International Journal of Information Technology and Management

Vol. IX, Issue No. XIII, August-2015, ISSN 2249-4510

PERFORMANCE ANALYSIS AND IMPROVEMENT OF CROSS LAYER BASED VIRUS DETECTION TECHNIQUES FOR WIRELESS LOCAL AREA NETWORKS

www.ignited.in

International Journal of Information Technology and Management
Vol. IX, Issue No. XIII, August-2015, ISSN 2249-4510

Performance Analysis and Improvement of Cross Layer Based Virus Detection Techniques for Wireless Local Area Networks

Davinder Pal Singh[1] Dr. Vijay Pal[2]

[1]Research Scholar, Dept. of Computer Science, OPJS University, Churu, Rajasthan

[2]Associate Professor, Dept. of Computer Science, OPJS University, Churu, Rajasthan

Abstract – The security problems of virus detection techniques for wireless local area networks (WLAN) are well known, and the threat of war driving is well publicized. However so far, no known studies have been conducted to assess the risk faced by organizations and the full extent of unauthorized use of wireless LANs. This paper seeks to investigate virus detection in the wireless LAN. Wireless LAN standards offer very unsatisfactory level of security and one could not truly trust them. When using products based on these standards security issues must be taken care in the upper layers. Some commonly used attacks are more stressed in wireless environment and some additional effort should be used to prevent those.

Keywords – VDS, LAN, WLAN

- - - - - - - - - - - - - - X - - - - - - - - - - - - - -

INTRODUCTION

In the past number of techniques had been developed to address different types of attacks, but the effective detection of especially the session hijacking, man-in-the-middle, denial of services; distributed denial of services and shrew attacks are remain open challenges. When the wireless networks are used in strategic applications like hospitals the possibility of this kind of attack should be taken into account with a great care. This paper seeks to investigate virus detection in the Wireless LAN to maintain the confidentiality, integrity and availability of data transmitted on a LAN.

This paper investigates the performance analysis and improvement in virus detection techniques for wireless local area networks.

VIRUS DETECTION SYSTEM

Virus detection is a problem of great significance to protecting information systems security, especially in view of the worldwide increasing incidents of cyber-attacks. Since the ability of an VDS to classify a rage variety of virus in real time with accurate results is important, we will consider performance measures in three critical aspects: misdetection ratio, false positive rate and packet delivery ratio. Since most of the intrusions can be located by examining patterns of user activities and audit records (Denning, 1987), many VDSs have been built by utilizing the recognized attack and misuse patterns. VDSs are classified, based on their functionality, as misuse detectors and anomaly detectors. Misuse detection systems use well-known attack patterns as the basis for detection.

LITERATURE REVIEW

Zhongua Zhang et al [55] 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.

Mark Handley et al [56] have proposed a fundamental problem for network intrusion detection system. In this system an efficient attacker can avoid detection by creating uncertainties in the traffic stream as seen by the monitor. This problem can be avoided by introducing a new network forwarding element called traffic normalizer. A number of tradeoffs in designing a normalizer, highlighting the important question of the degree to which normalizations weaken end-to-end protocol semantics are examined.

Martin Rehak et al [57] 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 NetFlow 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.

John Haggerty et al [58] have proposed that a major threat to the information economy is denial-of-service attacks. These attacks are common even though the widespread usage of the perimeter model countermeasures. Therefore to provide early detection of flooding denial-of-service attacks, a new approach is assumed which uses statistical signatures at the router. There are three advantages for this approach. They are: Computational load on the defense mechanism is reduced by analyzing fewer packets, if the system is under protection then the state information is not required and alerts may span many attack packets. Thus to prevent malicious packets from reaching their proposed target in the first the defense mechanism may be placed within the routing infrastructure.

Giovanni et al [59] have proposed that the mobile ad hoc network routing protocols are highly vulnerable to subversion. Particularly some attacks against the AODV and some threats to wireless ad hoc networks are discussed. They have also presented a tool which aims at the real-time detection of these attacks. The tool observes the network packets to detect local and distributed attacks within its radio range. Experiments show that when a limited amount of resources are used then the tool provides efficient intrusion detection.

Shukor Abd Razak, Steven Furnell, Nathan Clarke, and Phillip Brooke [60] 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.

Eduardo Mosqueira-Rey et al [61] 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.

Magnus Almgren et al [62] have investigated the procedure to use the alerts from may audit sources to improve the accuracy of the intrusion detection system (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.

Curtis A. Carver et al [63] 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.

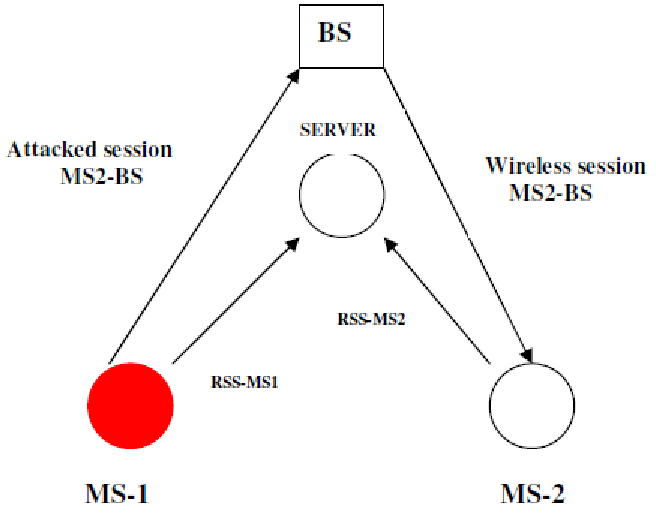
Naeimeh Laleh et al [64] have proposed that fraud is growing remarkably with the growth of modern technology and the universal superhighways of communication which results in the loss of billions of dollars throughout the world each year. This technique tends to propose a new taxonomy and complete review 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.

PROPOSED WORK

In this paper, we propose to design a cross-layer based virus detection technique for wireless local area networks. In this technique a combined weight value is computed from the received signal strength (RSS) and time taken for RTS-CTS Handshake (TT).

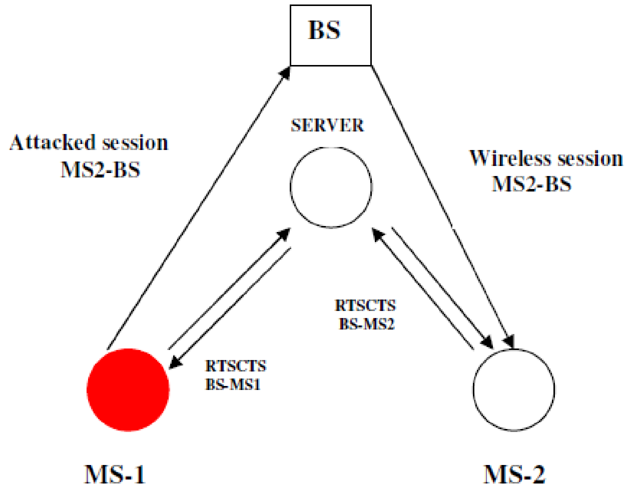
MONITORING RECEIVED SIGNAL STRENGTH (RSS)

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. 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.



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 atomic and free from collisions with other wireless nodes. 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.



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.

TESTING THE RESULT

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 virus 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.

CONCLUSION

In this research article a cross-layer based virus detection technique for wireless network is proposed.

A dynamic profile of received signal strength (RSS) values for the communicating nodes is developed, through monitoring the RSS values periodically for a specific MS or a BS from a server. The performance of the proposed technique is compared with that of Radio Frequency Fingerprinting (RFF) at different transmission range (100,250,300,350 and 400M, 500M) and at different traffic rates (50,100,150,200 and 250kb). The simulation results shows that the cross layer based techniques are more effective than the Radio Frequency Finger printing (RFF) for the detection of both session hijacking attacks in WLAN. The packet delivery ratio was improved by more than 1%, whereas the misdetection ratio was significantly reduced (by more than 1%) in the proposed cross-layer scheme when compared with RFF scheme at different transmission ranges and at different attack traffic rates.

The cross-layer scheme also attains low false positive rate (.02% to .06% approximately) as compared to RFF scheme, which indicates the better detection efficiency of the proposed technique. The investigation shows that the proposed technique attains low misdetection ratio as well as false positive rate while increasing the packet delivery ratio. The novelty of the proposed technique is that it achieves scalability from 100 meters to 400 meters with high detection efficiency.

REFERENCES

A. Lazarevic, V. Kumar, and J. Srivastava (2005). Intrusion detection: a survey, managing cyber threats: issues, approaches, and challenges. *Springer Verlag*, page 330.

Arunesh Mishra and William A. (2002), "Your 802.11 Wireless Network has No Clothes," IEEE *Wireless Communications Magazine*, Vol.9, No. 6, pp. 44-51.

Arunesh. Mishra, M. ho Shin, and W. A. Arbaugh, (2003), "An Analysis of the Lay er 2 Handoff costs in Wireless Local Area Networks", *ACM Computer Communications Review* , Vol. 33, No. 2, pp. 93 - 102.

Curtis A. Carver, Jr., Jeffrey W. Humphries, and Udo W. Pooch "Adaptation Techniques for Intrusion Detection and Intrusion Response Systems."

Denning E. D. (1987). An intrusion detection model. *IEEE Transactions on Software Engineering*, pages 222–32.

Eduardo Mosqueira-Rey, Amparo Alonso-Betanzos, Belen Baldonedo Del Rio, and Jesus Lago Pineiro (2007). A Misuse Detection Agent for Intrusion Detection in a Multi-agent Architecture". Springer-Verlag Berlin Heidelberg.

Giovanni Vigna, Sumit Gwalani, Kavitha Srinivasan, Elizabeth M. Belding-Royer and Richard A. Kemmerer (2004). "An Intrusion Detection Tool for AODV-based Ad hoc Wireless Networks", IEEE Computer Society Washington, DC, USA.

J. M. Estevez-Tapiador, P. Garcia-Teodoro, and J. E. Diaz-Verdejo (2004). Anomaly detection methods in wired networks: a survey and taxonomy. In *Computer Networks*, pages 1569–84.

Jeyanthi Hall Michel Barbeau and Evangelos Kranakis, "Detecting Rouge Devices In Bluetooth Networks Using Radio Frequency Fingerprinting", School Of computer Science, Carleton University.

Jeyanthi Hall, Michel Barbeau and Evangelos Kranakis, **"**Enhancing Intrusion Detection in Wireless Networks Using Radio Frequency Fingerprinting", School Of computer Science, Carleton University.

John Haggerty, Qi Shi and Madjid Merabti (2006). "STATISTICAL SIGNATURES FOR EARLY DETECTION OF FLOODING DENIAL-OFSERVICE ATTACKS", Springer Boston.

L. Portnoy, E. Eskin, and S. J. Stolfo (2001). Intrusion detection with unlabeled data using clustering. In *The ACM Workshop on Data Mining Applied to Security*.

Magnus Almgren, Ulf Lindqvist, and Erland Jonsson (2008). A Multi-Sensor Model to Improve Automated Attack Detection", Springer-Verlag Berlin Heidelberg.

Martin Rehak, Michal pechoucek, karel Bartos, Martin Grill, Pavel celeda and vojtech krmick (2008). "An intrusion detection system for high-speed networks", national institute of informatics.

Naeimeh Laleh and Mohammad Abdollahi Azgomi (2009). "A Taxonomy of Frauds and Fraud Detection Techniques", Springer-Verlag Berlin Heidelberg.

P Kabiri and A. A. Ghorbani (2005). Research in intrusion detection and response – a survey. *International Journal of Network Security*.

P. Garcia-Teodoro, J. E. Diaz-Verdejo, G. Macia-Fernandez, and E. Vazquez (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. *Computers & Security*, pages 18–28.

Shukor Abd Razak, Steven Furnell, Nathan Clarke, and Phillip Brooke (2006). "A Two-Tier

Intrusion Detection System for Mobile Ad Hoc Networks – A Friend Approach", Springer-Verlag Berlin Heidelberg.

V. Barnett and T. Lewis (1994). *Outliers in statistical data*. Wiley.

Y. Liao and V. R. Vemuri (2002). Use of k-nearest neighbor classifier for intrusion detection. *Computers & Security*.