A Survey on Cross Layer Security

Sandeep Sharma
Gautam Buddha University,Greater Noida (U.P.)

Rajesh Mishra
Gautam Buddha University,Greater Noida (U.P.)

Karan Singh
Gautam Buddha University,Greater Noida (U.P.)

ABSTRACT

Computer network is very essential part of our life by which we can share the information via different technologies such as wired or wireless. Generally the wireless is mostly adopted technology by us due to various advantages like ease of installation, mobility, reconfigure ability, low infrastructural cost etc. but suffers from more attacks as the wireless channel is open. Therefore, many researchers are working in this hot area to secure the wireless communication. Cross layer design refers to protocol design done by actively exploiting the dependence between the protocol layers to obtain better performance gain in the wireless environment. In this paper, we are providing a survey of different security mechanism of cross layer which is the part of wireless network security.

General Terms

Wireless Network, Network Security, Cross Layer Design

Keywords

Cross layer, Attack, Wireless Authentication, EAP, WEP, WPA

1. INTRODUCTION

Wireless networks offer mobility to the users due to which everybody wants to join it. As the number of the users are increasing hence the security of the message is the main concern. The devices comprises of the wireless network are available to the potential intruders and also modifiable for such intrusions. If the intruder is within the range, he can listen to the unintended information. Although a number of cryptographic algorithms are available which provides a high level of security, still there is a need of more secure algorithm.

The physical properties of a wireless medium are a powerful source of the domain specific information that can be used to complement and enhance the traditional security mechanism. The main objective of the physical layer security in the wireless network is to maximize the rate of reliable information from the source to the destination by keeping the intruder mode as ignorant as possible for the transmitted information. Security can be applied to different layers. In this work, we emphasize to achieve security by the concepts of cross layer design.Cross layer design refers to protocol design done by actively exploiting the dependence between the protocol layers to obtain better performance gain. This is unlike the layered architecture where the protocols at the different layers are designed independently and do not depend on the other layer protocol. In a layered architecture, the designer has two choices at the time of the protocol design. Firstly protocol can be designed by respecting the rules of the reference architecture i.e. designing a protocol such that the higher layer protocol only makes use of the services at the lower layers and is not concerned about the details of how the service is being provided. Secondly, protocols can be designed by violating the reference architecture, for example by allowing direct communication between protocols at the nonadjacent layers. Such violation of the layered architecture is cross layer design with respect to the reference architecture.

Today, there exist some theoretical and practical aspects and contributions that support the potential of the physical layer security ideas to strengthen the security of the wireless networks. The paper is arranged in the following way: we begin in Section 2, discussing the problem with wireless LAN. In Section 3, we are providing with different related work of wireless network security. We present comparative summary of wireless security in Section 4 and conclusions of this paper is briefed in section 5.

2. PROBLEM WITH WLAN

It has been discovered that Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) and Extensible Authentication Protocol-Tunneled Transport Layer Security (EAP-TTLS) protocols are vulnerable to Man-in-the-Middle (MitM) vulnerability and Denial of Services (DoS) vulnerability that would allow a malicious entity to infiltrate the network. This security vulnerability is still marked as an open issue to be solved. In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. A man in the middle attack is one in which the attacker intercepts messages in a public key exchange and then retransmits them, substituting his own public key for the requested one, so that the two original parties still appear to be communicating with each other. The the subsection 2.1 and 2.2 we are discussing the EAP authentication method to provide mutual authentication and the way to vulnerable via the Man-in-the-Middle attack in the EAP authentication method.

2.1 Tunneled EAP Authentication Method

During the first phase of a tunneled EAP authentication method, the network client verifies the identity of the RARIUS server by validating the server's TLS signature. The client and server will both derive a symmetric key to protect the second phase of the EAP authentication. The goal of the second phase is to validate the identity of the network client using what is called an 'Inner method'.
Typically a legacy password based method is used in the second phase. Even methods know to have security vulnerabilities can be used as inner methods because the security association derived from the initial TLS authentication will protect message exchanges that take place during the second phase.

2.2 Man-in-middle Attacks on tunnel EAP Authentication

This can allow a man-in-the-middle to authenticate to the server as legitimate client by posing as an authenticator to a legitimate client using a non-tunneled protocol. When the same proof of credentials can be used in both authentications,

the attacker merely shuttles the credential proof between them. Protected-EAP version 0 (PEAPv0) and several other TLS tunneled methods are vulnerable to such an attack. The active attack by Man-in-the-Middle (MitM) proceeds as follows:

- MitM waits for a legitimate device to enter an un-tunneled legacy remote authentication protocol and captures the initial message sent by the legitimate client.
- MitM initiates a tunneled authentication protocol with an authentication agent.
- After the tunnel is set up between MitM and the authentication agent, the MitM starts forwarding legitimate client's authentication protocol messages through the tunnel.
- MitM un-wraps the legacy authentication protocol messages received through the tunnel from the authentication agent and forwards them to the legitimate client.
- After the remote authentication ended successfully, MitM derives the session keys from the same keys it is using for the tunnel.

The IETF EAP working group has recognized the problem of Man-in-the-middle attacks on tunneled EAP authentication methods. The DoS problem can be solved by enhancing the Authentication and Man-in-the-Middle (MitM) by the use of Encryption Method. In the next section, we talk about the related work of the cross layer security.

3. RELATED WORK

This section summarizes the literature survey on the security aspects of the wireless networks at the physical layer through algorithms at the physical layer, and the concept of cross layer approach in wireless networks.

The paper [26] had discussed the challenges ahead of security at the physical layers. The author uses the channel frequency responses of the user for the authentication in wireless environment. The paper [27] proposed a physical layer authentication scheme to detect Sybil attack by exploiting the spatial variability of the radio channels in indoor and urban environment [28].The author suggests the ways to minimize the no. of sensors needed for estimating the signal coverage in the cell [19]. The physical layer properties of the wireless medium are a powerful source of domain specific information that can be used to complement and enhance the traditional security mechanism. Cross layer approach has been proposed to enhance the security of wireless networks for indoor wireless environment [17]. Several physical layer authentication techniques have been proposed to enhance the security in wireless networks, exploiting the physical-layer information such as the received signal strength (RSS) [12],[7],[6], channel impulse response (CIR) [13] and channel frequency response (CFR) [18],[20],[10].

Liang Xiao et al. propose a MIMO-assisted channel-based authentication scheme, exploiting current channel estimation mechanisms in MIMO systems to detect spoofing attacks with very low overheads [20].The work by Liang Xiao in [9] proposed a scheme to investigate the localization of MTs using a network of N spatially dispersed sensors, where the sensors communicate with each other and with the cellular system. A key benefit of this approach is that it provides round the-clock measurements from many low-cost devices. Willie K. Harrison et al. discussed and proposed a scheme to enhance the security by means of cryptography and channel coding [29]. The author in [11] proposed the induction of noise-like intentional interference to achieve security. M. Tahir et al. proposed a Wireless Communication Protocol which uses CSI to provide security at the physical layer [30]. Tommaso Melodia in [31],[16] proposed a design of cross layer communication architecture to provide the quality of service in a wireless multimedia network. The simulation results shows the delays are low, with low jitter and throughput is fairly constant over time. Suhas Mathur et al. in [32] argue that a new paradigm which exploits the physical layer properties of the wireless medium such as rapid spatial, spectral and temporal de-correlation properties of the radio channel can enhance the confidentiality and authentication.

Kai Zeng et al. in [33] discussed and compared the software-based, hardware-based and channel/ location- based physical layer authentication schemes and found that the channel based fingerprinting is most robust in terms of uniqueness, location distinction, adaptiveness and difficulty to mimic. Nikolaos Gatsis et al. in [15] have given an algorithm for cross-layer design of wireless networks in the presence of fading. The author also found the optimal design variables-end to end rates, multi commodity flows, link capacities and average power.

A network control strategy utilizing the optimal solution of the cross-layer design problem was also outlined. Whereas the cross layer approach for wireless ad-hoc network with fading is discussed in [68].Spoofing attacks are very easy to launch in wireless networks such as 802.11 in which a device can alter the MAC address by simply issuing an ifconfig Command. This weakness is a serious threat that can lead to attacks like session hijacking [3], attacks on the access control list which gives privilege to the user to use the services of the network [2]. Paul in [21] suggested a multicarrier authentication scheme at the physical layer. In this paper the author suggested a method which allows low complexity but high quality authentication decisions. Experiments performed in [6] show that although Received Signal Strength Indicator (RSSI) is a time varying and unreliable in general and the radio transmission is non-isotropic, using ratio of RSSIs from multiple receivers it is feasible to overcome from the Sybil Attacks.

To address the problem of unauthorized access, a technique to identify the network interface card NIC is proposed by Cherita Corbett et al. in [8].For a 802.11 wireless network, the Wired Equivalent Protocol WEP is discussed in detail by Nikita Borisov et al. in [1] also they have pointed on the security threats in WEP. In [24] the author has proposed a physical layer approach to enhance the wireless security by using the unique wireless channel state information (CSI) of the legitimate user for authentication. The spoofer whose spatial location is different has different value of CSI and hence can be differentiated from the legitimate user. A survey on the Cross-Layer Design and the suggested future work in this area is discussed in [4] .Byounghoon Kim and Sungwoo Tak has proposed the extensible cross layer design platform which enables the exchange of information between different layers for the optimization of the performance. Also they have proposed a cross layer based adaptive routing algorithm for packet delivery in the end-to-end connections. Shantidev Mohanty in [5] proposed cross layer architecture by merging the layer 2 with layer 3 of the wireless network and develops a handoff management protocol which supports both intrasystem and intersystem handoff management for the new generation wireless system. This protocol uses mobile speed and handoff signaling delay to enhance handoff performance. The next section is providing comparative summary

4. COMPARATIVE SUMMARY

This section discusses the summary of various security mechanisms of cross layer architecture in the following ways:

- Shantidev Mohanty in 2006 [5] proposed a cross layer (layer 2 +3) Handoff Management Protocol for the next generation wireless system by using mobile speed and handoff signaling delay of possible handoff. Efforts can be made to use the concept proposed on the physical layer design to enhance wireless security.
- Marut Demirbas et al. in 2006 [6] proposed a technique based on the RSSI for the first time to detect the Sybil attack in wireless networks. The experiments were performed only for two monitoring node and a single Sybil node. This can be extended to large scale.
- Cherita Corbett et al. in 2006 [8] proposed a method of authentication of the user which is based on the wireless NIC identification. They have used switching algorithm as an attribute to identify the network cards of different vendors. But this method could not help to distinguish between the wireless NICs manufactured by the same vendor.NIC configuration parameters like RTS threshold, maximum retries were not taken into account. Single type host is taken in the experiments.
- Liang Xiao et al. in 2007 [10] uses physical layer to provide security in wireless network by using channel response technique as a fingerprint. The tests were done in the in-building environment. The enhance work could use RSSI, temporal variation, spatial variation due to movement in the building, signal to noise ratio fluctuations , and cross layer approach.
- Y. Chen, et al. in 2007 [12] suggested to introduce a noise like intentional interference to make the eavesdropper incapable of decoding the secret wireless message. Cross layer design approach is not used to increase the wireless security.
- Geetpriya et al in 2007 [14] discussed the advantages of cross layer design in terms of optimization of the network performance in terms of bandwidth, energy and other network resources. They have discussed the challenges and opportunities in cross layer design approach and also suggested and evaluated two cross layer approach based intrusion detection mechanism based on shared data base model.
- Liang Xiao et al. in 2008 [17] suggest an algorithm for the physical layer authentication algorithm using the channel probing technique/channel frequency response of the wireless channel. The tests were carried out in the in-building environment with an assumption of stationary terminals which could not be a practical case of today's scenario. Cross layer approach is not applied to enhance the security level.
- Liang Xiao et al. in 2008 [18] uses a channel response technique for the authentication of mobile terminals in wireless network. The algorithm was tested for mobile terminals with a terminal velocity of 1.43 m/s. Cross layer design approach can be used to enhance the wireless security.
- Byounghoon Kim et al. in 2008 [23] proposed a framework based on cross layer design to improve the network performance in wireless networks. The Cross-Layer based Adaptive Routing algorithm (CAR) shows lower throughput than Ad-hoc on Demand Distance Vector (AODV) and Dynamic Source Routing (DSR).
- Jitendra Tugnait in 2009 [24] proposed a physical layer approach to enhance wireless security by using the wireless channel state information (CSI). This paper used the frequency domain approach (frequency selective due to multipath propagation) and has not used the time domain approach (time selective due to motion between transmitter and receiver). Work could be done to integrate these two approaches.
- Liang Xiao et al. in 2009 [27] proposed a channel based authentication scheme for the detection of Sybil attack in wireless networks. The authentication scheme is based on multipath propagation and hence suited for wideband system. Efforts can be made to make it suitable for narrowband systems.
- Liang Xiao et al. in 2009 [28] suggests a channel based spoofing detection algorithm based on the frequency selective Rayleigh channel considering the channel time variations due to environmental changes and terminal mobility. The algorithm which is suggested had cumbersome computation. The wireless security can be enhanced by applying cross layer approach.
- Nikolaos Gatsis et al. in 2010 [15] proposed a cross layer algorithm for wireless networks in presence of fading. In the paper offline network is considered and in future work can be done for the online network.
- Xiawen Xiao in 2010 [22] proposed a four way handshake mechanism to derive the PTK (pair-wise transient key) which played an important part in 802.11i . This protocol decreases the transmission load. The complexity part of the protocol is not touched and need to explore.
- Suhas Mathur et al. in 2010 [32] proposed a physical layer based authentication technique for wireless network using the rapid spatial, spectral and temporal decorrelation properties of the radio channel. Attempts have to make to integrate the cross layer design and existing physical layer techniques to enhance wireless security.
- Kei Zeng et al in 2010 [33] proposed a scheme for authentication and identification of the spoofing attacks using the physical layer parameters but it is applicable to static cases and future work could be done on mobility.
- Anand Sharma in 2010 [34] proposed a protocol for WLAN 802.11i based on the quantum key distribution technique using BB84 protocol of 802.11i. Cost and complexity of the protocol were not taken into consideration so the future work could be on the complexity analysis of the proposed protocol.

5. CONCLUSION

The objective of this paper is to make aware the readers about the cross layer security and recent trends to provide the security in cross layer based wireless network. This paper discussed about the various work of different researchers doing their research in the area of wireless network security. They discussed many attacks such as Man-in-the-middle, Denial-of-services etc. of cross layer based wireless network system. To provide security in the systems researches suggested authentication with the use of NIC identifications and used various parameters such as channel probing, channel state information, RSSI, spatial and temporal correlation etc. for wireless authentication and try to optimize communication, computation overheads and complexity in such systems.

REFERENCES

[1] N. Borisov, I. Goldberg, and D. Wagner, "Intercepting mobile communications:the insecurity of 802.11," in Proc. ACM Annual InternationalConference on Mobile Computing and Networking (MOBICOM), pp. 180–189, Sept. 2002.

[2] A. Mishra, M. Shin, and W. A. Arbaugh, "Your 802.11 network has no clothes," IEEE Commun. Mag., vol. 09, pp. 44–51, Dec. 2002.

[3] A. Mishra and W. A. Arbaugh, "An initial security analysis of the IEEE 802.1x standard," Tech. Rep. CS-TR-4328, University of Maryland, College Park, 2002.

[4] Vineet Shrivastav, "Cross-Layer Design: A Survey and the Road Ahead," in IEEE Communication Magazine, 2005, pp. 112-119.

[5] Shantidev Mohanty, Ian Akyildiz, "A Cross-Layer (Layer 2+3) Handoff Management Protocol for Next Generation Wireless System," in IEEE Transaction on Mobile Computing., vol.5, No. 10, pp. 1347-1360, 2006.

[6] M. Demirbas and Y. Song, "An RSSI-based scheme for sybil attack detection in wireless sensor networks," in Proc. IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), June 2006.

[7] D. Faria and D. Cheriton, "Detecting identity-based attacks in wireless networks using signalprints," in Proc. ACM Workshop on Wireless Security, pp. 43–52, Los Angeles, CA, Sept. 2006.

[8] C. Corbett, R. Beyah, and J. Copeland, "A passive approach to wireless NIC identification," in Proc. IEEE International Conference on Communications, vol. 5, pp. 2329–2334, June 2006.

[9] L. Xiao, L. Greenstein, and N. Mandayam, "Sensor-assisted localization in cellular systems," IEEE Transactions on Wireless Communications, vol. 6, pp. 4244-4248, Dec. 2007.

[10] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Fingerprints in the ether: Using the physical layer for wireless authentication," in Proc. IEEE International Conference on Communications (ICC), June 2007, pp. 4646–4651.

[11] Jorgensen, M.L.; Yanakiev, B.R.; Kirkelund, G.E.; Popovski, P.; Yomo, H.; Larsen, T.., "Shout to Secure: Physical-Layer Wireless Security with Known Interference ," in IEEE Global Telecommunications Conference, 2007. pp. 33-38.

[12] Y. Chen, W. Trappe, and R. Martin, "Detecting and localizing wireless spoofing attacks," Proc. Sensor, Mesh and Ad Hoc Communications and Networks, pp. 193–202, 2007.

[13] N. Patwari and S. Kasera, "Robust location distinction using temporal link signatures," in Proc. ACM Int. Conf. Mobile Computing and Networking, 2007, pp. 111–122.

[14] Thamilarasu, Geethapriya; Sridhar, Ramalingam, "Exploring Cross-Layer Techniques for Security: Challenges and Opportunities in Wireless Networks," IEEE Military Conference, 2007, pp. 1-6.

[15] Nikolaos Gatsis,Alejandro Ribeiro and Georgios B. Giannakis, "A Class of Convergent Algorithms for Resource Allocation in Wireless Fading Networks," IEEE Trans. On Wireless Comm., vol. 9, no.5, pp. 1808–1823, May. 2008.

[16] T. Melodia and I. F. Akyildiz, "Cross-layer Quality of Service Support for UWB Wireless Multimedia Sensor Networks," in Proc. IEEE Conference on Computer Communications (INFOCOM), Mini-Conference, Phoenix, AZ, Apr. 2008.

[17] L. Xiao,Larry J. Greenstein ,Narayan B Mandayam, Wade Trappe, " Using the Physical layer for Wireless Authentication in Time-Variant Channels" IEEE Transactions on Wireless Communication, vol.7, no.7, pp. 2571-2579, July. 2008.

[18] L.Xiao,Larry J. Greenstein ,Narayan B Mandayam, Wade Trappe, "A Physical-Layer Technique to Enhance Authentication for Mobile Terminals" ," in Proc. IEEE International Conference on Communications, Beijing, China, 2008., pp 1520-1524.

[19] L. Xiao, L. Greenstein, N. Mandayam, and S. Periyalwar, "Distributed measurements for estimating and updating cellular system performance," IEEE Transactions on Communications, vol. 56, pp. 991-998, Jun. 2008.

[20] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "MIMO-assisted channel-based authentication in wireless networks," in Proc. IEEE Conf. Information Sciences and Systems (CISS), Mar. 2008, pp.642–646.

[21] Yu, P.L.; Baras, J.S.; Sadler, B.M, "Multicarrier Authentication at the Physical Layer," in Proc. IEEE International Conference on Wireless, Mobile and Multimedia Networks, 2008., pp 1-6.

[22] Xiawen Xiao, Lie Ding, Nanrun Zhou, "An Improved Mechanism for Four-Way Handshake Procedure in IEEES02.11i," in IEEE International Conference on Computer Science and Information Technology., 2010. pp. 419-422.

[23] Byounghoon Kim , Sungwoo Tak, "A Communication Framework supporting Cross-Layer Design for Wireless Networks," in Proc International Symposium on Ubiquitous Multimedia Computing, 2008, pp. 232-237.

[24] Jitendra K Tugnait ,Hyosung Kim, "On Channel-Based Authentication for Mobile Terminals," in Proc. Forty-Third Asilomar Conference on Signals, Systems and Computers, 2009, , pp. 967-971.

[25] N. Gatsis, A. Ribeiro, and G. B. Giannakis, "Cross-layer optimization of wireless fading ad-hoc networks," in Proc. IEEE Int. Conf. Acoustics,Speech, and Signal Processing, Taipei, Taiwan, Apr. 2009, pp. 2353– 2356.

[26] Di Renzo, M.; Debbah, M., "Wireless physical-layer security: The challenges ahead" International Conference on Advanced Technologies for Communications, 2009.pp. 313 – 316.

[27] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Channel-based detection of Sybil attacks in wireless networks," IEEE Transactions on Information Forensics & Security , vol.04,no.03,pp. 492-503,Sept.2009.

[28] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Channel-based spoofing detection in frequency-

selective Rayleigh channels," IEEE Transactions on Wireless Communications, vol.8,no.12,pp. 5948 - 5956.Sept.2009.

[29] Harrison, W.K.; Almeida, J.; Klinc, D.; McLaughlin, S.W.; Barros, J., "Stopping sets for physical-layer security ," in IEEE Information Theory Workshop, 2010, pp. 1-5.

[30] M. Tahir, Sigit P.W Jarot and M.U Siddiqi, "Wireless Physical Layer Security Using Channel State Information," in International Conference on Computer and Communication Engineering, May 2010. pp. 1-5.

[31] Tommaso Melodia and Ian F. Akydildiz, "Cross-Layer QoS-Aware Communication for Ultra Wide Band Wireless Multimedia Sensor Networks," IEEE J. Sel. Areas Commun., vol. 28, no. 5, pp. 653–663, June. 2010.

[32] Suhas Mathur, Alex Reznik,Rajat Mukharjee, Akbar Rahman ,Yogesh Shah,Wade Trappe and Narayan Mandayam , "Exploiting the Physical Layer for Enhanced Security," IEEE Trans. On Wireless Comm., vol. 17, no.5, pp. 71-80, October.2010.

[33] Kai Zeng,Kannan Govindan and Prasant Mohapatra"Non-Cryptographic Authentication and Identification in Wireless Networks," IEEE Journal On Wireless Comm., vol. 17, no.5, pp. 56-62, October.2010.

[34] Anand Sharma,Vibha Ojha, S.K.Lenka, "Quaantam Key Distribution in WLAN 802.11 Networks," in International Conference on Networking and Information Technology., 2010. pp. 402-405.