Cross Layer Based Virus Detection System for Wireless Local Area Networks

Dr. Vinod Kumar*

Assistant Professor, PG Department of Computer Science, Dev Samaj College for Women, Ferozepur City

Abstract – In this paper, we propose to design a cross-layer based virus detection technique for wireless networks. In this technique a combined weight value is computed from the Received Signal Strength (RSS) and Time Taken for RTS-CTS handshake between sender and receiver (TT). Since it is not possible for an attacker to assume the RSS exactly for a sender by a receiver, it is an useful measure for intrusion detection. We propose that we can develop a dynamic profile for the communicating nodes based on their RSS values through monitoring the RSS values periodically for a specific Mobile Station (MS) or a Base Station (BS) from a server. Monitoring observed TT values at the server provides a reliable passive detection mechanism for session hijacking attacks since it is an unspoofable parameter related to its measuring entity. If the weight value is greater than a threshold value, then the corresponding node is considered as an attacker. By suitably adjusting the threshold value and the weight constants, we can reduce the false positive rate, significantly. By simulation results, we show that our proposed technique attains low misdetection ratio and false positive rate while increasing the packet delivery ratio.

Keywords: Intrusion detection, wireless networks, RSS, cross layer, RTS-CTS handshake, TT.

- X -

1. INTRODUCTION

Wireless network can be defined as a network of wireless Local Area Networks (LAN) that are linked together to set up a Metropolitan Area Network(MAN), generally situated in one geographical area. There are several wireless interface standards that are available at present. Few of them function inside the licensed and unlicensed spectrum, few point to point, and others point to multi-point, etc., The most widely used standard is the 802.11 family (802.11, 802.11a, 802.11b and 802.11g) which is a consumer tool that functions under an unauthorized radio frequency. Every single wireless network comprises of several nodes which are connected together. A node can be illustrated as a set of numerous PCs or other devices linked together by directly making use of the IP network and within direct radio range. A node comprises of a minimum of one router and one or more clients. The clients require fewer configurations and communicate only to the router. The router routes its own and client's data to the remainder of the network. By using radio links or any another ways, the nodes can be linked together. In order to establish a robust

Network, it requires a complex mesh of connections between the nodes. The network's clients connect to the nodes from their home or office and complete the entire network. The nodes which do not have any clients become each group's network environment (Carver, et. al., 2000).

2. VIRUS DETECTION

Intrusion detection has found to be an active research field. In spite of a wide research, intrusion detection undergoes several difficulties. Despite the improvements in security, the risk of intrusion is still a matter of concern because preventive measures may not be practiced at all. As a consequence, intrusion detection systems for wireless LAN neighborhood have begun detecting unauthorized access. Detecting unauthorized access creates a chance to respond to the intrusion and control the potential damage to restore the privacy and integrity of the network. Intrusions are the actions that break the security policy of the system, and intrusion detection is the process which is employed to detect such intrusions. In wireless LAN, intrusion detection

Techniques can be categorized into two methodologies; anomaly detection which is based on the normal behavior of a subject or misuse detection which is based on attributes of known attacks or system vulnerabilities.

Intrusion detection is assumed to be very difficult to avoid security breach in the distant future. At a later point in time, all defensive security mechanism may fail. Usually, a defensive technique was employed to block the attacker. Intrusion detection attempts to discover the attacks and analyze the damage caused in real time. Security violations can be identified from abnormal patterns of usage of system and to gauge these abnormal patterns is not a difficult task. These days, intrusion detection holds a good scope for research.

2.1. Classification of Virus Detection Techniques

Basically, there are two main categorizations of intrusion detection systems. Porras classify intrusion detection into two main categories: statistical and rule-based. And the other categorization is between host based and network based intrusion detection.

2.1.1. Statistical Anomaly Detection Techniques

The statistical approach employs other statistical methods to obtain metrics that model the behavior of a user. In addition, Porras divided this category into threshold and profile based detection. Threshold detection illustrates global threshold independency of users. Profile based detection attempts to set up a profile for normal behavior for each users. Anomalies detection is not on the basis of predefined rules and so it has the positive features of detecting new attacks. The drawbacks of statistical detection are that, it requires huge amount of statistical data to build the threshold/profiles.

2.1.2. Rule-Based Intrusion Detection Techniques

A rule based approach has a set of rules that define normal behavior. Porras again detailed this into anomalies and expert systems. A rule based anomalies system is more or less similar to statistical anomaly detection. The rules are set up from the previous behavior pattern. Rule based anomalies face lots of challenges, namely, monitoring etc.

A rule-based expert (penetration) system, which is also known as signature based, employs pre-defined signatures to identify attacks. Signature based detection is assumed that all attacks have their own unique signature that can be identified. Every time a new attack is detected, a new rule must be written, distributed and installed.

2.2. Various Intrusion Detection Techniques for Wireless Networks

- ***Specification-Based Technique***: In this technique, traces and ordered sequences of execution events are used to identify the intended behaviors of concurrent programs in a network. The drawback of this approach is that considerable work has to be done to specify correctly the behavior of the many privileged system programs, and these conditions will be operating-system specific.

- ***Radio Frequency Fingerprinting (RFF) Based Technique***: This technique incorporates RFF into a wireless Intrusion Detection System (IDS), for sensing Media Access Control (MAC) address spoofing attack which leads to the unauthorized deployment of network resources. RFF technique identifies a transceiver which is based on the transient portion of the signal it produces.

- ***A Swarm-Intelligence-Based Technique***: Swarm intelligence based intrusion detection technique reduces the inaccuracies and augments the real-time response in the present intrusion detection techniques for WLAN.

- ***Immune System Technique***: This technique provides a detailed description of work relating to the application of Artificial immune systems to the problem of intrusion detection in WLAN.

- ***Adaptive Hierarchical Agent-Based Technique***: The adaptive hierarchical Agent-based Intrusion Detection Technique uses a fully distributed, multiagent framework. This framework consists of Director Agents, Manager Agents, Tool agents and Surrogate agents.

- ***Distributed Technique***: This technique is an overview of Intrusion Detection Technology for distributed computing networks. The technique employs data mining techniques to help the hierarchical DIDS to construct required features from raw data and dynamically create normal user behavior profiles.

- ***Layered Technique***: Layered technique involves the development and deployment of multiple layers of security with each layer responsible for the overall security.

- ***Statistical Approach***: Statistical-Based systems employ statistical models to discover malicious packets. Statistical models are basically deployed to relate the information relating the occurrence and the variables related to factors that influence occurrence. Statistical systems adjust to various system behaviors and develop a usage pattern.

- ***Battery-Based Technique***: This technique is an efficient alerting system through a mobile host based form of intrusion detection which alerts administrators to safeguard their corporate network by an innovative technique that functions through the implementation of smart battery-based intrusion detection (B-bid) on wireless networks.

- ***Honeypots Technique***: A honeypot is known as an information system resource whose value lies in unauthorized use of that resource. This concept is deployed to study attackers and kinds of attacks, by providing useful details about tools, methods, and intentions of attackers.

- ***Text Categorization Techniques***: Text Categorization techniques are on the basis of the k- Nearest Neighbor (kNN) classifier, which is employed to categorize program behavior as normal or intrusive.

- ***Dependency-Based Distributed Technique***: In Dependency-Based Distributed Technique hosts are clustered into regions which are on the basis of network proximity and dependency. Here, communication among them becomes well organized. To obtain the dependency, different intrusion detection techniques are applied within the regions and across the regions.

3. RELATED WORK

Zhang *et al.* [14] focused on the examination of the anomaly-based intrusion detector's operational capabilities and drawbacks through their operating environments. Anomaly detection is classified in a statistical framework based on the similarity with the induction problem for describing their general expected behaviors. For the apparent subjects from hosts and networks, several key problems and respective potential solutions about the normality characterization for the observable subjects are addressed. Based on some existing achievements anomaly detector's evaluations are also examined. However, the negative aspects of statistical anomaly detection are that, it requires large amount of statistical data to setup the threshold or profiles.

(Rehak, et. al., 2008) have proposed a research to detect malicious traffic in high-speed networks by correlated anomaly detection methods. Based on FPGA elements transparent inline probes are used to obtain the real time traffic statistics in Net Flow format and gives a traffic statistics to the agent-based detection layer. The agent uses a particular anomaly detection method in this layer to detect the anomalies and describes the flows in its extended trust model. The agent shares the anomaly estimation of the individual network flows which are uses as an input for the agents trusts models. In order to estimate their maliciousness the trustfulness values of individual flows from all agents are combined. The drawback of this method is that it does not support the distributed adaptation mechanism. And as a future work, they have planned to introduce the distributed adaptation mechanism with more effectiveness in its performance. Abd Razak *et al.* [13] have proposed a new IDS framework for MANET environments based upon the concept of a friend in a small world phenomenon. The proposed two-tier IDS framework has been designed to overcome longer detection mechanisms and detection suffering from the potential for blackmail attackers and false accusations with the help of friend nodes. It is hypothesized that with the introduction of friend nodes, the impacts of the IDS problems can be minimized. It is noted that the proposed framework would not be able to work on a diverse MANET environments. (Mosqueira-Rey, et. al., 2007) have described the design of misuse detection agent which is one of the different agents in a multiagent-based intrusion detection system. Using a packet sniffer the agent examines the packets in the network connections and creates a data model based on the information obtained. This data model is the input to the rule based agent inference engine which uses the Rete algorithm for pattern matching. So the rules of the signature-based intrusion detection system become small. One of the drawbacks of the misuse detection is that the database of its signatures must be updated regularly in order to ensure adequate protection.

Almgren, et. al., 2008, have investigated the procedure to use the alerts from may audit sources to improve the accuracy of the IDS. A theoretical model is designed automatically for the reason about the alerts from the different sensors through concentrating on the web server attacks. It also provides a better understanding of possible attacks against their systems for the security operators. This model enables reasoning about the absence of the expected alerts by taking the sensor status and its capability into account. This model is built using Bayesian networks which needs some Initial parameter values that can be provided from the IDS operator. The model exhibits poor sensitivity and in the future work, they plan to program the system in other challenging environments to study more about its drawbacks.

Carver, et. al., 2000, have examined the techniques for providing adaptation in intrusion detection and intrusion response systems. The adaptive hierarchical agent based intrusion system provides detection adaptation by adjusting the amount of system resources which is dedicated to the task of detecting forward activities. This is achieved by dynamically appealing new combinations of lower level detection agents in response to changing circumstances and also by adjusting the confidence related with these lower level agents. For the techniques which do not have successful response, the Adaptive Agent based Intrusion.

Response System (AAIRS) provides response adaptation by considering those responses which is successful in the past. It should be noted that the systems that make use of adaptive training techniques encounter the problem of averting an attacker from steadily training the system in due course to admit a range of anomalous behavior as normal. To overcome this difficulty, it remains an open challenge. (Laleh and Azgomi, 2009) have proposed that fraud is growing remarkably with the growth of modern technology and the universal superhighways of communication which results in the loss of billions of dollars throughout the world each year. This technique tends to propose a new taxonomy and complete review for the different types of fraud and data mining techniques of fraud detection. The uniqueness of this technique is gathering all types of frauds which can be detected by data mining techniques and analyzes some real time approaches which have the ability to detect the frauds in real time. Generally, the data mining techniques tend to waste the resources needlessly and produce a longer time delay.

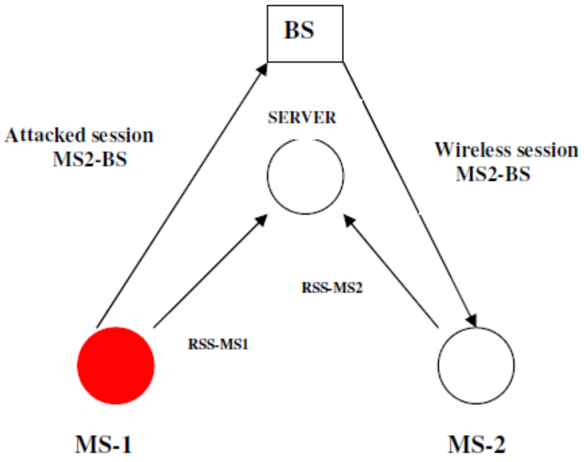
4. CROSS-LAYER BASED VIRUS DETECTION TECHNIQUE

In this paper, we propose to design a cross-layer based intrusion detection technique for wireless networks. In this technique a combined weight value is computed from the RSS and Time Taken for RTS-CTS Handshake (TT).

4.1. 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 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. From the above points, it is clear that it is not possible for an attacker to assume the RSS exactly for a sender by a receiver. The attacker will not be exactly at the same location as the receiver but in order to know the exact RSS value by the receiver it uses the same radio equipment and receives the radio signal with the same level of interference, reflections and refractions. 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. We propose that we can develop a dynamic profile for the communicating nodes based on their RSS values through monitoring the RSS values periodically for a specific MS or a BS from a server. Any sudden or unusual changes can be marked as doubtful activity which indicates the possible session of hijacking attack. The RSS profile is called dynamic because it is rebuilt for every session between two nodes and it is constantly updated with new observed RSS values for each node per session. 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 both insider and outsider 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 and Received signal strength (RSS). 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.

Detection Algorithm

Step 1: Server measures RSS

Step 2: Server measures TT

Step 3: Server calculates the weight W as

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

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.

By suitably adjusting the values of $Dthr$, and $w1$ and $w2$, we can reduce the false positive rate, significantly.

5. SIMULATION RESULT

This section deals with the experimental performance evaluation of our algorithm through simulations. In order to test our protocol, the NS2 simulator is used. The experimental setup is similar to Figure. We compare our proposed cross-layer based intrusion detection technique with the Radio Frequency Fingerprinting (RFF) technique in terms of parameters; **delivery ratio, false positive rate and misdetection ratio** at different transmission ranges and at different attacks rates. The simulation results show that the proposed technique attains low misdetection ratio and false positive rate while increasing the packet delivery ratio.

5.1 Effect of Varying Ranges

In our first experiment, we vary the transmission range as 100,250,300,350 and 400m.

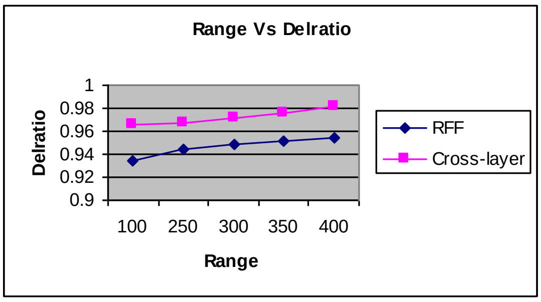


Fig 1: Range Vs Delivery Ratio

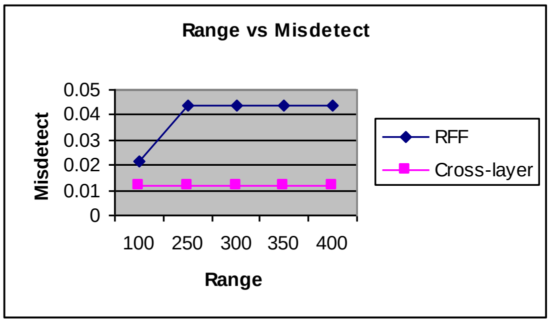


Fig2 : Range Vs Misdetection ratio

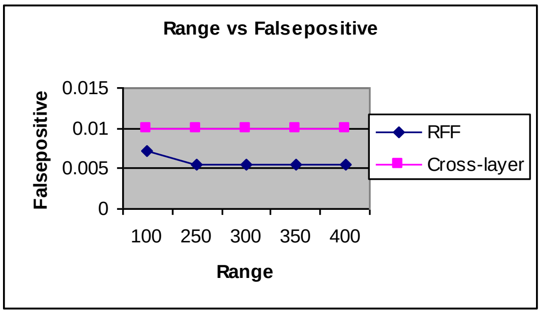


Fig3 : Range Vs False positive

Figure1 above shows the delivery ratio of our cross-layer technique and RFF. From the figure, we can see that packet delivery ratio is more in cross-layer scheme when compared with RFF scheme.

Figure 2 above shows the misdetection ratio of our cross-layer technique and RFF. From the figure, we can see that the misdetection ratio is significantly less in our cross-layer scheme when compared with RFF scheme, since it accurately detects the intrusion.

Figure 3 above shows the false positive rate of our cross-layer technique and RFF. From the figure, we can observe that our cross-layer scheme attains low false positive rate, when compared with RFF scheme, since it accurately detects the intrusion.

6. CONCLUSION

1. The various methods and IDS available in the literature for intrusion detection in WLAN have been thoroughly investigated. The issues involved there in like (i) the outstanding vulnerabilities and different types of attacks in WLAN,(ii) existing wireless IDS techniques (iii) the intrusion detection tools, to analyze their performance and enhancements for WLAN are critically examined by using NS2 Simulator.

2. To address the issues involved in intrusion detection, the intrusion detection technique

have been designed in WLAN. The proposed intrusion detection technique is cross layer based. The technique is evaluated using NS2 simulator on Fedora platform. The quantitative evaluation was done using the three performance metrics i.e. false positive rate, misdetection ratio and packet delivery ratio.

REFERENCES

Almgren M., Lindqvist U., and Jonsson E. (2008). "A Multi-Sensor Model to Improve Automated Attack Detection," *in Proceedings of Lecture Notes in Computer Science*, Berlin, pp. 291-310.

Barbeau J. and Kranakis E. (2004). "Enhancing Intrusion Detection in Wireless Networks Using Radio Frequency Fingerprinting," *in Proceedings of the 3rd IASTED International Conference on Communications, Internet and Information Technology (CIIT}*, Kranakis, pp. 201-206.

Bellaaj H., Ketata R., and Hsini A. (2007). "Fuzzy Approach for 802.11 Wireless Intrusion Detection," *in Proceedings of 4th International Conference: Sciences of Electronic, Technologies of Information and Telecommunications*, Tunisia, pp. 1-7.

Carver C., Humphries J., and Pooch U. (2000). "Adaptation Techniques for Intrusion Detection and Intrusion Response Systems," *in Proceedings of IEEE International Conference on Systems Man and Cybernetics*, USA, pp. 2344-2349.

Debar H. (2002). "An Introduction to Intrusion-Detection Systems," *in Proceedings of Connect, IBM Research,* USA, pp. 1-18.

Encyclopedia-PC Magazine, available at: http://www.pcmag.com, last visited 2012.

Laleh N. and Azgomi M. (2009). "A Taxonomy of Frauds and Fraud Detection Techniques," *in Proceeding of Communications in Computer and Information Science*, Berlin, pp. 256-267.

Magalhaes R. (2003). "Host-Based IDS vs. Network-Based IDS (Part 2-Comparative Analysis)," available at: http://www.windowsecurity.com/articles/hids_vs_nids_part2.html, last visited2003.

Mosqueira-Rey E., Alonso-Betanzos A., Rio B. and Pineiro J. (2007). "A Misuse Detection Agent forA *Cross-Layer Based Intrusion Detection Technique for Wireless Networks* 207 Intrusion Detection in a Multi-agent Architecture," *in Proceedings of the 1st KES International Symposium on Agent and Multi- Agent Systems: Technologies and Applications*, Berlin, pp. 466-475.

Rehak M., Pechoucek M., Bartos K., Grill M., Celeda P., and Krmick V. (2008). "An Intrusion Detection System for High-Speed Networks," *in Proceedings of National Institute of Informatics*, Berlin, pp. 65-74.

Salmanian M., Lefebvre J., Leonard S., and Knight S. (2004). *Intrusion Detection in 802.11 Wireless Local Area Networks*, Defence R&D Canada & Ottawa.

Corresponding Author

Dr. Vinod Kumar*

Assistant Professor, PG Department of Computer Science, Dev Samaj College for Women, Ferozepur City

E-Mail – vinodkumarkamboj@gmail.com