Detection, Localization And Prevention Of Spoofing Attacks In Wireless Network

Arjunsingh Sushil Yadav, Deshana Manoj Sethia, Amruta Balaji Mundkar, Pooja Milind Natu
Pimpri Chinchwad College of Engineering, Pune, Maharashtra, India
Email: arjun.yadav015@gmail.com

Abstract — The performance of networks can be severely damaging by the use of wireless spoofing networks. Since they can be easily established, the attacker doesn’t find much hassles in destroying these networks. Although the identity of a node can be verified through cryptographic authentication, conventional security approaches are not always desirable because of their overhead requirements. We will use this spatial information, a physical property associated with each node, hard to falsify, and not reliant on cryptography, as the basis for 1) detecting spoofing attacks 2) determining the number of attackers when multiple adversaries masquerading as the same node identity 3) localizing multiple adversaries. 4) Preventing the attacks. We propose to use the spatial correlation of received signal strength (RSS) inherited from wireless nodes to detect the spoofing attacks. We then formulate the problem of determining the number of attackers as a multi-class detection problem. Cluster-based mechanisms are developed to determine the number of attackers.

In existing systems, the attacker is detected after it has attacked so in order to prevent the attack, we will consider what the attacker is requesting from the server. There will be an intermediate node between server and the attacker so as to prevent the traffic on server and based on the analyzed data from the intermediate node we will decide whether the requester is an attacker or a trusted user.

I. INTRODUCTION

The problem of determining the number of attackers as a multi-class detection problem. Cluster-based mechanisms are developed to determine the number of attackers. Wireless spoofing attacks are easy to launch and can significantly impact the performance of networks. Although the identity of a node can be verified through cryptographic authentication, conventional security approaches are not always desirable because of their overhead requirements. Due to the limitations of most MANET routing protocols, nodes in MANETs assume that other nodes always cooperate with each other to relay data. This assumption leaves the attackers with the opportunities to achieve significant impact on the network with just one or two compromised nodes.

II. LITERATURE SURVEY

A. Detection and Localization of Multiple Spoofing Attackers in Wireless Networks

Wireless spoofing attacks are easy to launch and can significantly impact the performance of networks. They propose to use the spatial correlation of received signal strength (RSS) inherited from wireless nodes to detect the spoofing attacks. They then formulate the problem of determining the number of attackers as a multiclass detection problem. When the training data are available, they explore using the Support Vector Machines (SVM) method to further improve the accuracy of determining the number of attackers. In addition, they developed an integrated detection and localization system that can localize the positions of multiple attackers. They evaluated their techniques through two test beds using both an 802.11 (Wi-Fi) network and an 802.15.4 (ZigBee) network in two real office buildings. The experimental results show that the proposed methods can achieve over 90 percent Hit Rate and Precision when determining the number of attackers. The localization results using a representative set of algorithms provide strong evidence of high accuracy of localizing multiple adversaries. [1].

B. Detecting Spoofing Attacks in Mobile Wireless Environments

The flexibility and openness of wireless networks enables an adversary to masquerade as other devices easily. Identity-based spoofing attacks are serious network threats as they can facilitate a variety of advanced attacks to determine the normal operation of networks. However, the existing mechanisms can only detect spoofing attacks when the victim node and the spoofing node are static. There is a proposal of a method for detecting spoofing attacks in the mobile wireless environment that is when wireless devices, such as the victim node and/or the spoofing node are moving. The DEMOTE system, which exploits Received Signal Strength (RSS) traces collected over

ISSN (Online): 2347-2820, Volume -2, Issue-8.9  2014
time and achieves an optimal threshold to partition the
RSS traces into classes for attack detection. Further, the
novel algorithm alignment prediction (ALP), when
without the knowledge of spatial constraint of the
wireless nodes, utilizes temporal constraints to predict
the best RSS alignment of partitioned RSS classes for
RSS trace reconstruction over time. Through
experiments from an office building environment, the
mentioned paper shows that DEMOTE achieves accurate
attack detection both in signal space as well as in
physical space using localization and is generic across
different technologies including IEEE 802.11 b/g and
IEEE 802.15.4.[2].

C. Detecting and Localizing Wireless spoofing Attacks

Wireless networks are vulnerable to spoofing attacks,
which allows for many other forms of attacks on the
networks. Although the identity of a node can be
verified through cryptographic authentication,
authentication is not always possible because it requires
key management and additional infrastructural
overhead. They have proposed that there is method for
both detecting spoofing attacks, as well as locating the
positions of adversaries performing the attacks. Next,
they described how they integrated their attack detector
into a real-time indoor localization system, which is also
capable of localizing the positions of the attackers. It
then shows that the positions of the attackers can be
localized using either area-based or point-based
localization algorithms with the same relative errors as
in the normal case. They have evaluated their methods
through experimentation using both an 802.11 (Wi-Fi)
network as well as an 802.15.4 (ZigBee) network. The
results show that it is possible to detect wireless
spoofing with both a high detection rate and a low false
positive rate, thereby providing strong evidence of the
effectiveness of the K-means spoofing detector as well
as the attack localizer. [3]

D. Detecting Identity-Based Attacks in Wireless
Networks Using Signal prints

Wireless networks are vulnerable to many identity-based
attacks in which a malicious device uses forged MAC
addresses to masquerade as a septic client or to create
multiple illegitimate identities. For example, several
link-layer services in IEEE 802.11 networks have been
shown to be vulnerable to such attacks. They have
shown that a transmitting device can be robustly
indented by its signal print, a topple of signal strength
values reported by access points acting as sensors. They
show that, different from MAC addresses or other
packet contents, attackers do not have as much control
regarding the signal prints they produce. Moreover,
using measurements in a tested network, they
demonstrated that signal prints are strongly correlated
with the physical location of clients, with similar values
found mostly in close proximity. By tagging suspicious
packets with their corresponding signal prints, the
network is able to robustly identify each transmitter
independently of packet contents, allowing detection of
large class of identity-based attacks with high
probability. [4]

E. Secure and Efficient Key Management in Mobile Ad
Hoc Networks.

In mobile ad hoc networks, due to unreliable wireless
media, host mobility and lack of infrastructure, providing
secure communications is a big challenge. Usually,
cryptographic techniques are used for secure
communications in wired and wireless networks.
Symmetric and asymmetric cryptography have their
advantages and disadvantages. In fact, any
cryptographic means is ineffective if its key
management is weak. Key management is also a central
aspect for security in mobile ad hoc networks. In mobile
ad hoc networks, the computational load and complexity
for key management are strongly subject to restriction
by the nodes available resources and the dynamic nature
of network topology. They proposed that a secure and
efficient key management (SEKM) framework for
mobile ad hoc networks. SEKM builds a public key
infrastructure (PKI) by applying a secret sharing scheme
and using an underlying multi-cast server groups. [5]

F. Access Points Vulnerabilities to Dos Attacks in
802.11 Networks.

There are various possible denial of service attacks to
infrastructure wireless 802.11 networks. To carry out
such attacks only commodity hardware and software
components are required. The results mentioned in this
paper show that serious vulnerabilities exist in different
access points and that a single malicious station can
easily hinder any legitimate communication within a
basic service set. [6]

III. SOFTWARE REQUIREMENTS
SPECIFICATION

A. Introduction

Wireless spoofing attacks are easy to launch and can
significantly impact the performance of networks.
Although the identity of a node can be verified through
cryptographic authentication, conventional security
approaches are not always desirable

because of their overhead requirements. In this paper,
we propose to use spatial information, a physical
property associated with each node, hard to falsify, and
not reliant on cryptography, as the basis for 1) detecting
spoofing attacks; 2) determining the number of attackers
when multiple adversaries masquerading as the same
node identity; and 3) localizing multiple adversaries.
4) Preventing the attacks. We propose to use the spatial
correlation of received signal strength (RSS) inherited
from wireless nodes to detect the spoofing attacks. We
then formulate the problem of determining the number of attackers as a multiclass detection problem. Cluster-based mechanisms are developed to determine the number of attackers. Our localization results using a representative set of algorithms provide strong evidence of high accuracy of localizing multiple adversaries.

In general, MANETs are vulnerable based on the basic characteristics such as open medium, changing topology, absence of infrastructure, restricted power supply, and scalability. In such case, Intrusion detection can be defined as a process of monitoring activities in a system which can be a computer or a network. The mechanism that performs this task is called an Intrusion Detection System. In addition to that, in case of wireless and sensor networks, they will increasingly become tempting targets for malicious attacks. Due to the openness of wireless and sensor networks, they are especially vulnerable to spoofing attacks where an attacker forges its identity to masquerade as another device, or even creates multiple illegitimate identities. Spoofing attacks are a serious threat as they represent a form of identity compromise and can facilitate a variety of traffic injection attacks, such as evil twin access point attacks. It is thus desirable to detect the presence of spoofing and eliminate them from the network. The traditional approach to address spoofing attacks is to apply cryptographic authentication. However, authentication requires additional infrastructural overhead and computational power associated with distributing, and maintaining cryptographic keys. Due to the limited resources available to the wireless devices and sensor nodes, it is not always possible to deploy authentication. In addition, key management often incurs significant human management costs on the network.

There are different approach by using the physical properties associated with wireless transmissions to detect spoofing. Specifically, we propose a scheme for both detecting spoofing attacks, as well as localizing the positions of the adversaries performing the attacks. Our approach utilizes the Received Signal Strength (RSS) measured across a set of access points to perform spoofing detection and localization. Our scheme does not add any overhead to the wireless devices and sensor nodes. By analyzing the RSS from each MAC address; we have found that the distance between the centroids in signal space is a good test statistic for effective attack detection. We then describe how we integrated our K-means spoofing detector into real-time indoor localization system. Our K-means approach is general in that it can be applied to almost all RSS-based localization algorithms.

1: Project Scope

This project can be used to detect various attacks occurred across the MANET or wireless network using RSS mechanism we can judge our attack detection and localization with high efficiency rather than Cryptographic mechanism.

2: User Classes and Characteristics

Users in Application are:

Network Admin: Root user for the entire infrastructure.

Scope: Access to all cloud instances within the service provider domain, access to all tenants.

End user: Regular user without any administration privileges can use resources, see utilization reports, but cannot select reports outside privilege scope.

Scope: Very limited scope down to the virtual machine level access.

Intermediate Node: Acts like a filter, segregating the necessary requests to avoid congestion from the repeated data.

Scope: Prevent DR attack.

3: Operating Environment

This product is web-based and will be hosted by a web server. It can be viewed by any web browsers and will be compliant with Internet Explorer, Mozilla, Netscape Navigator and Opera. It will work on Microsoft Environment only supported by .net framework and Java.

4: Design and Implementation Constraints

It is limited to work on Microsoft Windows Environment only. System must have .Net framework or Java.

System requires SQL Server or Higher installed on the server system which is very vital to maintain integrity of database.

5: Assumptions and dependencies

The users must be aware of computer hardware and their different attributes.

The user must have basic knowledge of computer and operating system.

Application development requires a good knowledge of operating systems and WMI architecture of windows.

For application, the users should be aware of JAVA language and basic database operations.

The computer in which this application is to be installed should be compatible with Eclipse (IDE) Framework.
B. Functional Requirements:

1: User Interfaces
The user can use the system through software installed in all the systems in organization premises. This software can run on any machine that supports Java Virtual Environment or a Dot Net Framework.

2: Hardware Interfaces
- RAM: 512 MB - 1 GB
- HDD: 40 GB
- Processor: Pentium IV
- Keyboard: Standard Windows Keyboard
- Mouse: Two or Three Button Mouse
- Monitor: LCD/LED

3: Software Interfaces
- Operating System: Windows XP Service Pack 2 or Higher
- Coding Language: JAVA
- Database: SQL Server 2005/2008 R2
- Tool: Eclipse JUNO

C. Non-Functional Requirements

1: Performance Requirements
- Time/Space Bounds:
  - Response time, throughput and available storage space should be reasonable under normal operational circumstances.

- Reliability:
  - Integrity of information maintained and supplied to the system and availability of components.

- Capacity:
  - Workloads should be handled for example the system must handle 1000 transactions per second.

2: Safety Requirements
- Power Failure:
  - In case of power failure system resume for current operation is there by maintaining a log file and backup of the data is provided in encrypted form.

- Data Loss:
  - If any file is accessed mentioned in the database but deleted from the system then it is removed from the database and appropriate message is displayed.

- Survivability:
  - System will need to survive fire, natural catastrophes etc.

3: Security Requirements
- Access Rights:
  - Different levels of access rights are given to different user by authenticating with pass-words.

- Encryption/Decryption:
  - Data is encrypted as soon as it is given for storage. Encryption and decryption is provided by different service providers so as to minimize the risk of data leakage.

4: Software Quality Attributes
- Availability:
  - The system shall be available as long as operations are performed on application.

- Updateability:
  - The system shall allow addition and deletion of files based on access rights provided.

- Reliability:
  - Integrity of information maintained and supplied to the system and availability of components.

- Testability:
  - New modules designed to be added to system must be tested to check whether they are integrated properly and compatible with input-output format of the system.

- Usability:
  - The system does not need much learning. Knowledge of basic computer its hardware and C# language is necessary to operate the system. Documentation provided for the system will include user manuals, developer reference and common FAQ.

D. Other Requirements

1: Database Requirements
- MS SQL Server 2008:
  - Microsoft SQL Server is a relational database management system developed by Microsoft. As a database, it is a software product whose primary function is to store and retrieve data as requested by other software applications, be it those on the same computer or those running on another computer across a
network (including the Internet). There are at least a dozen different editions of Microsoft SQL Server aimed at different audiences and for different workloads (ranging from small applications that store and retrieve data on the same computer, to millions of users and computers that access huge amounts of data from the Internet at the same time).

SQL Server 2008 (formerly codenamed "Katmai") was released on August 6, 2008 and aims to make data management self-tuning, self-organizing, and self-maintaining with the development of SQL Server Always on technologies, to provide near-zero downtime. SQL Server 2008 also includes support for structured and semi-structured data, including digital media formats for pictures, audio, video and other multimedia data. In current versions, such multimedia data can be stored as BLOBs (binary large objects), but they are generic bit-streams. Intrinsic awareness of multimedia data will allow specialized functions to be performed on them. According to Paul Flessner, SQL Server 2008 can be a data storage backend for different varieties of data: XML, email, time/calendar, file, document, spatial, etc. as well as perform search, query, analysis, sharing, and synchronization across all data types. Other new data types include specialized date and time types and a spatial data type for location-dependent data. Better support for unstructured and semi-structured data is provided using the new FILESTREAM data type, which can be used to reference any file stored on the file system. Structured Data and metadata about the file is stored in SQL Server database, whereas the unstructured component is stored in the file system. Such files can be accessed both via Win32 file handling APIs as well as via SQL Server using T-SQL.

SQL Server includes better compression features, which also helps in improving scalability. It enhanced the indexing algorithms and introduced the notion of filtered indexes. It also includes Resource Governor that allows reserving resources for certain users or workflows. It also includes capabilities for transparent encryption of data (TDE) as well as compression of backups. SQL Server 2008 supports the Eclipse Framework and the reporting tools, replication, and data definition will be built around the Entity Data Model. The version of SQL Server Management Studio included with SQL Server 2008 supports IntelliSense for SQL queries against a SQL Server 2008 Database Engine. SQL Server 2008 also makes the databases available via Windows PowerShell providers and management functionality available as Cmdlets, so that the server and all the running instances can be managed from Windows PowerShell.

2. Internalization Requirements
Physical constraints (size and weight)  
Personal availability and skill level  
Accessibility for maintenance  
Environmental conditions

3. Legal Requirements
Applications Software development tools should be legally Approved.
Database storage should not violate government rules and regulations (Whatsapp banned in few countries).

E. Analysis Models
1: Data Flow Diagram

![Data Flow Diagram Level 0](image1)

![Data Flow Diagram Level 1](image2)

![Data Flow Diagram Level 2](image3)
2. State Chart Diagram:

![State Chart Diagram](image1)

Figure 4: State Chart Diagram

3. ER Diagram

![ER Diagram](image2)

Figure 5: ER Diagram

IV. SYSTEM DESIGN

F. UML Diagrams

1. Sequence Diagram

A sequence diagram in a UML is a kind of interaction diagram. It is a construct of a Message Chart. A sequence diagram shows object interactions arranged in time sequence. It depicts the objects and classes involved in the scenario and the sequence of messages exchanged between the objects needed to carry out the functionality of the scenario. Sequence diagrams typically are associated with use case realizations in the Logical View of the system under development. Sequence diagrams are sometimes called event diagrams, event scenarios, and timing diagrams. A sequence diagram shows, as parallel vertical lines (lifelines), different processes or objects that live simultaneously, and, as horizontal arrows, the messages exchanged between them, in the order in which they occur. Figure 5 represents the sequence diagram of the system.

![UML Sequence Diagram](image3)

Figure 6: Sequence Diagram 1

![UML Sequence Diagram](image4)

Figure 7: Sequence Diagram 2
2: Use Case Diagram

Use Case diagram shows the overall functionalities of the system. Use case diagrams overview the usage requirements for a system. They are useful for presentations to manage and/or project stakeholders, but for actual development you will find that use cases provide significantly more value because they describe "the meat" of the actual requirements. Use case diagrams are behavior diagrams used to describe a set of actions (use cases) that some system or systems (subject) should or can perform in collaboration with one or more external users of the system (actors).

![Use Case Diagram](image)

3: Class Diagram

In software engineering, a class diagram in the Unified Modeling Language (UML) is a type of static structure diagram that describes the structure of a system by showing the system’s classes, their attributes, operations (or methods) and the relationships among the classes. The class diagram is the main building block of object oriented modeling. It is used both for general conceptual modeling of the systematic of the application, and for detailed modeling translating the models into programming code. Class diagrams can also be used for data modeling. The classes in a class diagram represent both the main objects and or interactions in the application and the objects to be programmed. In the class diagram these classes are represented with boxes which contain three parts: The upper part holds the name of the class. The middle part contains the attributes of the class. The bottom part gives the methods or operations the class can take or undertake.

![Class Diagram](image)

4: Deployment Diagram

![Deployment Diagram](image)

5: Collaboration Diagram

![Collaboration Diagram](image)
II. TECHNICAL SPECIFICATION

A. Advantages

Low or no startup cost

Great flexibility in relationship to fast up and down scaling of resources needs.

Easier access to new version.

Other common outsourcing advantages like security for uptime, availability, contingency arrangements, reduced cost of investment in organization infrastructure

B. Disadvantages

As it is web based it is dependent on network traffic.

Vulnerability in relation to the solution being delivered and operated by suppliers.

C. Applications

Many web application, such as meta querying, data integration and comparison shopping, need the data from multiple web database. For these application to further utilize the data embedded in HTML pages, automatic data extraction is necessary. Only when the data are extracted and organized in a structured manner, such as tables, can they be compared and aggregated. Hence, accurate data extraction is vital for these application is vital for these applications to perform correctly.

ACKNOWLEDGEMENT

We express our sincere thanks to our Guide Prof. S. SAMBARE, for his constant encouragement and support throughout our project, especially for the useful suggestions given during the course of project and having laid down the foundation for the success of this work.

We would also like to thank our Project Coordinator Mrs. Reena Kharat, for her assistance, genuine support and guidance from early stages of the project. We would like to thank Prof. Dr. J. S Umale, Head of Computer Department for his unwavering support during the entire course of this project work. We are very grateful to our Principal Dr. A. M. Fulambarkar for providing us with an environment to complete our project successfully. We also thank all the staff members of our college and technicians for their help in making this project a success. We also thank all the web committees for enriching us with their immense knowledge. Finally, we take this opportunity to extend our deep appreciation to our family and friends, for all that they meant to us during the crucial times of the completion of our project.

REFERENCES

[1]. Jie Yang, Student Member, IEEE, Yingying (Jennifer) Chen, Senior Member, IEEE, Wade Trappe, Member, IEEE, and Jerry Cheng “Detection and Localization of Multiple Spoofing Attackers in Wireless Networks”, 2013

