N. Mohamed Bayas *et al*, International Journal of Computer Science and Mobile Applications,
Vol.2 Issue. 1, January- 2014, pg. 101-108 **ISSN: 2321-8363**

HIDING PACKET SEND THROUGH MULTIPLE TRANSMISSION LINE BY VIRTUALLY IN AD HOC

N. MOHAMED BAYAS[1], Mr. S.Rajesh[2]

[1] PG Student, [2]Assistant Professor , Department of Computer Science and Engineering,

PRIST University, Trichy District, India

([1] mdfayasn@gmail.com)

Abstract

The nature of the Ad hoc Network leaves it vulnerable to intentional attacks. This intentional interference with wired transmission can be used for mounting denial of service attacks on Ad hoc Network. The protocol specification and network secrets can low effect attacks that are difficult to detect. In this work a problem of selective attacks is actively for a short period of time, selectively targeting messages of high importance. A selective attack on TCP can be launched performing real time packet classification at physical layer. Every hiding of the packet to be sent through many transmission lines but the transmission line will be selected based on virtually to setting a path by randomly. The random of selecting the transmission lines for the packet that will be protected from the unauthorized users. The transmission line can be changed from time to time based on the current traffic and the topology. The sending of every packet from source to destination via the various intermediate nodes can be changed dynamically. We analyze and evaluate have been conducted to verify the effectiveness and efficiency of using the transmission line.

1 INTRODUCTION

The incredible growth of the Internet and the network-based applications has contributed to enormous security leaks. Even the cryptographic protocols, which are used to provide secure communication, are often targeted by diverse attacks. Intrusion detection systems (IDSs) are often employed to monitor network traffic and host activities that may lead to unauthorized accesses and attacks against vulnerable services. Most of the conventional misuse-based and anomaly-based IDSs are ineffective against attacks targeted at encrypted protocols since they heavily rely on inspecting the payload contents. To combat against attacks on encrypted protocols, we propose an anomaly-based detection system by using strategically distributed monitoring stubs (MSs). We have categorized various attacks against cryptographic protocols. The MSs, by sniffing the encrypted traffic, extract features for detecting these attacks and construct normal usage behavior profiles. The effectiveness of the proposed detection and trace back methods are verified through extensive simulations and Internet datasets.

Cryptographic protocols rely upon encryption to provide secure communication between involved parties. Secure Socket Layer (SSL) and its successor Transport Layer Security (TLS) are extensively used to provide authentication and encryption in order to transmit sensitive data. The purpose of all these encrypted protocols is to resist malicious intrusions and eavesdropping. The number of attacks against encrypted protocols has increased significantly in recent times. With the evolution of high-speed Internet and processing power, it is only natural to assume that more sophisticated attacks will emerge and pose serious threats to encrypted protocols. In a distributed

detection mechanism that is able to detect the anomalous events as early as possible, especially before significant damage is inflicted on the victim by the attacker.

2 PROBLEM DEFINITION

The coordination of distinct agents monitoring the network flows at different points requires an appropriated architecture that must be developed. It address these issues in the project effectively and attempt to design adequate solutions to these problems. We propose the catching scheme, which is not limited to constructing a defensive mechanism to discover attacks; we devise an aggressive countermeasure that not only detects a potential threat, but also investigates the root of the threat by attempting to trace back the attacker's original network or sub network. To deal with packet droppers, a widely adopted countermeasure is multipath forwarding in which each packet is forwarded along multiple redundant paths and hence packet dropping in some but not all of these paths can be tolerated.

To deal with packet modifiers, most of existing countermeasures aim to filter modified messages en-route within a certain number of hops. These countermeasures can tolerate or mitigate the packet dropping and modification attacks, but the intruders are still there and can continue attacking the network without being caught. To locate and identify packet droppers and modifiers, it has been proposed that nodes continuously monitor the forwarding behaviors of their neighbors to determine if their neighbors are misbehaving, and the approach can be extended by using the reputation based mechanisms to allow nodes to infer whether a non-neighbor node is trustable. This methodology may be subject to high-energy cost incurred by the promiscuous operating mode of wireless interface moreover, the reputation mechanisms have to be exercised with cautions to avoid or mitigate bad mouth attacks and others. Recently, Ye et al. proposed a probabilistic nested marking (PNM) scheme. But with the PNM scheme, modified packets should not be filtered out en route because they should be used as evidence to infer packet modifiers; hence, it cannot be used together with existing packet filtering schemes.

In this, Project proposes a simple yet effective scheme to catch both packet droppers and modifiers. In this scheme, a routing tree rooted at the sink is first established. When sensor data are transmitted along the tree structure toward the sink, each packet sender or forwarder adds a small number of extra bits, which is called packet marks, to the packet. The format of the small packet marks is deliberately designed such that the sink can obtain very useful information from the marks. Specifically, based on the packet marks, the sink can figure out the dropping ratio associated with every sensor node, and then runs The proposed node categorization algorithm to identify nodes that are droppers/modifiers for sure or are suspicious droppers modifiers. As the tree structure dynamically changes every time interval, behaviors of sensor nodes can be observed in a large variety of scenarios. As the information of node behaviors has been accumulated, the sink periodically runs The proposed heuristic ranking algorithms to identify most likely bad nodes from suspiciously bad nodes. This way, most of the bad nodes can be gradually identified with small false positive.

That is, it can be deployed together with the false packet filtering schemes, and therefore it cannot only identify intruders but also filter modified packets immediately after the modification is detected.

3 EXISTING SYSTEM

3.1 OVERVIEW

The Existing system, many intrusion detection systems have been proposed to detect the intruder, however it will ensure that the attack paths and the information over it. And ineffective when they encounter encrypted traffic. In some systems, from the packet losses they found that attacker may hack the data. The sender will send the details of packets to the receiver. From the packet loss the existing systems are finding the attacks.

3.2 DISADVANTAGES OF THE EXISTING SYSTEM

The client knows the data loss after it reached the intruder level, when a hacking of the data packets occurred only raises the error report.

Client may trace back it but it's inefficient because of without using a monitoring stub. The receiver checks the count of the packets and received packets count. If it is differed from the data which sent then the data may hacked.

4 PROPOSED SYSTEM

4.1 OVERVIEW

Monitoring stub will helps to improve the efficiency of the trace back mechanism and also identifying the paths.

Behavioral distance used to find out the hacking of information before the data corrupted or updated by the intruder.

Combating against attacks on encrypted protocols in the wireless network environment. The proposed detection scheme manages to avoid false alarms when the flash crowd occurred.

4.2 ADVANTAGES

1. Save from data files, altering program and altering content of message.

2. To confuse the attackers by passing the information send another route instead of actual route.

5 SYSTEM IMPLEMENTATION

5.1 MODULES DESCRIPTION

5.1.1 PACKET HIDING

At the Physical layer, a packet m is encoded, interleaved, and modulated before it is transmitted over the wireless channel. At the receiver, the signal is demodulated, de-interleaved and decoded to recover the original packet m. Nodes A and B communicate via a wireless link. Within the communication range of both A and B there is a congested node J. When A transmits a packet m to B, node J classifies m by receiving only the first few bytes of m. J then corrupts m beyond recovery by interfering with its reception at B.

5.1.2 AUTHENTICATION MODULE

This module contains two sub modules:

1. **User**
2. **Administrator**

5.1.2.1 User

User can view their personal information and the data which sent by him. In the server module have the static and secure login to enter and starts the server to receive the data.

5.1.2.2 Administrator

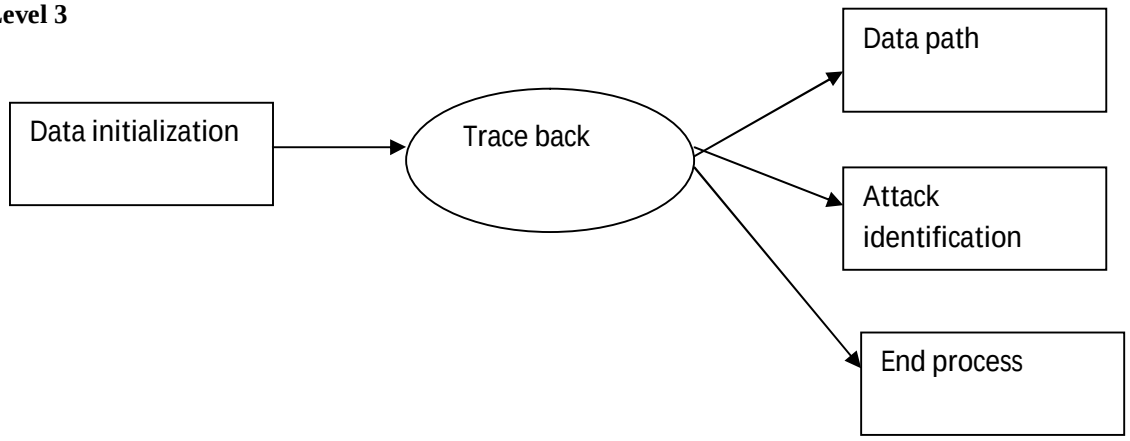
The admin will have permission to view the entire processes done by the user. The user can only view the authenticated page after getting registered to the approach.

5.1.3 BEST PATH MODULE

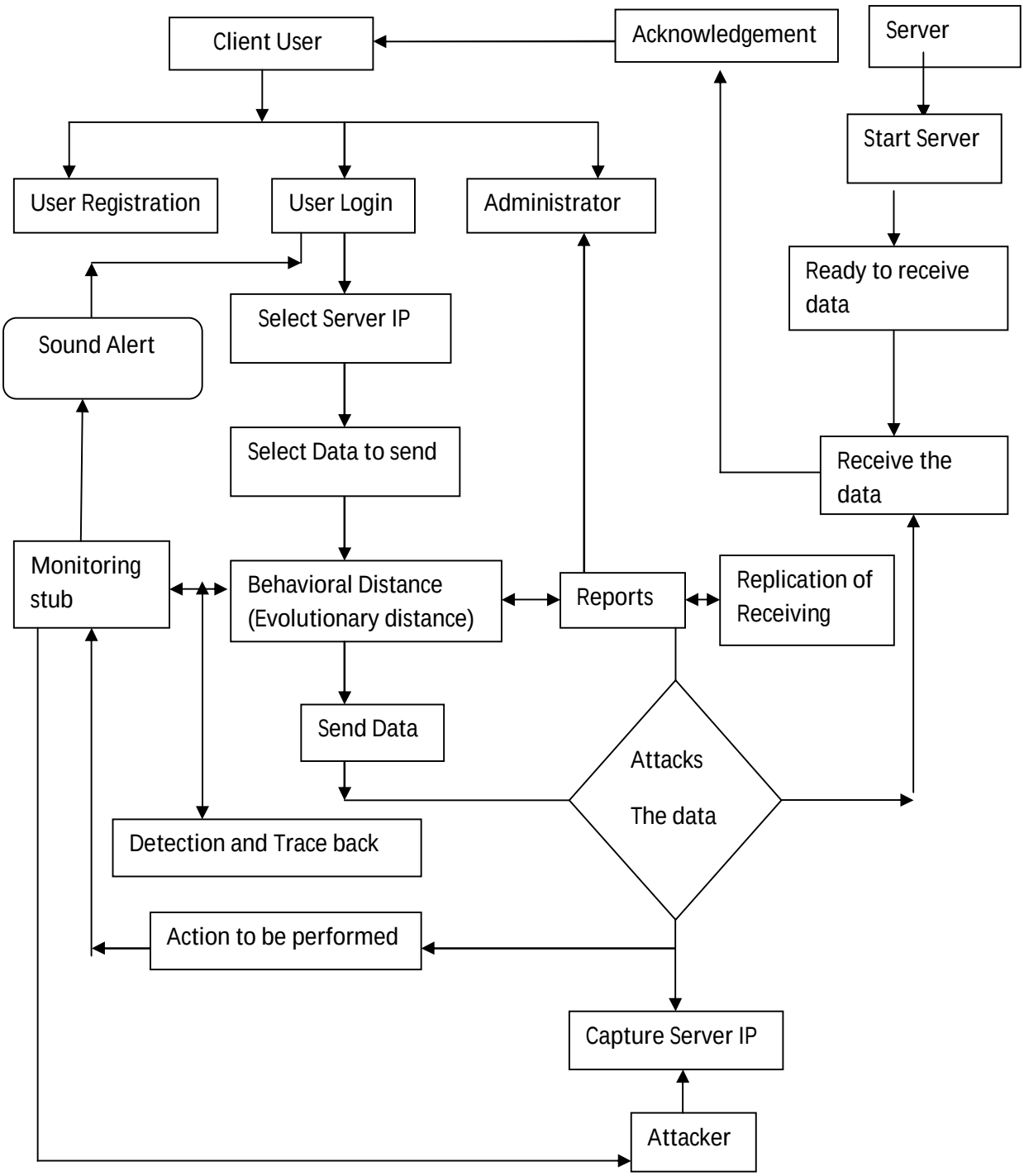
The network has divided by workgroups. This module will help us to get the connected and the active systems in the network. After getting login to the process, this module will get the connected systems and shows the best path to the users. The user can select the best path to deliver their data by file transfer. The disconnected and the shutdown systems are not visible in the list.

6 DATA FLOW DIAGRAM

Level 3



7 SYSTEM ARCHITECTURE



8 CONCLUSION

This Project proposes a simple yet effective scheme to identify misbehaving forwarders that drop or modify packets. Each packet is encrypted and padded so as to hide the source of the packet. The packet mark, a small number of extra bits, is added in each packet such that the sink can recover the source of the packet and then figure out the dropping ratio associated with every sensor node. The routing tree structure dynamically changes in each round so that behaviours of sensor nodes can be observed in a large variety of scenarios. Finally, most of the bad nodes can be identified by The heuristic ranking algorithms with small false positive. Extensive analysis, simulations, and implementation have been conducted and verified the effectiveness of the proposed scheme.

SAMPLE CODINGS

```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Windows.Forms;
using System.Data.SqlClient;
using System.Net;
using System.IO;
using System.Net.Sockets;



namespace Sender
{
   public partial class userhome : Form
   {
      string strname;
      public userhome(string strnme)
      {
         InitializeComponent();
         strname = strnme.ToString().Trim();
      }
      SqlConnection con = new SqlConnection("server=TECHCODES-5;uid=sa;pwd=abc;database=catch;");

      private void userhome_Load(object sender, EventArgs e)
      {
         try
         {
            groupBox1.Text = strname.ToString().Trim();
         }
         catch (Exception ex)
         {
            MessageBox.Show(ex.ToString());
         }
      }
```



```
    private void linkLabel4_LinkClicked(object sender, LinkLabelLinkClickedEventArgs e)
    {
       this.Close();
    }

    private void linkLabel6_LinkClicked(object sender, LinkLabelLinkClickedEventArgs e)
    {
       try
       {
          groupBox2.Visible = true;
          NetworkBrowser nb = new NetworkBrowser();
          foreach (string pc in nb.getNetworkComputers())
          {
             listBox1.Items.Add(pc);




          }
       }
       catch (Exception ex)
       {
          MessageBox.Show(ex.ToString()+"Currently Not Connect to wireless", "Info");
       }

    }

    private void linkLabel3_LinkClicked(object sender, LinkLabelLinkClickedEventArgs e)
    {

    }

    private void linkLabel1_LinkClicked(object sender, LinkLabelLinkClickedEventArgs e)
    {
       filetransfer filetrans = new filetransfer();
       filetrans.Show();
    }
  }
}
```

REFERENCES

1. H. Chan and A. Perrig, “Security and Privacy in Sensor Networks,” Computer, vol. 36, no. 10, pp. 103-105, Oct. 2003.

2. C. Karlof and D. Wagner, “Secure Routing in Wireless Sensor Networks Attacks and Countermeasures,” Proc. IEEE First Int’l Workshop Sensor Network Protocols and Applications, 2003.

3. V. Bhuse, A. Gupta, and L. Lilien, "DPDSN Detection of Packet-Dropping Attacks for Wireless Sensor Networks," Proc. FTheth Trusted Internet Workshop, 2005.

4. M. Kefayati, H.R. Rabiee, S.G. Miremadi, and A. Khonsari, "Misbehavior Resilient Multi-Path Data Transmission in Mobile Ad-Hoc Networks," Proc. FTheth ACM Workshop Security of Ad Hoc and Sensor Networks (SASN '06), 2006.

5. R. Mavropodi, P. Kotzanikolaou, and C. Douligeris, "Secmr—A Secure Multipath Routing Protocol for Ad Hoc Networks," Ad Hoc Networks, vol. 5, no. 1, pp. 87-99, 2007.

