiplexing. We introduce the Sliding Window here in this layer for data transfer.Since the window size can be now variable to the max Window Size, we tend to achieve high throughput and low overhead, which makes the network better and efficient. As seen in the below diagram the source first takes the unsafe path containing the intruder. As and when it gets to know about this intruder due to heavy packet loss and delay in acknowledge, we block this path (the one indicated with a red cross) and find another route to transfer data to the Destination (the one indicated with a green tick). Once another route us established we send packets in a window. (As seen in the diagram)

In such systems, the network is altered to lessen the overall efficiency of the system. In our paper we describe two algorithms, namely Node Deployment Algorithm and Routing Table Formation. The former algorithm enables to deploy the nodes in a region. The node count and Node Distance are served as inputs to this algorithm. The mapping of Node ID and its position decides the output. The routing tables for all nodes are formed from the latter algorithm. Information about other nodes present in the network is given by the routing table. The information consists of node id and inter node distance.

As seen above, we start off having information about the Node Counts and inter node Distance. We run a loop till we complete iterating all nodes. In each loop we calculate the distance from node 0 by adding the previous node position with distance. First node will be at 0 distance. We then generate a Node Id and a map with its node_position.
We fill in values for the \( i \)th node in the table by calculating its distance from all the other nodes in the network.

**B. Hardware components.**
The deployment of such planned architecture needs suitable supporting hardware. For this purpose, we require a processor of any specification with the speed of above 500MHz RAM of memory 512MB, Hard Disk of 18 GB, keyboard, mouse and VGA and High Resolution Monitor.

**C. Software components.**
The implementation and testing of the following project demands the utilization of the following software: Ubuntu Operating System, Ns2 simulation tool, Language-AWK and TCL.

**V. RESULTS**

**Fig V. Packet Drop Ratio**
From the above graph, we can see that the packet drop ratio is improved in the proposed system. The existing has a ratio of about 0.918 while the proposed has around 0.9241 which is 1% above.

**Fig VI. Overhead**
Overhead is defined as the ratio of total number of packets sent at the sender end to the number of packets received at the receiver end. From the above graph, it is implied that the proposed system has a smaller ratio which is of high benefit. The existing has around 2.557 while the proposed is around 2.442.

**Fig VII. End-To-End Delay**
This defines the total delay while transmitting the complete package. This needs to be as minimum as possible. As seen, the existing has a value of 2.525 and proposed as 2.103.
Fig VIII. Throughput
It is defined the maximum amount of data that can be passed from one node to another for a given unit of time. The existing system has a throughput of about 165.61 while the proposed has about 184.60 which are better.

VI. CONCLUSION
For the improvement of efficiency and faster data transfer in the network we acknowledge the concept of resizable window. The performance of the proposed system was found to be better than the existing system with the following parameter values.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Without Attacker</th>
<th>With Attacker (Existing)</th>
<th>Proposed System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Throughput</td>
<td>206.27</td>
<td>165.61</td>
<td>184.60</td>
</tr>
<tr>
<td>End-to-End delay</td>
<td>2.31498</td>
<td>2.52565</td>
<td>2.10316</td>
</tr>
<tr>
<td>Packet-Drop Ratio</td>
<td>1.0</td>
<td>0.9168</td>
<td>0.9241</td>
</tr>
<tr>
<td>Overhead</td>
<td>2.754</td>
<td>2.557</td>
<td>2.442</td>
</tr>
</tbody>
</table>

ACKNOWLEDGMENT
This work is done, supervised and supported by the students and faculty members of the Department of Computer Science and Engineering, BMS Institute of Technology, Bangalore.

REFERENCES