Int. J. Communications, Network and System Sciences, **2012, 5, 81-85**
http://dx.doi.org/10.4236/ijcns.2012.52010 Published Online February 2012 (http://www.SciRP.org/journal/ijcns)

Role of Cross Layer Based Intrusion Detection System for Wireless Domain

Ravneet Kaur
Department of Computer Science & Engineering, Beant College of Engineering & Technology, Gurdaspur, India
Email: reet.kahlon@gmail.com

Received August 18, 2011; revised December 12, 2011; accepted January 18, 2012

ABSTRACT

Wireless mesh networks are very common both for organizations and individuals. Many laptops, computers have wireless cards pre-installed for buyer. However a wireless networking has many security issues. An intrusions detection system aim to detect the different attacks against network and system. An intrusion detection system should be capable for detecting the misuse of the network whether it will be by the authenticated user or by an attacker. They detect attempts and active misuse either by legitimate users of the information systems or by external. The present paper deals with cross layer based intrusion detection system for wireless domain—a critical anlaysis. The present paper deals with role of cross layer based intrusion detection system for wireless domain.

Keywords: Cross Layer Design; Intrusion Detection; Radio Frequency (RF)

1. Introduction

A Wireless Local Area Network (WLAN) is a flexible data communications system implemented as an extension to or as an alternative for, a wired LAN. Using radio frequency (RF) technology, wireless LANs transmit and receive data over the air, minimizing the need for wired connections. Wireless LANs frequently augment rather than replace wired LAN networks often providing the final few meters of connectivity between a wired network and the mobile user.

At its simplest form, wireless LAN technology, lets computers to communicate with the rest of a local area network via radio signals rather than over wires. There are two key components. First is the access point, or AP, which is the last wired stop on your network. Connected to the rest of the network via Ethernet cable, the AP translates the wired network traffic into radio signals and transmits it out. The signals are picked up by laptops or desktops with either removable or permanently embedded wireless-network interface cards. **Figure 1** shows architecture of wireless LAN and **Figure 2** shows functioning of wireless LAN.

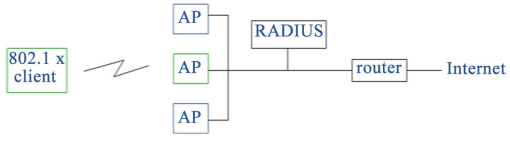

Figure 1. Architecture of wireless LAN.

1.1. Need of Wireless Network Security

The fundamentals of wireless security are largely similar to those of the wired Internet, wireless data networks present a more constrained communication environment compared to wired networks. Because of fundamental limitations of power, available spectrum and mobility, wireless data networks tend to have less bandwidth, more latency, less connection stability, and less predictable availability. Similarly, handheld wireless devices tend to have limited battery life, less powerful CPUs, restricted power consumption, smaller displays, and different input presenting a more constrained computing environment compared to desktop computers.

With a WLAN, transmitted data is broadcast over the air using radio waves. This means that any WLAN client within an access point (AP) service area can receive data transmitted to or from the access point. Because radio waves travel through ceilings, floors, and walls data may hence easily reach unintended recipients. Tools like Ethereal; AirSnort can easily be used to passively collect data of any Client within the broadcast range. Users have no way of knowing if they are connecting to rogue access point set-up as part of a man-in-the-middle attack.

WLAN security, involves concern in three separate issues:

- Authentication.
- User Privacy.
- Authorization.

Figure 3 shows the wireless security issues and **Figure 4**

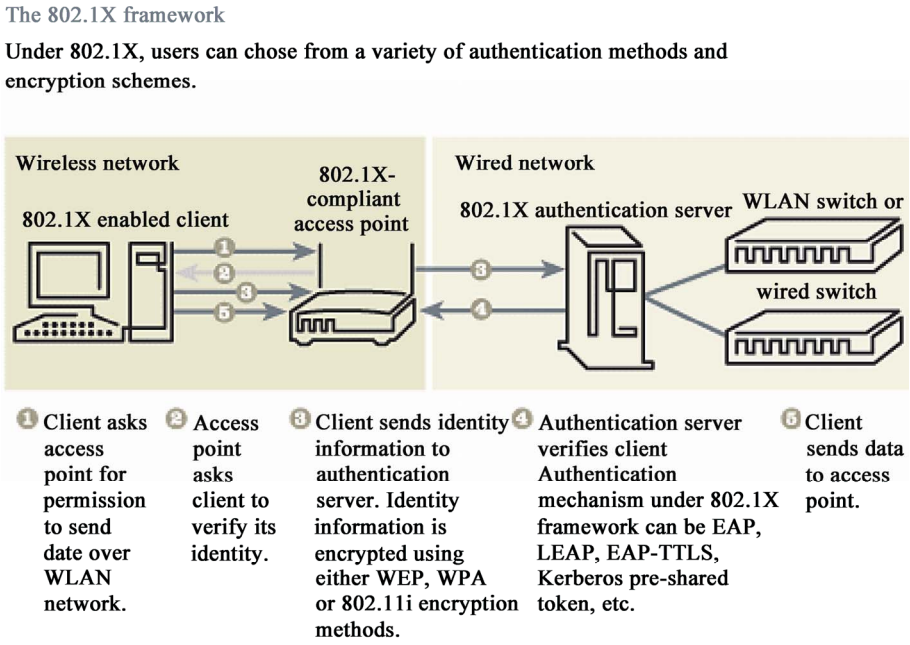

Figure 2. Functioning of wireless LAN.

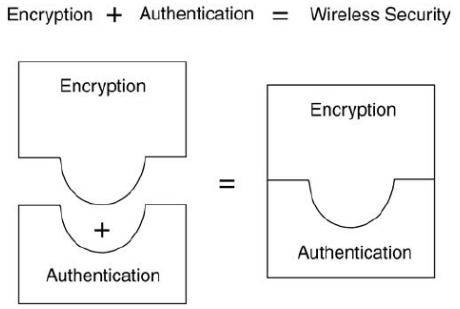

Figure 3. Wireless security issues.

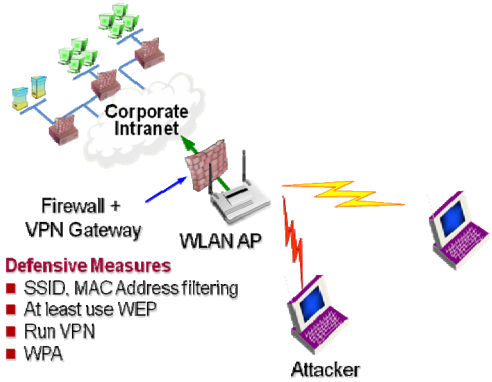

Figure 4. Need of network security.

shows the need of network security.

1.2. IEEE 802.11 Standards

The first wireless LAN standard, 802.11, was introduced by the IEEE less than a decade ago, in 1997. It utilizes the 2.4 GHz Industrial Scientific Medical (ISM) frequency band with Frequency Hoping Spread Spectrum (FHSS) or Direct Sequence Spread Spectrum (DSSS) modulation and is capable of delivering data rates of 1 Mbps and 2 Mbps. The 802.11 standard is now considered a legacy technology, mainly due to its very limited data rates, and is no longer deployed in new installations.

The 802.11b standard was approved in July 1999, roughly two years after the introduction of the initial 802.11 standard. Like its predecessor 802.11, 802.11b also operates in 2.4 GHz ISM band, which provides relatively good range and wall penetration capabilities in indoor environments.

The 802.11g standard was approved in June 2003. Just like 802.11b it also operates in the ISM band, utilizes the same OFDM modulation used in the 802.11a standard, and provides a maximum data rate of 54 Mbps. In addition, the standard is also fully backwards-compatible with existing 802.11b wireless networks. **Figure 5** shows the comparison b/w various wireless routers.

1.3. Wlan Security Standards

To provide security to the clients various security standards have been proposed by IEEE which are as follows:

1) IEEE 802.11/WEP (Wired Equivalent Privacy);

2) WPA (Wi-Fi Protected Access; based on draft 3 of IEEE 802.11i);

3) IEEE 802.11i/WPA 2;

4) 3GPPTS 33.234 (3G Security; Wireless Local Area Network Internetworking Security).

So the best way to protect your wireless network is to

Performance and Technology	802.11	802.11b	802.11a	802.11g
Max Data Rate	2 Mbps	11 Mbps	54 Mbps	54 Mbps
Max Throughput (Approx.)	1 Mbps	7 Mbps	25 Mbps	25 Mbps
Frequency	2.4 GHz	2.4 GHz	5 GHz	2.4 GHz
Compatibility	Interoperability with 802.11b (DSSS)	No interoperability	Interoperability with 802.11 (DSSS)/802.11g	Interoperability with 802.11b

Figure 5. Comparison b/w various wireless routers.

put on as many layers of protection as possible. Doing so may reduce the network's throughput but it's worth that price for better network security, especially if you have valuable data to protect. The more layers of protection you stack on, the more time, skill and effort the hacker need to penetrate your network, making it less and less attractive.

Intrusion detection can be of misuse detection and anomaly based detection. In misuse detection the decision by gathering the data of attacker and then compare it with large database of attack signature. It looks for specific attack that has been already documented. In anomaly detection the system administrator define the baseline or normal state of network like packet size, protocol, traffic load. Then it monitor by comparing network segment to normal behavior and look for anomalies [1-7]. In cross layer based intrusions detection the decision is based on the combine weight value of two or more layer. So the decision is not based on single layer, it will reduce false positive rate.

2. Intrusion Detection System

2.1. Types of Intrusion Detection Systems

There are two types of intrusion detection system First, Network Based Intrusion Detection system (NIDS) which resides on network. Second, Host Based Intrusion Detection system (HIDS) which resides on host *i.e.* computer system [8].

2.2. Network Based Intrusion Detection System (NIDS)

Network based intrusion detection system resides on network. It exists as software process on hardware system. It change the network interface card (NIC) into promiscuous mode, *i.e* the card passes all traffic on the network to the NIDS software. The software includes the rules which are used to analyze the traffic. It analyzes the incoming packets against these rules to determine the signature of the attacker. Whether this traffic signature is of any attacker or not. If it is of interest then events are generated.

The data source to NIDS is raw packets. It utilizes a network adapter which is running in promiscuous mode to monitor and analyze the network. There are four common techniques to identify attack.

1) Frequency or threshold crossing.
2) Correlation of lesser events.
3) Statistical anomaly detection.
4) Pattern, expression or byte code matching.

NIDS is not limited to read all the incoming packets only. But also learn the valuable information on outgoing traffic. With this feature the attacker form inside the monitored network are identified.

2.3. Host Based Intrusion Detection System (HIDS)

Host based IDS are embedded on host computer. It exists as a software process on a system. So it examines the log entries in system for specific information. It identifies the new entries and compares them to pre configured rules. It also works on rule based, if the entry match to the rule then it will generate alarm that this is not legal user.

2.4. Anomaly Based Detection

Anomaly detection attempts to model the normal behavior. Any occurring event which violates this model behavior is reflect to be suspicious. It aim is to detect the patterns that do not conform normal behavior. The pattern that does not conformed as normal are called as anomalies.

2.5. Misuse Based Detection

The equations are an exception to the prescribed specifications of this template. You will need to determine whether or not your equation should be typed using either the Times New Roman or the Symbol font (please no other font). To create multileveled equations, it may be necessary to treat the equation as a graphic and insert it into the text after paper is styled.

3. Cross Layer Based Technique

Cross layer based technique is used to make decision that whether there is an attacker or not by combining the result of two or more layer in TCP protocol [9,10].

3.1. Monitoring Received Signal Strength (RSS)

A measure of energy which is observed by the physical

layer at the antenna of the receiver is called as Received signal strength (RSS). In IEEE 802.11 networks, while performing MAC clear channel measurement and in roaming operations, the RSS indication value is used. The radio frequency (RF) signal strength can be measured through absolute (decibel mill watts-dBm), or relative (RSSI) manner [11-13].

Exact RSS value from sender to receiver is not easy to assume as mention above. To assume exact value of RSS the attacker has to be present on the same location which is not possible. The radio equipment used by the receiver have to be same for identify exact value of RSS. Moreover there should be same level of reflection, refraction, and interface. Even if the sender is fixed, RSS value seems to vary a little and it is proved that it is almost not possible to guess. This restricts the attacker from using the radio equipment to spoof the RSS clearly by the receiver.

A dynamic profile is build of the computer node which are communicating depend upon the RSS value from a server. Any sudden or unusual changes can be marked as doubtful activity which indicates the possible session of hijacking attack. Reason why we call RSS profile dynamic is because during every session it is build again and keep on updating. Any sudden changes in the RSS dynamic profile can be marked as doubtful activity with a higher confidence level because BSs are generally immobile. On the other hand, if the MS is mobile, then its respective RSS values will vary quickly which can be observed by the server. Therefore the uncertainty of the wireless medium can be used in the favor of intrusion detection, where the attacker is unable to know what RSS values to spoof. Therefore it is effective for the session hijacking attacks and it does not need any additional bandwidth consumption.

For example, based on the observed RSS values at the server it can develop a dynamic RSS profile for both MS2 and BS when a valid MS2 has an active session with a BS (Refer). If a attacker MS1 hijacks MS2 through isolating from the network and spoofing its MAC address then the server will pick up the abrupt changes in the RSS profile of MS2's MAC and gives an alert signal. Since they depend on the MS1's actual location, radio equipment and surrounding environment the RSS values for the MS2's MAC address will change.

In another situation, if the attacker MS1 spoofs the base station BS then it will also get detected as the dynamic RSS profile for the BS undergoes sudden variations. Therefore this mechanism gives detection for both session hijacking and man-in-the-middle attacks which is targeted at either MSs or BSs.

3.2. Monitoring Time Taken for RTS-CTS Handshake

Virtual carrier sensing is created using RTS-CTS which makes the transmission of data frames possible without collision. The successful delivery of the CTS frame from the receiver shows that the receiver is received the senders RTS frame successfully and ready for receiving the data. The time taken to complete the RTS-CTS handshake between itself and receiver *i.e.* TT can be examined by the sender. This is the total time taken for the RTS frame to travel from the sender to receiver and also for the CTS frame to send an acknowledgement. RTS-CTS handshake is free from collisions with any network node.

The TT values for a fixed transmission rate are not affected because the size of RTS and CTS frames are fixed and makes the TT between two nodes as an unspoofable parameter. So this cannot be easily guessed by an attacker when tracking the waves. Since it is calculated by the sender of the RTS-CTS handshake it is also protected from snooping. Since it is a measurement related to the entity measuring, the attacker should be exactly at the same location as the sender. Also the attacker should use the same radio equipment with the same attenuation and antenna gain. In order to predict the values of TT between the sender and receiver as measured by the sender, the attacker should receive the radio waves after the same number of reflections and refractions. It can also be calculated without any particular computational.

From the intrusion detection point of view, a mechanism which is used to detect the session hijacking attacks uses the quick and sudden changes in the TT between the two nodes. Server can measure the time elapsed between when it detects RTS frame from the sender to receiver and when it detects a return CTS from the receiver back to the sender *i.e.* TT. For understanding, this time can be represented as,

$$TT = TT_M - TT_{s\text{-}r} - TT_{m\text{-}s} \quad (1)$$

where,

$TT_{s\text{-}r}$—time taken for a RTS frame to cover the distance between the sender and the server;

$TT_{m\text{-}s}$—time taken for a RTS frame to cover the distance between the server and the receiver;

TT_M—time taken for a RTS-CTS handshake to complete between a sender and receiver as observed by the server.

But the server does not know these actual values.

Monitoring observed TT values at the server provides a reliable passive detection mechanism for session hijacking attacks since TT is an unspoofable parameter related to its measuring entity. Also this cannot be guessed because its exact value depends on

1) The position of the receiver and the server;

2) The distance between the server and receiver;

3) The environment around the receiver and the server.

This is a property which cannot be measured or spoofed by an attacker when tracking the network traffic or using

a specialized radio equipment.

We propose that changes in TT between two communicating nodes can be observed by a passive server and the sudden variations are marked as suspicious. This helps to detect the attacker who tries to take over a receiver's session by isolating it off the network and spoofing its MAC address. On the other hand, the RTS-CTS handshakes which originates from the receiver is used to detect the session hijacking attacks which aims the sender.

For example, the server can develop a dynamic RSS profile which gets constantly updated per session and it calculates the TT for every RTS-CTS handshake from both MS2 and BS when a valid MS2 has an active session with a BS (**Figure 2**). If an attacker MS1 hijacks MS2 through spoofing its MAC address then the server will observe abrupt changes in the TT for MS2 and gives an alert signal. Also to detect the man-in-the-middle attacks against BS, TT values from RTS-CTS handshakes between MS2 and BS which originates from MS2 can be registered by the server in the MS2's profile.

4. Conclusion

By developing a dynamic profile based upon the RSS value and keep on updating it. RSS value is difficult to assume because the attacker must use same equipment and same level of interface, refraction which is not possible. Cross layer based technique help to make decision based on two layer physical layer where we compute RSS value and on MAC layer where we compute RTS-CTS time taken. This will reduce the positive false rate.

5. Impact of Study

Wireless mesh networking has been a cost-effective technology that provides wide-coverage broadband wireless network services. They benefit both service providers with low cost in network deployment, and end users with ubiquitous access to the Internet from anywhere at anytime. However, as wireless mesh network (WMN) proliferates, security and privacy issues associated with this communication paradigm have become more and more evident and thus need to be addressed. In future cross layer based intrusion detection system in wireless domain such as WLAN will be attempted. The present study will be useful to provide a good foundation to implement real time detection.

6. Acknowledgements

The author is thankful to Dr. Jatinder Singh Bal (Dean and Professor, Computer Science & Engineering Desh Bhagat Enggineering College, Moga) for critical discussion as well as constant help during the present study. The constant encouragement provided by Dr. H. S. Johal as well as Mr. Dalwinder Singh and Deepak Prashar, Lovely Professional University Jalandhar is also acknowledged.

REFERENCES

[1] B. Mukherjee, L. T. Heberlein and K. N. Levitt, "Network Intrusion Dtetction," *Ieee Network*, May-June 1994, pp. 8-10.

[2] D. Dasgupta, *et al.* "Cougaar Based Intrusion Detection System (Cids)," Cs Technical Report, No. Cs-02-001, 4 February 2002.

[3] H. Debar, M. Dacier and A. Wespi, "Towards a Taxonomy of Intrusion-Detection Systems," Computer Networks, Vol. 31, No. 8, 1999, pp. 805-822. doi:10.1016/S1389-1286(98)00017-6

[4] D. Denning, "An Intrusion-Detection Model," *IEEE Transactions on Software Engineering*, Vol. 13, No. 2, 1987, pp. 222-232.

[5] G. Thamilarasu, A. Balasubramanian, S. Mishra and R. Sridhar, "A Cross-Layer Based Intrusion Detection Approach for Wireless Ad Hoc Networks," *IEEE International Conference on Mobile Adhoc and Sensor Systems*, Washington DC, 7 November 2005, p. 861. doi:10.1109/MAHSS.2005.1542882

[6] J. Hall, "Enhancing Intrusion Detection in Wireless Networks Using Radio Frequency Fingerprinting," *IEEE Transactions on Dependable And Secure Computing*, 12 July 2005, pp. 18-22.

[7] Y. Lim, T. Schmoyer, J. Levine and H. L. Owen. "Wireless Intrusion Detection and Response," *Proceedings of the* 2003 *IEEE Workshop on Information Assurance United States Military Academy*, West Point, New York, June 2003, pp. 22-26.

[8] Y. Zhang, and W. Lee, "Intrusion Detection in Wireless Ad-Hoc Networks," *Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking*, Boston, 6-11 August 2000, pp. 26-31.

[9] X. Wang, J. S. Wong, F. Stanley and S. Basu, "Cross-Layer Based Anomaly Detection in Wireless Mesh Networks," *Ninth Annual International Symposium on Applications and the Internet*, Bellevue, 20-24 July 2009, pp. 9-15.

[10] J. S. Bal, *et al.*, "A Cross Layer Based Intrusion Detection Technique for Wireless Network," *International Journal of Computer Science* & *Information Security*, Vol. 5, Paper No. 25080924, 2009.

[11] S. Rakesh, "A Novel Cross Layer Intrusion Detection System in MANET," 24*th Proceedings of IEEE International Conference on Advanced Information Networking and Applications*, Perth, 20-23 April 2010, pp. 38-48.

[12] S. Madhavi, "An Intrusion Detection System in Mobile Adhoc Networks," *International Journal of Security and Its Applications*, Vol. 2, No. 3, 2008, pp. 11-17.

[13] S. Khan. "Framework for Intrusion Detection in IEEE 802.11 Wireless Mesh Networks," *The International Arab Journal of Information Technology*, Vol. 7, No. 4, 2010, pp. 50-55.

