International Journal of Computer Engineering Research Vol. 2(5), pp. 75-81, November 2011
Available online at http://www.academicjournals.org/IJCER
ISSN 2141- 6494 ©2011 Academic Journals
DOI: 10.5897/IJCER11.038

Full Length Research Paper

Cross layer based miss detection ratio under variable rate for intrusion detection in WLAN

Ravneet Kaur

Department of Computer science and Engineering, Beant College of Engineering and Technology, Gurdaspur Punjab, India. E-mail: reet.kahlon@gmail.com.

Accepted 18 October, 2011

The emphasis for the use of wireless LAN in industry is on robustness, reliability and security. Almost any given single secruity mechanism (such as MAC filtering) alone may be easily overcome by attackers. However, proper configuration and implemetation of the maximum possible security mechanism must be used to form a multiple security layers, to provide the best possible wireless protection. The present paper deals with cross layer based miss detection ratio under variable rate for intrusion detection in WLAN. In cross layer based intrusions detection, the decision is based on the combine on weight value of two or more layer. So the decision is not based on single layer, it will reduce false positive rate. Two different layers, physical and MAC have been used in the present study and the results have been compared with existing technique.

Key words: Reciever signal strength (RSS), time taken for RTS-CTS handshake (TT), radio frequency (RF).

INTRODUCTION

Owing to developments made in the wireless technology in the recent years, wireless LAN is rapidly winning acceptance as an alternate solution for many applications in industrial environments. The high degree of flexibility it provides within the plant can lead to cost reduction during both installation and operation. Features such as fast roaming times, coverage, worldwide acceptance and proven security concepts have further increased the attractiveness of wireless solution in business and industry. 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 intrusion 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 (Mukherjee et al., 1994). The aim of intruder is to gain the access of the privileges. Generally, this show that intruder want information which is protected.

INTRUSION DETECTION SYSTEM

Inevitably, the best intrusion prevention system will fail. A system's second line of defense is intrusion detection, and this has been the focus of much research in recent years (Dasgupta, 2002; Debar et al., 1999; Denning, 1987; Thamilarasu et al., 2005; Jeyanthi, 2005; Lim et al., 2003)

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 that is computer system (Rakesh, 2010; Madhavi, 2008; Shafiullah, 2010; Zhang and Lee, 2000)

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, that is, 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 (Mukherjee et al., 1994; Dasgupta, 2002; Debar et al., 1999).

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.

(a) Frequency or threshold crossing.
(b) Correlation of lesser events.
(c) Statistical anomaly detection.
(d) 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.

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 a legal user.

Anomaly based detection

Anomaly detection attempts to model the normal behavior. Any occurring event which violates this model behavior is reflecting 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 anomalies (Wang et al., 2009; Bal, 2009).

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 your paper is styled.

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 (Wang et al., 2009; Bal, 2009).

Monitoring received signal strength (RSS)

A measure of energy which is observed by the physical layer at the antenna of the receiver is called 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.

Exact RSS value from sender to receiver is not easy to assume as mention previously. 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. 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 (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

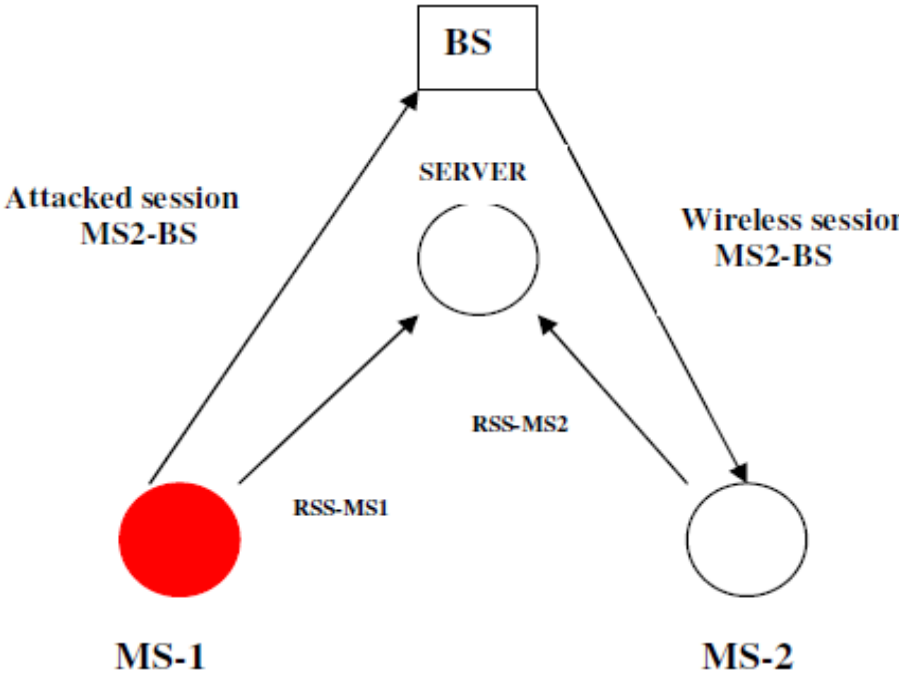

Figure 1. Received signal strength (RSS).

variations. Therefore, this mechanism gives detection for both session hijacking and man-in-the-middle attacks which is targeted at either MSs or BSs.

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 that is, 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 betoneen 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 betoneen 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 computation.

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 betoneen the two nodes. Server can measure the time elapsed betoneen when it detects RTS frame from the sender to receiver and when it detects a return CTS from the receiver back to the sender that is, TT. For understanding, this time can be represented as:

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

Where, TT_{s-r} is time taken for a RTS frame to cover the distance betoneen the sender and the server, TT_{m-s} - time taken for a RTS frame to cover the distance betoneen the server and the receiver, TT_M - time taken for a $RTS-CTS$ handshake to complete betoneen 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;

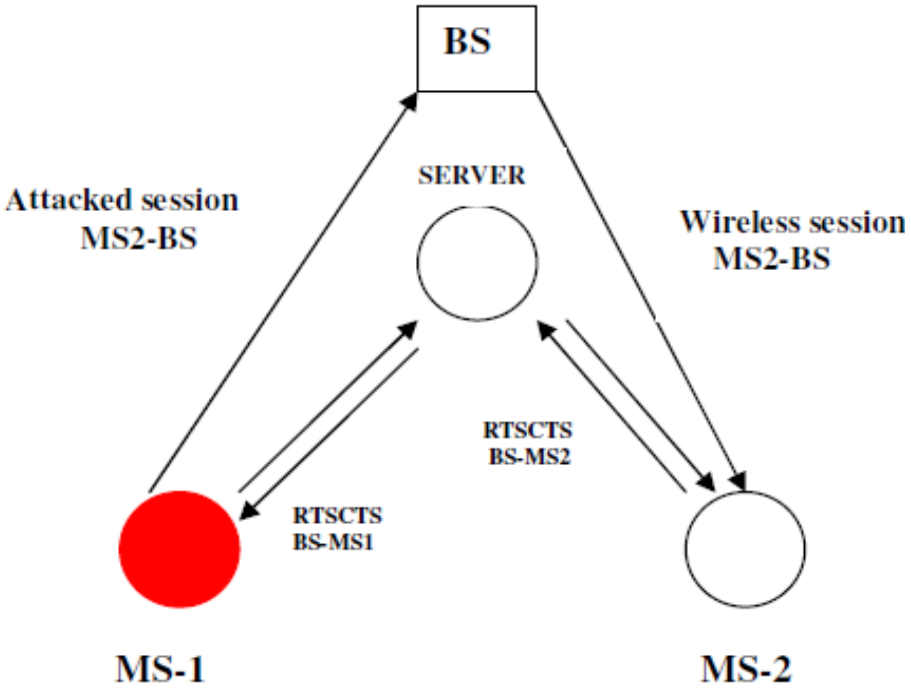

Figure 2. Round trip time (RTT).

1. The position of the receiver and the server
2. The distance betoneen 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. It has been proposed (Bal, 2009) that changes in TT betoneen 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 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 betoneen MS2 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.

Detection algorithm

Step 1: Server measures RSS
Step 2: Server measures TT
Step 3: Server calculates the on eight W as.,

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

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.

This technique has been successfully applied for intrusion detection in mobile adhoc network (Bal, 2009). The present study aims to determine the application of the technique proposed by Bal (2009) for WLAN system in order to study the effect of range on the performance asonell as compared to existing techniques.

EXPERIMENTAL ASPECT IN PRESENT STUDY

The following hardware/software platforms have been used to conduct the proposed study:

1. Hardware platform: INTEL CORE i5 n series processor.

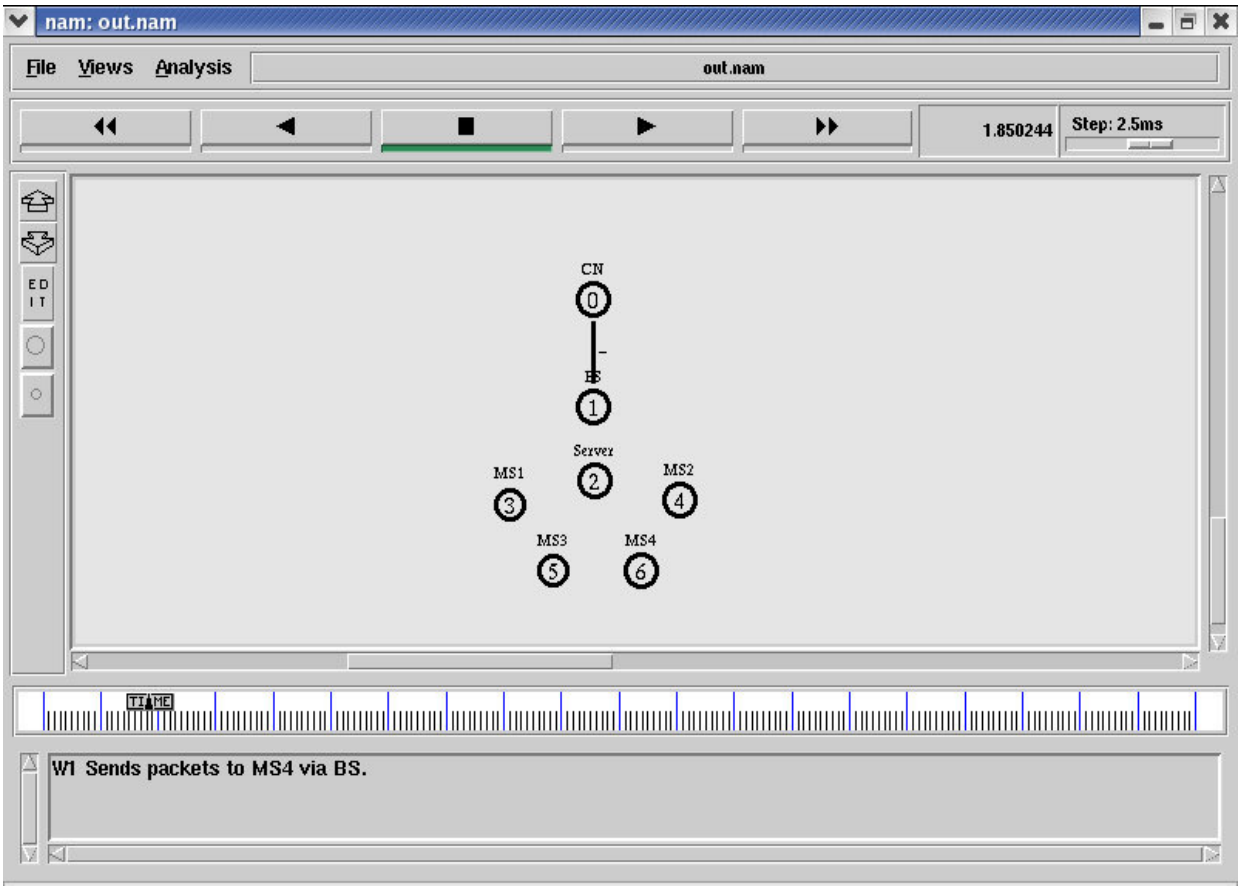

Figure 3. Simulation scenario.

2. Software platform: LINUX OS and Ns 2 simulator.

The number of wireless network devices will soon surpass the number of wired devices, and the amount of research in the area of wireless networking is increasing at a similar rate (Madhavi, 2008). Wireless research often involves a test bed implementation and/or a simulation study. Network simulators allow researchers to analyze the behavior of these wireless devices at every level. As a result, these simulations are capable of producing very large amounts of data. The simulation community has made available many types of scripts (e.g., tracegraph to parse and analyze this output data, but visualization of the data is needed to further aid understanding of the output. A good visualization package is important, because the human visual system is unrivaled in pattern recognition and offers the ability to process large amounts of data quickly and clearly (Debar et al., 1999). Visualization adds to the understanding gained via statistical analysis. As one show in this paper, certain erroneous network behaviors could go undetected without visualizations.

The Network simulator 2 (NS-2) is a popular and powerful simulation environment, and the number of NS-2 users has increased greatly in recent years. Although, it was originally designed for wired networks, NS-2 has been extended to work with wireless networks, including wireless LANs, mobile ad hoc networks, and sensor networks.

RESULTS AND DISCUSSION

In order to test the protocol, the NS2 simulator is used. The experimental consist of 1 wired node, 1 base station and 4 master stations with one server. One compares our proposed cross-layer based intrusion detection technique with the radio frequency fingerprinting (RFF) technique. Figure 3 shows the snapshot of experimental setup for the present study.

Effect of varying rate on miss detection ratio

In the first experiment, the attack traffic rate is varied as 50,100,150,200 and 250 kb. Figure 4 shows the misdetection ratio of our cross-layer technique and RFF. From the figure, one can see that the misdetection ratio is

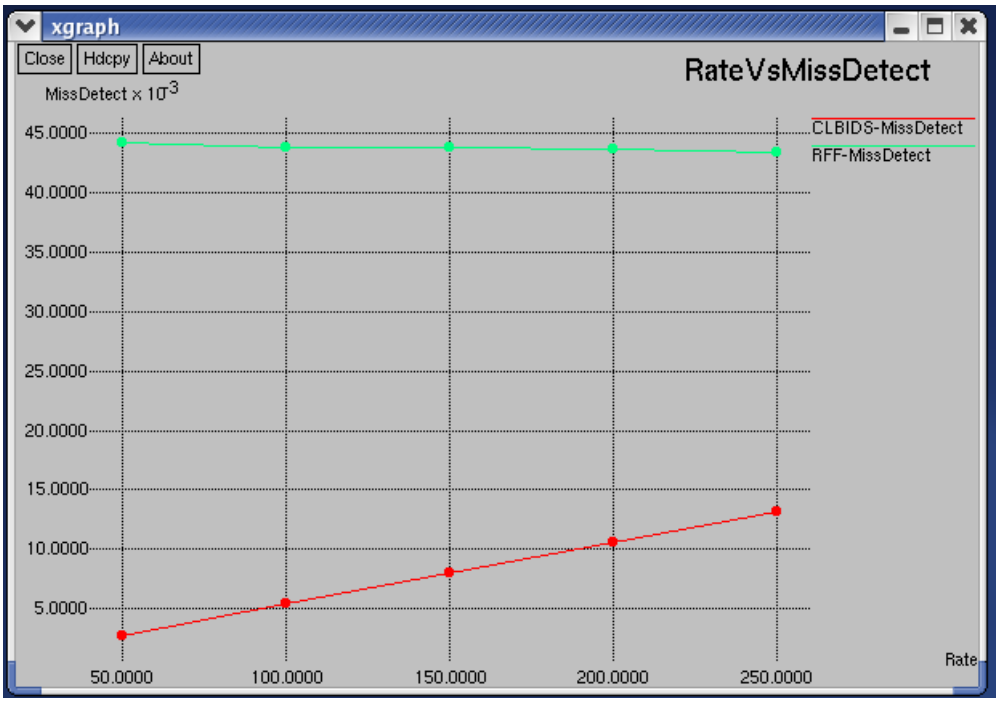

Figure 4. Rate Vs miss detection ratio.

significantly less in the cross-layer scheme when compared with RFF scheme, since it accurately detects the intrusion.

The purposed technique is based on cross layer, where two layers have been used that is, physical layer and MAC layer. On physical layer, one computes the RSS value, which is evaluated by the receiver at destination node. RSS value is computed by the omnidirectional antenna at receiver node. Second on MAC layer RTS/CTS handshake time is computed. RTS/CTS is used to avoid collision on network. The combine result value is submitted to the server, which becomes the threshold value Dthr and when a new session is made the server will compare the current RSS and RTS/CTS time taken with the previous value Dth. If that value is less than previous value then it is an attacker. RSS value depends upon the type of antenna being used as well as the reflection, refraction and interference. If an attacker want to pretend as the authenticated user by accessing its MAC address, but using this technique the attacker is unable to identify the RSS value because he may not be using same antenna and even there is not same reflection, refraction and interference. So he is unable to know the exact value.

RTS/CTS fame makes the transmission of packets without collision. RTS/CTS time taken is computed by the sender. A successful delivery of CTS frame from receiver to sender shows that RTS frame is delivered to the receiver. RTS/CTS frame has a fixed transmission rate. This makes TT parameter unspoofable, so the attacker is unable to detect TT parameter. As describe in previous cases, it is difficult for an attacker to access the session, because only with MAC address he cannot access the session, the server is computing RSS and RTS/CTS time taken (which is not exactly as the authenticated user). This shows that this technique will reduce the chance of intrusion. Moreover, due to combine result of two layers the false positive rate is also reduced.

Conclusion

In the scenario, there are 1 wired node, 1 base station and 4 master stations (1 as server). The transmission range is set from 100 to 400 m. The antenna used here is omnidirectional, with two way propagation. There are two domains with one cluster in each, 1 node in first cluster and 6 in the second cluster. When the simulation starts the RSS value and RTS/CTS handshake time is captured. The threshold value is taken by the packet size plus the channel idle time. Then the procedure to check the attacker is started where one gets the delta RSS, TT values by subtracting it from current values form the previous values. Both of these values are evaluated by multiplying two of the eight parameters of W1 and W2. Then the combine result of these is checked against the Dth (threshold value). If it is less than the Dth value then that person is an attacker.

Purposed technique is compared with the figure printing technique and the simulation result shows that

the cross layer based intrusion detection system (CLBIDS) technique is better technique than the RFF technique. It is concluded that the misdetection ratio is significantly less in the cross-layer scheme when compared with RFF scheme, since it accurately detects the intrusion.

Future work

The effect of other dominant performance enhancing parameters will be incorporated in future for efficient intrusion detection system in the wireless domain. The future scope of this technique is one can implement this technique in many wireless hardware devices. It can be implemented in network where the decision is made whether to accept that attacker data for a destination node by computing RSS and TT values.

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 any time. However, as wireless mesh network (WMN) proliferate security and privacy issues associated with this communication paradigm have become more and more evident and thus need to be addressed. The present study will be useful to provide a good foundation to implement real time detection.

ACKNOWLEDGEMENTS

The author is thankful to Dr. Jatinder Singh Bal (Dean and Professor, Computer Science and 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

Bal JS (2009). A cross layer based intrusion detection technique for wireless network. Int. J. Comput. Sci. Inf. Secur., p. 5.

Dasgupta D (2002). Cougaar Based Intrusion Detection System (Cids). Cs Technical Report No. Cs- 02- 001.

Debar H, Dacier M, Onespi A (1999). Towards A Taxonomy of Intrusion-Detection Systems. Computer Networks, pp. 805-822.

Denning D (1987). An Intrusion-Detection Model. IEEE Trans. Softw. Eng., 13(2): 222-232.

Jeyanthi H (2005). Enhancing Intrusion Detection in Wireless Networks Using Radio Frequency Fingerprinting. IEEE Trans. Dependable Secure Computi., pp. 18-22.

Lee WY (2000). Intrusion Detection in Wireless Ad-Hoc Networks. Proc. of the Sixth Annual International Conference on Mobile Computing And Networking, Boston: Massachussetts, pp. 26-31.

Lim Y, Schmoyer T, Levine J, Oonen HL (2003). Wireless Intrusion Detection and Response. Proc of IEEE Workshop On Information Assurance United States Military Academy, pp. 22-26.

Madhavi S (2008). An Intrusion Detection System In Mobile Adhoc Networks**.** Int. J. Secur. Appl., 2(3): 11-17.

Mukherjee B, Heberlein LT, Levitt KN (1994). Network Intrusion Dtetction. Ieee Network, pp. 8-10.

Rakesh S (2010). A Novel Cross Layer Intrusion Detection System in MANET. Proc. IEEE International Conference on Advanced Information Networking and Applications, pp. 38-48.

Shafiullah K (2010). Framework for Intrusion Detection in IEEE 802.11 Wireless Mesh Networks. Int. Arab J. Inf. Technol., 7(4): 50-55.

Thamilarasu G, Balasubramanian A, Mishra S, Sridhar R (2005). A Cross-Layer Based Intrusion Detection Approach For Wireless Ad Hoc Networks. Proc. IEEE International Conference on Mobile Adhoc and Sensor Systems Conference, p. 861.

Wang X, Wong JS, Stanley F, Basu S (2009). Cross-layer Based Anomaly Detection in Wireless Mesh Networks. Ninth Annual International Symposium on Applications and the Internet.