# Secure Wireless Network System against Malicious Rogue Threats (System Attacks) within cooperative distributed network and wireless network

Latesh Kumar K.J, Research Scholar, Department of CSE, SIT, Tumkur-572103, latesh.kj@hotmail.com,
Dr.Lawrance R, Director, School of MCA, ANJA College, Sivakasi, lawrancer@yahoo.com

**Abstract**— With the expanse of the Internet and the increased reliance on computer networking technology for everyday business, the need to protect electronic data and communication from malicious attack has become increasingly critical. This paper addresses the rogue system problem, a significant threat in modern networks. A rogue system is a device installed within a network without the authorization or knowledge of network administrators, which is typically engaged in unauthorized activities. These systems pose a major threat to network data and resources, potentially resulting in the exposure of sensitive information or network performance degradation. This paper presents analysis and solutions for rogue system threats within a cooperative distributed network environment and within various types of wireless environments. In addition, a tool is presented which enables high speed network packet logging, for the purpose of rogue system detection, using inexpensive equipment in a scalable distributed storage infrastructure. Also the development of a secure communication protocol which protects a distributed network from potential rogue system attacks while enabling the implementation of bandwidth conservation techniques for efficiency. An important enhancement of a standard wireless communication protocol for the purpose of preventing both insider and outsider rogue eavesdropping attacks. A novel packet payload slicing technique for the purpose of detecting rogue wireless access points within a corporate network environment. Analyses of the potential of host-based rogue wireless man-in the middle attack detection. The development of a tool for high speed traffic analysis to aid in rogue system detection. Rogue system threats will continue to grow as networks become more complex and new attack techniques evolve to better evade detection. The future direction of this work includes applying these techniques to newly identified threats for the purpose of gauging the effectiveness of the proposed methods and to aid in discovering new means of defending against rogue system attacks. In addition, rogue threats in less traditional types of network environments, such as peer-to-peer and personal area networks, will be addressed in order to provide protection from all means of electronic rogue system attacks.

**Index Terms**— Wireless Network, Intrusion Detection, Local Round-Trip Time (LRTT).

## 1 INTRODUCTION

THE expanse of the Internet has provided a means for millions of people to quickly access information from almost anywhere in the world. Not only one can gather a vast amount of news, facts, and other public information, but access to private data such as bank accounts, corporate information, and confidential email is readily available as well. The ability to access this type of private data provides a great incentive for mischievous parties to attack network communication in order to steal this confidential data. It is important for users and administrators of computer networks to be able to protect against many different methods of attack. One method of executing a variety of types of attacks is through the use of Rogue systems. This Research area presents solutions for defending against rogue system attacks and detecting the existence of such systems [1].

### 1.1 Corporate Network

For the purpose of this research the term "corporate network" refers generally to a network which is centrally managed and is comprised of data servers and a number of individual end user systems. Such networks contain valuable company information including employee personal data, customer information, financial information, and possibly trade secrets. Whether the company is a small business with only a few employees, or a billion dollar international conglomerate, it is vital that the information contained within the computer network remain secure for the wellbeing of the company. Network administrators who are charged with protecting these corporate networks must be prepared to defend against a wide variety of attacks. Viruses and worms are two related types of attacks which infiltrate computer networks by means such as exploiting a weakness in an application running on systems within the network. Viruses are characterized by a manual mechanism of spreading such as through email. Worms, however, are self-propagating and may infect a system without depending on some action to be taken by a user of the victim system. The effects of a worm or virus infection can vary greatly as the infection is essentially a programming executing on the victim system. The malicious program can engage in activities such as erasing files, copying data, forwarding the infection to other systems, or consuming resources such as memory, storage, and CPU [2],[3].

Denial-of-Service (DoS) attacks may be very costly to a company in terms of lost time and money. The purpose of a

DoS attack is to somehow render the victim network useless, typically by overwhelming the network or systems on the network resulting in congestion levels which prevent the efficient flow of data through the network. Distributed DoS (DDoS) attacks are an extremely potent form of the attack because in this scenario the attack is launched from a large number of locations making identifying the source of the attack very difficult. While the attack is being executed employees may be unable to perform their duties and customers may be unable to utilize services. In terms of lost time and revenue, and the degradation of customer satisfaction, the negative impact can be dramatic.

An individual computer hacker gaining access to a corporate system is a very targeted and dangerous attack. This motive behind such a targeted attack is typically for the purpose of obtaining some kind of confidential information. Financial information, private customer or employee data, and trade secrets are all valuable pieces of information to an attacker. The loss of such information may have a significant negative impact on the finances of the company as well as the reputation of the company. Protecting a computer network requires the implementation of a variety of devices and procedures. Firewalls, virus scanners, and intrusion detection systems (IDS) are commonly used devices which are designed to protect a network from outside attack. Network resources are typically password protected to prevent access by unauthorized parties. Highly trained and knowledgeable individuals are crucial in order to administer the network protection plan. A plan which utilizes knowledgeable personnel and state-or-the-art security devices may provide an effective defense against network attacks, however, attacks evolve and new attacks are created leaving even highly protected networks vulnerable to compromise.

### 1.2 Rogue Systems

Network administrators typically focus on protecting the gateway to the Internet in order to prevent outsiders from entering the network. However, in this case an outsider may be able to associate with the rogue wireless access point to gain access to the network. Thus, in order to fully secure the network, administrators must not only protect the gateway, but must defend against rogue devices which may potentially exist in the network. Rogue systems are not limited to wireless access points as any network device could potentially be configured to be a rogue system. This fact makes detecting rogue systems very difficult as rogue systems can infiltrate a network in many ways and engage in a variety of malicious activities. Thus, network administrators and end users must not only know what types of rogue systems may exist, but must also know how to detect or defend against these systems. This dissertation addresses the rogue system problem within a cooperative distributed network environment and within various types of wireless environments

## 2 BACKGROOUND

### 2.1 Wired Network Rogue Systems

In a corporate network there is typically a significant barrier-to-entry from being able to install a rogue device close to the core of the network. This is a physical barrier as access to core network hardware is not accessible except by authorized personnel. A rogue device deep within the routing infrastructure of a network would be in position to do a significant amount of damage in terms of data and system compromise. However, it is not required that a rogue device be installed in this manner in order to attack network resources. The easiest access to a network is obtained at the edge. Throughout corporate offices there are ethernet jacks which are used to connect desktop machines for employee use. These jacks may be very easy to access and are an easy target for a rogue device to be connected. It is possible that unused ethernet ports are not active and cannot be used without the authorization of network administrators. However, if this is the case an authorized system can simply be disconnected from the ethernet jack and be replaced by the rogue device. In a corporate network there is typically a significant barrier-to- entry from being able to install a rogue device close to the core of the network. This is a physical barrier as access to core network hardware is not accessible except by authorized personnel. A rogue device deep within the routing infrastructure of a network would be in position to do a significant amount of damage in terms of data and system compromise. However, it is not required that a rogue device be installed in this manner in order to attack network resources. The easiest access to a network is obtained at the edge. Throughout corporate offices there are ethernet jacks which are used to connect desktop machines for employee use. These jacks may be very easy to access and are an easy target for a rogue device to be connected. It is possible that unused ethernet ports are not active and cannot be used without the authorization of network administrators. However, if this is the case an authorized system can simply be disconnected from the ethernet jack and be replaced by the rogue device. Various security mechanisms may be in place which identify the system connected to each ethernet port and would prevent a rogue device, without modification, from being properly configured in the network. A common method of doing this is through MAC address filtering which depends on the MAC address of the client machine for identifying network systems. This information however is easily spoofed and a rogue system can be configured to mimic the settings of the authorized system. A rogue device can launch a variety of attacks by injecting traffic into the network or by mimicking the authorized system and attempting to penetrate deep into the network infrastructure [1], [2] .

### 2.2 Wireless Network Rogue System

Wireless rogue systems are very similar to wired systems installed at the edge of a network. However, an advantage of wireless attacks, from the attacker's perspective, is that a wireless rogue system may be even easier to establish as physical access to the network hardware is not required. As shown in Figure 1, the attacker must only be within reach of the wireless

Signal in order to attempt an attack. Similar to wired spoofing, a wireless rogue device can spoof certain settings which enable the ability to connect to the wireless network. In addition, however, many wireless networks require an encryption key or some other type of authentication mechanism in order to gain access to the network. If the encryption key can be discovered or if the network does not require such authentication then the rogue system can associate with the network. Without connecting to an existing wireless network other wireless attacks are still possible. Mimicking an authorized network may trick users into associating with a malicious wireless network rather than the intended one. Passively monitoring the wireless medium is another attack which may result in the malicious device discovering sensitive information.

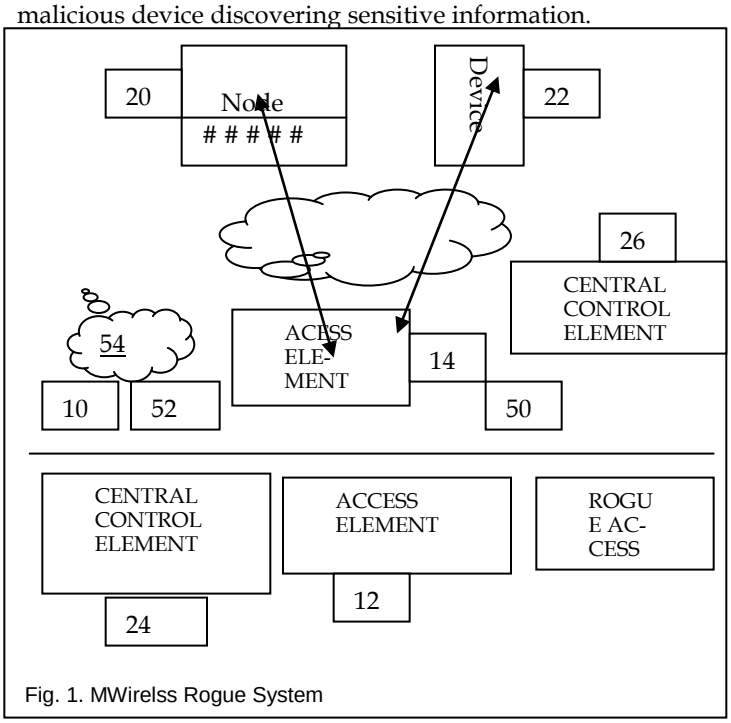


Fig. 1. MWirelss Rogue System

## 3 PROPOSED TECHNIQUES AND ALGORITHM

Our Research area work on the Rogue Identifying Packet Payload Slicer (RIPPS) system which is designed to quickly and accurately detect RWAPs using a novel technique which overcomes the limitations discussed previously. The system combines an active network traffic conditioning technique with a packet timing analysis to effectively detect when a new RWAP has been activated on the network. The wireless medium detection technique is based on a statistical analysis of the local round-trip time (LRTT) of network communication. The LRTT metric identifies invariant characteristics of wired and wireless media, enabling the identification of the connection type of a host. While the LRTT metric is based on purely passive network observation, it suffers due to the limited number of optimally sized packets available for analysis. Therefore, a packet payload slicing technique is implemented which performs network traffic conditioning to significantly enhance the effectiveness of LRTT measurements. This conditioning technique manipulates existing traffic and does not require modifications to client systems nor the ability to communicate directly with these systems. RIPPS operates as a pass-through device which works transparently to both clients and servers. It conditions traffic by taking individual large TCP packets and slicing them into many smaller packets. This action enables the LRTT metric to quickly exacerbate invariant physical characteristics of the wireless medium while negating influences of transmission speed capabilities. Through this process, RIPPS is able to quickly and efficiently identify unauthorized WAPs with minimal false alarms. Furthermore, RIPPS incorporates intelligent dynamic triggers to selectively monitor hosts, thus resulting in a minimal impact on the overall performance of monitored systems and the network in general.

### 3.1 Metric Descriptions

Latency of network based communication can be viewed as the result of either WAN-side or LAN-side effects. WAN-side latency is the result of many factors which can vary significantly between communication sessions and especially between differing communication host pairings. On the other hand, LAN-side latency, while not constant, is the result of a more controlled and consistent environment. Therefore, the metric is limited to the RTT associated only with LAN-side traffic in order to remove WAN-side jitter effects and emphasize the connectivity medium of hosts in the LAN. Local round-trip time is a measurement of the time delay between a message to and response from a specific host in the LAN. A sensor placed at the edge of the LAN collects data in a passive manner. The metric is obtained by categorizing packets based on source/destination pairing and storing both a timestamp as well as an expected acknowledgment (ACK) number based on the sequence number in the packet, as described in Algorithm 1. The timestamp associated with the messages is calculated solely by the sensor; hence the relative time between messages is consistent and free from time synchronization problems. Outbound packets are similarly classified by source/destination pairs and the ACK number from the TCP header is compared to the expected ACK numbers calculated previously, as described in Algorithm 2. The LRTT is the time difference between incoming packets and corresponding ACK packets as observed by the monitor.

Algorithm 1 Calculating Local RTT - Inbound Packet Processing
//
for each packet do
identify destination host host
  if monitoring host
    calculate expected ACK ACKEXP
    store time stamp and ACKEXP
  end if
forward packet to host
end for
Algorithm 2 Calculating Local RTT - Outbound Packet Processing
//

```
for each packet arrival do
identify source host host
   if monitoring host
      if ACK flag set
         match ACK = ACKEXP
         get stored time stamp TSold
         calculate LRTT = TSnew − TSold
      end if
   end if
forward packet to destination
end for
//
```

The LRTT is influenced by a variety of factors. First and foremost, the metric is influenced by the transmission medium between the monitoring system and host. The purpose of RIPPS is to isolate this influence in order to accurately identify the transmission type.

A second influence is the packet size of communication data. The variance in packet size results in varying LRTT values for a single host which may cause misleading results when comparing hosts to one another. This problem can be eliminated by calculating multiple LRTT values each based on packets of uniform size. LRRT values calculated with small packets are desirable in that small packets minimize the influence of bandwidth capabilities on packet timing metrics, while large packets maximize the previous effects.

## 4 Result

The overall performance of the system can be determined by measuring the packet loss on the server while varying the number of clients and the speed of the input data. The packet loss rate of the system with only a single client logging packets. The input speed is the average speed over the trace file replay. Peak bandwidth during the replay is approximately 50% higher than the average speed. A single client is able to avoid packet loss at approximately an average bandwidth speed of 85Mb/s. At higher rates the storage buffer of the server reaches maximum capacity and packets are lost. As the average bandwidth rate increases, Packet Loss Rate (%) the system reaches a threshold where the buffer loses all effectiveness and extreme packet loss occurs. This can be seen in each case where a dramatic increase in packet loss occurs. At an average data rate of approximately 375Mb/s the number of dropped packets for the five client system is non-zero, although somewhat negligible (0.6%).

## 4 CONCLUSION

The importance of computer security continues to grow as the reach of the Internet spreads and the dependence on networks for daily business increases. A system or network which has been compromised by a successful attack can result in an extremely high amount of lost time and money. Individuals and organizations must protect valuable information and resources by building defenses against attacks and establishing means of identifying currently active or already successful attacks. Many types of attacks can stem from the presence of a rogue system within a network. Rogue systems are devices which are unknown to system administrators and users, and are engaged in malicious behavior. This dissertation has presented new approaches to aid in the defense against rogue systems in order to protect individuals and organizations.

The future direction of this work includes applying these techniques to newly identified threats for the purpose of gauging the effectiveness of the proposed methods and to aid in discovering new means of defending against rogue system attacks. In addition, rogue threats in less traditional types of network environments, such as peer-to-peer and personal area networks, will be addressed in order to provide protection from all means of electronic rogue system attacks.

The weaknesses in communication standards will be investigated on a per-environment basis in order provide increased overall protection for users. Perhaps the most challenging future work will be in addressing detection techniques for current and newly discovered attack techniques

## References

[1] S. Bose and A.Kannan , "Detecting Denial of Service Attacks using Cross Layer based Intrusion Detection System in Wireless Ad Hoc Networks", IEEE 2008

[2] Matthew Smith, Michael Engel, Thoms Fries, Bernd Frielsen, "Security Issues in On-Demand Grid and Cluster Computing", IEEE2006

[3] Xuhua Wang, Shuhong Wang, Baihua Zheng, "Secure Real-time User Preference Collection for Broadcast Scheduling", IEEE2006

[4] Fei Wang, Yijun Mo, Student Member IEEE and Benxiond Huang, "Defending Reputation System against False Recommendation in Moible Ad Hoc Network". IEEE2008

[5] Darcy Hagedorn, Bruce Honda, Dick Peterson, "PROCESS CONTROL SECURITY JOURNEY", IEEE2007.

[6] Bharath Madhusudhan, John Lockwood, "Design of System for Real-Time Worm Detection", IEEE2004.

[7] Atual Adya, Paramvir Bahl, Ranveer Chandru and Lili Qiu, Architecture and techniques for diagnosing faults in IEEE802.11 infrastructure networks. IN Proceedings of ACM MobiCom, pages 30-44 septem 2004.

[8] IEEE Std 802.11: IEEE Standard for Wirelness LAN Medium Acess Control (MAC) and Physical Layer (PHY) Specification, June 1997.

[9] Broadcom radically simplies the wi-fi setup experience. Press Releasem Broadcom Corporation, May 2004.

[10] Giuseppe Ateniese, Michael Steiner, and Gene Tsudik, New multipart authentication services and key agreement protocols. IEEE Journal on Selected Areas in Communications, 18(4):628-639:2000.

[11] Steven M.Bellovin. Spamming, Phishing, Authentication, and Privacy communications of the ACM, 47(12):144, 2004.