International Journal of Innovative Research in Advanced Engineering (IJIRAE)
Volume 1, Issue 1 (March 2014)

WIRELESS DEVICE POSITIONING AND FINDING INTRUDER USING RSS

Franklin Alex Joseph
Asst. Professor/EEE
St. Joseph's college of engineering and technology, Tanjore.
afranklin.alex@gmail.com

Sharmila
Asst.Professor/EEE
St. Joseph's college of engineering and technology,
rsharmi2415@gmail.com

Abstract - Wireless security is the prevention of unauthorized access or damage to computers using wireless networks. The risks to users of wireless technology have increased as the service has become more popular. Wi-Fi can be less secure than wired connections (such as Ethernet) because an intruder does not need a physical connection. By any chance if the wireless device attacked by intruder it is hard to locate the device. Locating a wireless device in a Wi-Fi network by calculating the distance of each node and localize the wireless accurately. A common measure to deter unauthorized users involves hiding the access point's name by disabling the SSID broadcast. While effective against the casual user, it is ineffective as a security method because the SSID is broadcast in the clear in response to a client SSID query. Another method is to only allow computers with known MAC addresses to join the network. The robust location estimation assumes the reference location in the target environment, the proposed location system maps the input to the physical location using RSS algorithm. In SSID is the application software used to list the set of wireless device available in the surrounding and it used to create a gpx file. Converting gpx file in a table format for further distance estimation.

Keywords- Wi-Fi, mobile phone positioning, RSS (Received Signal Strength),SSID(Signal Strength Identifier), MAC (Media Access Control) .

I.INTRODUCTION

Wireless device positioning system proposes an attack-resistant that uses a robust location estimation model. Unlike the product model, the proposed algorithm assumes that reliable observations may be any RSS or RSS combinations that belongs to the complete set. In Wi-Fi network it captures more robust location information because it offers a tolerance of all possible attack conditions. And it includes conducted in an actual Wi-Fi network. Actual Wi-Fi RSS data was collected to build a location system and a linear attack model that simulated various attacks on RSS. It includes the module for Xml to RDMS file, Location bases RSS, Intrusion Detection and Analysis. Many wireless localization algorithms based on different physical characteristics including received signal strength (RSS), time of flight, and angle or directional of arrival. Of these characteristics, RSS is the most attractive because reading RSS is economical and compatible with existing wireless networks.

Since estimations of position are often required for vital location-based services, such as assessment of secret document, positioning systems are becoming tempting targets for attacks. An attacker could easily prevent RSS based location systems from working correctly by altering the propagation environment, modifying the RSS readings, manipulating the transmitted power, or broadcasting false messages. Unfortunately, traditional security methods such as authentication and encryption keys cannot isolate physical RSS-based attacks, making defense against such attacks difficult. For this reason, researchers have devoted considerable research to designing robust location systems that provide valid location information resistant to malicious attacks. Most existing IDS are optimized to detect attacks with high accuracy. However, they still have various disadvantages that have been outlined in a number of publications and a lot of work has been done to analyze IDS in Wi-Fi network. RSS is the most attractive because reading RSS is economical and compatible with existing wireless networks. The assignment of the alert to an existing component is not accepted in any case, only if the quality of the model increases or does not decrease too much. The personal network security access of the wireless device will not be recognized and it will not be open in wireless network infrastructure.

IDS was not containing the robust location identification so not efficient to get the cleaned data and normal data. Distance estimation value of the wireless device shown the approximate target destination. IDS optimize to detect attack in high accuracy in wireless network if only the quality rate of the device is in high range. In this proposed system, The Robust location estimation system propose a novel technique for proposed attack-resistant which is based on a dynamic, probabilistic model of the current attack situation. To evaluate the effectiveness of the proposed attack-resistant location by using RSS algorithm, this included experiments conducted in an actual. Wi-Fi network and here analyzed three different data sets and showed that xml file conversion, Filtering individual devices by MAC address, experimental analysis using graph. In all cases, the amount of data could be reduced substantially. Actual Wi-Fi RSS data was collected to build a location estimation system and a linear attack model that simulated various attacks on RSS.

Using RSS was present the robust location estimation so efficiently get the cleaned data and normal data. This location estimation system was present RSS algorithm so predict the malicious attack in wireless network. Map the device in the infrastructure accurately and used to find the intruded device by giving threshold value manually.

II. PROPOSED ALGORITHM

A. PROBLEM FORMULATION:

The wireless device senses N base stations (BSs), then RSS can be represented by a vector $\mathbf{X}$ with N elements as $\mathbf{X}=(x_1,x_2,\cdots,xN)$, where x_n is the RSS from the nth BS. An RSS-based location system regards $\mathbf{X}$ as an input and outputs the estimated location through a previously constructed RSS-location relationship. However, the presence of an attacker or unreliable BSs may make some x_n very unreliable and inaccurately estimate the position of the user. The problem in secure localization is how to accurately locate the user given $\mathbf{X}$, which contains both un attacked (reliable) and attacked (unreliable) measurements.

B.DISTANCE ESTIMATION:

The RSS value from the insider application and also the quality rate of individual wireless device are stored in a XML based log file with the identity of each device (SSID), MAC Address, speed, longitude point, latitude point, time and date of the device when it is logged. The XML log files are then converted into a RDBMS table for the user recognition. '*BETWEEN*' is the keyword used the get the value from the entity to display it in a table. If we want to get the value of SSID name from the log file means,

Stringname Contains("<SSID>") ssidname = Between(Stringname, "<SSID>", "</SSID>");

From these we can get the values from the log file and implement it into the table. To evaluate the distance of the available device in the wi-fi network, pick the RSS value and quality rate from the table for each device available in the slot. The appropriate distance can be evaluate

*rss * rss / quality * 1.92 / 2*

By the formulae given. The received signal strength give the radio signal frequency and the quality rate gives the performance of the wireless device and range of usage based on the device quality. After these estimation the distance can be calculated and displayed in *sq.ft*

III. EXPERIMENTAL SETUP AND RESULTS

A. XML TO RDBMS FILE.

The user can be entering into the Wi-Fi user will log on to the services/ then the user will use the services. The authorized user will be entered into the Wi-Fi services unauthorized user cannot be accessing the services. The services can be based on the device available currently. Then take the overall log files of the user enter into the Wi-Fi based services and clustered the user enter into the Wi-Fi services. These clustering processes of the user log files can be processing as the unit process. The input file in the form of xml files and the file can be clustered and the file in the form of RDMS format.

B. FILE LOCATION BASED ON RSS.

In this pattern extraction the direction of the path can be identified and accessing the data in the online services in the WI-FI and identified in the cleaned training data. In this path direction the particular services can be provided and the particular data can be passed by the way of the online based services and it can be auditing the entire clean data and identify the pattern of the path and also identify any other possible attacks can be identified and getting the location information in this particular model based on RSS.

C. INTRUSION DETECTION

The localization information of the path in the model and getting information in the clean dataset and also identify the possible alert in the online services can be identified and other alert based on the attack can be identified by the possible attacks by using alert services. In this alert based services the different types of alert based on the online services of the data sending path in the services. Comparing the different messages and it can be stored in the buffer. Then the possible location information can be identified by this model and also the possible attacks in the Wi-Fi based online services and increasing the performance of the received signal of the sending data and the possible attacks can be reduced in the online services and sending the secured data without any major attack in the services.

In that particular time thousands of attacks can be spread it can be reduced by inclusive disjunction model and increased the performance of the online services in the WI-FI. e.g. DDOS Attack in the online services.

D. PERFORMANCE ANALYSIS

In this the localization information can be identified by the cleaned dataset and identify the path then the possible attacks can be reduced in the WI-FI based n online services and finding the path which can be in the secured online services based on WI-FI.in this overall attack can be identified in the cleared dataset and optimized location can be identified without any external attack in the online services. Compared to the other network services the performance can be increased in the online services compatible and increased the computation performance with online services. Now the performance of the computation time can be less compared to all other networking services and increased the received signal strength.

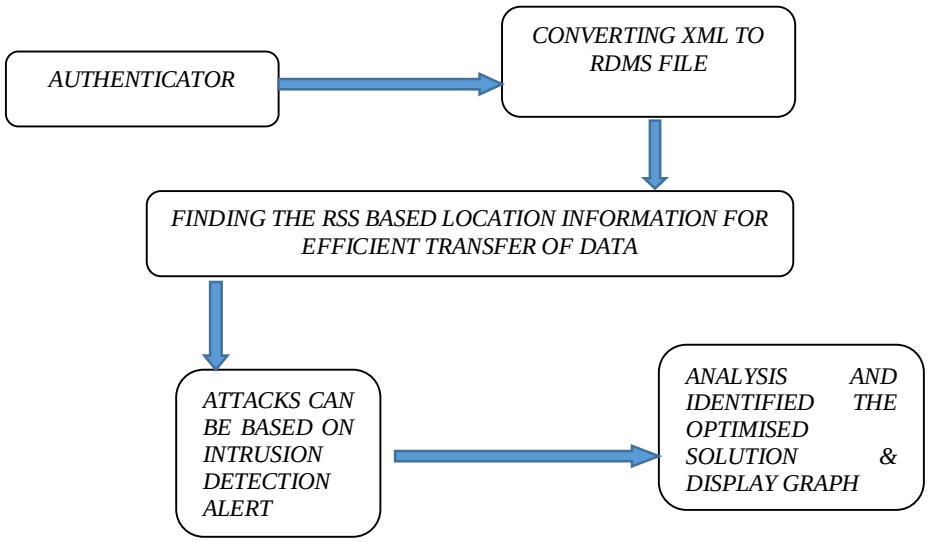

Fig. 1. System architectural diagram for wireless device positioning in Wi-Fi network.

IV. CONCLUSION:

Wireless positioning in Wi-Fi network system proposes an attack-resistant robust location estimation that uses a probabilistic inclusive disjunction model. The advantage of this approach is that, as a small probability contributes little to the inclusive disjunction model, this model allows an attacked observation to play a less significant role in the localization process, thus achieving more robust location estimations under security threats. To evaluate the effectiveness of this attack-resistant location estimation analyzed actual Wi-Fi RSS data, developed a robust location system, and simulated various attacks on RSS using a linear attack model. Finally the wireless positioning approach achieved better robustness than cluster based, distance based, and device based under various attacks on RSS.

V. FUTURE ENHANCEMENT:

In future the robust location of a wireless device in a wireless network can be reach the distance in a high range. By increasing the range of Wi-Fi, And to localize any device which is in too far of distance. A wireless access point (AP) is a device that allows wireless devices to connect to a wired network using Wi-Fi, or related standards. The AP usually connects to a router (via a wired network) if it's a standalone device, or is part of a router itself. In future this robust location estimation is applied in a sense means then the localization of the intruded device in a wireless network can be positioned easily. Most jurisdictions have only a limited number of frequencies legally available for use by wireless networks. However, the limited number of frequencies becomes problematic in crowded downtown areas with tall buildings using multiple WAPs. In such an environment, there is an overcome need for signal overlap becomes an issue causing interference, which results in signal drop page and data errors. Quality rate of the wireless device can also be localized accurately.

REFERENCES

[1] J. Cleary et al., "High precision traffic measurement," IEEE Communication Mag., vol. 40, no. 3, pp. 167–173, Mar. 2002.
[2] P. Ferrari, A. Flammini, D. Marioli, and A. Taroni, "A new distributed instrument for real time Ethernet networks: Experimental tests and characterization," in Proc. ETFA2007, IEEE Int. Conf. Emerging Technologies and Factory Automation, Patras, Greece, 2007, pp. 524–531.
[3] Gold smith A J, Wicker S B. Design Challenges for Energy Constrained Ad hoc Wireless Network [J]. IEEE Wireless Communications, 2002, 9(8):8 26
[4] DAI S J, JING X R, LI L N. Research and analysis on routing protocols for wireless sensor networks [A]. Communications, Circuits and Systems, 2005. Proceedings[C]. 2005 International Conference on Colume 1, 27-30 May 2005. Page(s):407 – 411
[5] S. Vitturi, "On the use of Ethernet at low level of factory communication systems," Comp. Std. and Interfaces, vol. 23, pp. 267- 277, 2001.
[6] OMRON Corporation, SYSMAC CS/CJ Series Ethernet Units Operational Manual. Kyoto, Japan: cat. no. W343-E1-06, 2005.
[7] L. Yong, M.J Lee, T.N. Saadawi. A Bluetooth scatternet-route structure for multi-hop adhoc networks. Selected Areas in Communications. IEEE Journal, Vol.21, pages 229-239, Issue: 2, Feb. 2003
[8] X. Zhang, G.F. Riley. Bluetooth Simulations for Wireless Sensor Networks using GTNetS. 12th IEEE/ACM International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS), Oct. 2004.
[9] J. Elson and D. Estrin. Time Synchronization for Wireless Sensor Networks. Int'l. Parallel and Distrib. Processing Symp., Wksp. Parallel and Distrib. Comp. Issues in Wireless Networks and Mobile Comp., San Francisco, CA, Apr. 2001.