A Design and Implementation for Secure Transmission against Spoofing Attacks Inducing Indirect Phishing in Static Network

Manne Naga V J Manikanth, Prof .Dr.KasukurthiVenkataRao
Department of Computer Science, Andhra university,Visakhapatnam
Department of Computer Science, Andhra university,Visakhapatnam

Abstract:*In recent days Cyber attacks have become common threat which is leading to exploit data confidentiality. Spoofing is a common technique which is used by the attackers to make themself unidentified and probe towards phishing the data from target machines. So to make the data not influenced to phishing and the nodes in the network are not subjecting to spoofing we use a mechanism called pilot signal which is used with Channel state indicator. When we like to send data from the source to receiver we use a mechanism called pilot signal which is used like a strobe to the node in the network and estimates the channel state having the genuine internet protocol address. We maintain uplink and downlink paths for the nodes. We set frequency energies to the node at the time of adding it to the network, these frequencies are used to send and receive the signals throughout the network. By using CSI in the downlink and uplink paths the difference in the frequency is calculated to detect a spoofing event over a node if the received parameters are in un order to the standard frequency which is aligned earlier we treat it as detection of spoofing attack. The detection probability is evaluated based on the derived parameters of CSI from a node at a given requirement on the less probability of false alarming. The achievable secrecy rate is utilized to measure the security level of the data transmission. Our analysis shows that even without any pre-assumed knowledge of eavesdropper, the proposed scheme is still able to achieve the maximal secrecy rate in certain cases. our scheme could achieve a high detection probability as well as secure transmission.*

Index Terms: channel state indicator, detection, frequency, pilot signal

I.INTRODUCTION

Data is being very important source .keeping the data safe without compromising the confidentiality is the biggest challenge. When it comes to sending and receiving the data at distinct nodes there is no clue about confidentiality state of the data .So to maintain the confidentiality of the data a strict mechanism needs to be developed , though the mechanism is developed as the data travels through the network so maintaining the standard for confidentiality of the data will change basing on the type of network on which it is implemented. In the wireless based network it is hardly impossible maintain the standard and also the reliability to become very low at every point because most of the nodes in the network are dynamic or movable in nature. As the network is dynamic adding up of new nodes and configuring them timely is also a challenge . so we adapt a mechanism for wired networks only to make sure that the nodes are not subjected to any spoofing and phishing attacks because these may exploit data confidentiality and integrity. Spoofing is a mechanism which transforms an identity to other identity giving an false assumption to the real entity which can be a prominent way for exploiting the data, In other case this spoofing can also be bridge in performing eavesdropping which is likely to disturb data integrity, this mechanism is popularly called as phishing. We have

numerous number spoofing methodologies but here we mainly concentrate on IP Spoofing over the nodes. When ever a node is subjected to spoofing we develop a system to detect the spoofing event and to make sure that the data is not transferred to that node. This will indirectly stop eavesdropping or phishing attack also.

II. EXISTING SYSTEM

In the existing system the data transfer is done through a network with synchronous and asynchronous time frames which have a collection of acknowledgements and retransmission basing on the traversal of the data through the nodes. But some devices really bother on transmission rate of the data , so such devices adapt a mechanism of strobe to save time in their transmission which can keep the network in high utilization. First the strobe signal is sent if acknowledgement is sent by the receiver the data is transferred over the network. If the acknowledgement is discarded the transmission event is called off assuming the node is down .

III.PROPOSED SYSTEM

In the proposed system we look for data transfer with security. So in this context we design a mechanism to detect IP spoofing. As the nodes in the network have dedicated links we assign a frequency energy for each link, frequency energy is generally a estimate of energy consumed by the link. All the nodes in the network posses only dedicated links based on the topology arrangements. The links among the nodes are divided into upload link and download link. Upload link is used to send the data to the receiver and the download link is used to receive the data from the receiver. This arrangement will also reduce data collision and congestion in a network we will not make two different links physically between each node but we will split the link into two way traffic i.e using one link physically we will run two way traffic scheme. In Addition to this we assign a predetermined frequency energy numbers for this links

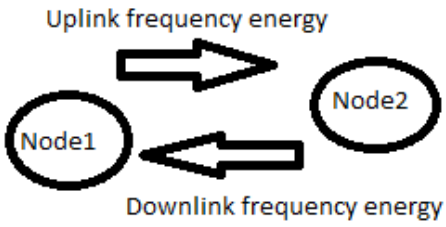

Figure1 Illustrates the mechanism of energy assignment of uplink and downlink frequency trunks

We assign frequency energy for upload and download links to all the nodes in the network , the mechanism is shown in the figure 1.when a node in a network wants to send data to the other node in the network first it will send a signal pilot signal which is similar to the strobe signal, the pilot signal will acknowledge with a receiver signal to make sure the frequency energy is unchanged, as the signal passes to the upload link and download link they hold frequency energies through their traversal from receiver to destination again to the destination The frequencies are monitored over the links with thehelp of channel state information(CSI) this will be able to sense the frequency through out the links over the network. This will help to observe the changes in the nodes as the nodes initially will be added in to the network with a IP address which will continue to remain the same for stable topology, In case if any of the node IP address changes dynamically CSI will record an event. If any dynamic IP address change is found it could be due to IP spoofing so we will discard the data traversal to this node where there is such event .The frequency energy used in upload and download links will be same if the IP address is unchanged if any IP address of nodes are changed then CSI will recognise the change the frequency in the upload and download links gets changed and the connections for the node is closed logically, This is the methodology which will ensure no Spoofing and Phishing attacks are

done. The data travelling in the network should pass multiple nodes routing is done by different routing algorithms basing on their system adaptability so if any of the node in the route is not accessible due to this above mechanism the data could be sent through a new route which is re –routing can be done from the previous node, If the node itself is the destination data will be discarded for security aspects.

IV CONCLUSION

In this paper we have studied how the behavioural aspects of network can be a keen way for the attacks like spoofing and phishing. We have adapted a pilot signal and CSI indicators to make sure the nodes in the network are secure in the vice versa we are able to eradicate the nodes which are unsecured for the data transmission. The above mechanism will ensure that data is not left to the attackers and the monitoring of nodes are done continuously.

REFERENCES

[1] W. Stallings, Cryptography and Network Security: Principles and Practice, 3rd ed. Upper Saddle River, NJ, USA: Prentice Hall, 2003.

[2] C. E. Shannon, “Communication theory of secrecy systems,” Bell Syst. Tech. J., vol. 28, no. 4, pp. 656–715, Oct. 1949.

[3] A. D. Wyner, “The wire-tap channel,” Bell Syst. Tech. J., vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[4] I. Csiszár and J. Korner, “Broadcast channels with confidential messages,” IEEE Trans. Inf. Theory, vol. 24, no. 3, pp. 339–348, May 1978.

[5] S. Shafiee and S. Ulukus, “Achievable rates in Gaussian MISO channels with secrecy constraints,” in Proc. IEEE Int. Symp. Inf. Theory (ISIT), Jun. 2007, pp. 2466–2470.

[6] A. Khisti and G. W. Wornell, “Secure transmission with multiple antennas—Part II: The MIMOME wiretap channel,” IEEE Trans. Inf. Theory, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[7] Q. Xiong, Y. Gong, Y.-C. Liang, and K. H. Li, “Achieving secrecy of MISO fading wiretap channels via jamming and precoding with imperfect channel state information,” IEEE Wireless Commun. Lett., vol. 3, no. 4, pp. 357–360, Aug. 2014.

[8] S. Goel and R. Negi, “Guaranteeing secrecy using artificial noise,” IEEE Trans. Wireless Commun., vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[9] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, “Channelbased detection of Sybil attacks in wireless networks,” IEEE Trans. Inf. Forensics Security, vol. 4, no. 3, pp. 492–503, Sep. 2009.

[10] Q. Li and W. Trappe, “Detecting spoofing and anomalous traffic in wireless networks via forge-resistant relationships,” IEEE Trans. Inf. Forensics Security, vol. 2, no. 4, pp. 793–808, Dec. 2007.

[11] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, “Channelbased spoofing detection in frequency-selective Rayleigh channels,” IEEE Trans. Wireless Commun., vol. 8, no. 12, pp. 5948–5956, Dec. 2009.

[12] L. Xiao et al., “PHY-authentication protocol for spoofing detection in wireless networks,” in Proc. GLOBECOM, 2010, pp. 1–6.

[13] F. J. Liu, X. Wang, and H. Tang, "Robust physical layer authentication using inherent properties of channel impulse response," in Proc. MILCOM, Nov. 2011, pp. 538–542.

[14] X. Zhou, B. Maham, and A. Hjorungnes, "Pilot contamination for active eavesdropping," IEEE Trans. Wireless Commun., vol. 11, no. 3, pp. 903–907, Mar. 2012. [15] D. Kapetanovic, G. Zheng, K.-K. Wong, and B. Ottersten, "Detection of pilot contamination attack using random training and massive MIMO," in Proc. 24th PIMRC, Sep. 2013, pp. 13–18.

[16] J. Yang, S. Xie, X. Zhou, R. Yu, and Y. Zhang. (2014). "A semiblindtwoway training method for discriminatory channel estimation in MIMO systems." [Online]. Available: http://arxiv.org/abs/1405.4626v1

[17] Q. Xiong, Y.-C. Liang, K. H. Li, and Y. Gong, "An energy-ratio-based approach for detecting pilot spoofing attack in multiple-antenna systems," IEEE Trans. Inf. Forensics Security, vol. 10, no. 5, pp. 932–940, May 2015. [18] S. M. Kay, Fundamentals of Statistical Signal Processing: Estimation Theory, vol. 1. Upper Saddle River, NJ, USA: Prentice Hall, 1998.

[19] D. J. Tylavsky and G. R. L. Sohie, "Generalization of the matrix inversion lemma," Proc. IEEE, vol. 74, no. 7, pp. 1050–1052, Jul. 1986.

[20] S. M. Kay, Fundamentals of Statistical Signal Processing: Detection Theory, vol. 2. Upper Saddle River, NJ, USA: Prentice Hall, 1998.

[21] T.-Y. Liu, S.-C.Lin, T.-H.Chang, and Y. P. Hong, "How much training is enough for secrecy beamforming with artificial noise," in Proc. ICC, Jun. 2012, pp. 4782–4787.

[22] T. Yoo and A. Goldsmith, "Capacity and power allocation for fading MIMO channels with channel estimation error," IEEE Trans. Inf. Theory, vol. 52, no. 5, pp. 2203–2214, May 2006.

[23] G. Strang, Linear Algebra and Its Applications. Cambridge, MA, USA: Wellesley-Cambridge, 1998.

Authors

Manne Naga VJ Manikanth pursing Master of technology in Andhra University College of Engineering Autonomous in Department of Computers science and System Engineering

Dr. KASUKURTHI VENKATA RAO Professor in Department of CS&SE,A.U. College of Engineering (A) and also Hon. Director, Computer Centre & Webmaster for Andhra university