Advances in Internet of Things, 2011, 1, 51-54
doi:10.4236/ait.2011.13007 Published Online October 2011 (http://www.SciRP.org/journal/ait)

Advances in Intrusion Detection System for WLAN

Ravneet Kaur
Department of Computer Science and Engineering, Beant College of Engineering and Technology, Gurdaspur, India
E-mail: *reet.kahlon@gmail.com*
Received July 8, 2011; *revised July* 28, 2011; *accepted August* 21, 2011

Abstract

A wireless network is not as secure as compare the wired network because the data is transferred on air so any intruder can use hacking techniques to access that data. Indeed it is difficult to protect the data and provide the user a secure information system for lifetime. 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. Cross layer based technique help to make decision based on two layer physical layer where we compute RSS value and on MAC layer where one compute RTS-CTS time taken. This will reduce the positive false rate. They detect attempts and active misuse either by legitimate users of the information systems or by external. The paper has highlighted the advances in intrusion detection in wireless local area network.

Keywords: Reciever Signal Strength (RSS), Time Taken for RTS-CTS Handshake (TT), 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. 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 [1-10]. 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. Multi-hop wireless networks are more unsafe as compared to wired or single hop wireless networks. Multilayer security attacks need to be considerate before the design of any security mechanism or intrusion detection system [11-13].

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 [11].

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 changes 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 reflected 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 [12,13].

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 [8-10].

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 keeps 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 **Figure 1**). If an 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

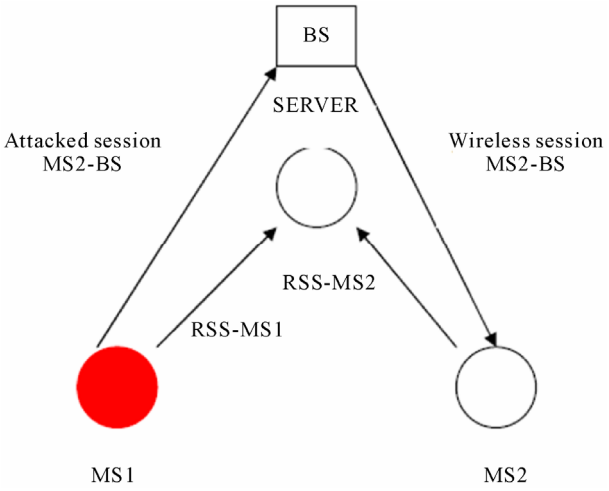

Figure 1. Received signal strength (RSS).

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,

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

where,

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

TT_{m-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 handshake which originates from the receiver is used to detect the session hijacking attacks which aims the senders. 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 (Refer **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

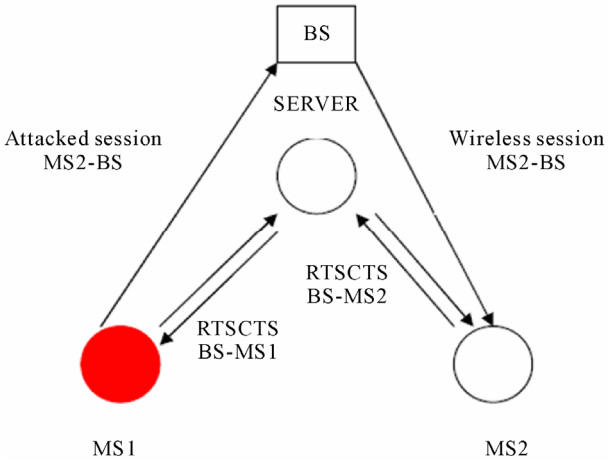

Figure 2. Round Trip Time (RTT).

and BS which originates from MS2 can be registered by the server in the MS2's profile. The server executes the following algorithm, to detect the attackers.

3.3. Detection Algorithm

Step 1: Server measures RSS
Step 2: Server measures TT
Step 3: Server calculates the weight W as

$$W = w1 \cdot \delta_{RSS} + w2 \cdot \delta_{TT} \quad (2)$$

where δ_{RSS} = Variation of RSS and
δ_{TT} = Variation of TT
$w1$ and $w2$ are two constants, which can be fine tuned .
Step 4: If $W > Dthr$, (where $Dthr$ is the detection threshold) Then MS is an attacker.

4. Conclusions

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. The cross layer design approach has impact on performance enhancement for intrusion detection system for WLAN [14,15].

5. 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.

6. References

[1] B. Mukherjee, L. T. Heberlein and K. N. Levitt, "Network Intrusion Detection," *IEEE Network*, Vol. 8, No. 3, 1994, pp. 8-10.doi:10.1109/65.283931

[2] D. Dasgupta, *et al*., "Cougar 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. Se-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," *Proceedings of IEEE International Conference on Mobile Adhoc and Sensor Systems Conference*, 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*, Vol. 3, No. 3, 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, 18-20 June 2003, pp. 22-26.

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

[9] 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.

[10] K. Shafiullah, "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.

[11] Y. Zhang and W. Lee, "Intrusion Detection in Wireless Ad-Hoc Network," *Proceedings of the* 6*th Annual International Conference on Mobile Computing and Networking*, Boston, 6-11 August 2000, pp. 26-31. doi:10.1145/345910.345958

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

[13] J. S. Bal, *et al*., "A Cross Layer Based Intrusion Detection Technique for Wireless Network," *International Journal of Computer Science and Information Security*, Vol. 5, September 2009, Article ID: 25080924.

[14] R. Kaur, "Study of Intrusion Detection Systems for Wireless Networks," *International Journal of Wireless Networks and Communication*, Vol. 13, 2011,In Press.

[15] R. Kaur, "Cross Layer Based Intrusion Detection System for Wireless Domain-Acritical Analysis," *International Journal of Computer Science and Communication*, Vol. 2, No. 2 (Accepted for publication), 2011.

