Research of Trusted Authentication in Wireless Mesh Networks

Zhai Peng
Department of Computer Science and Technology
University of Jining
Qufu, China
e-mail: sinomcse@hotmail.com

Cao Manman
Department of Computer Science and Technology
University of Jining
Qufu, China
e-mail: zbzx@jnxy.edu.cn

Zhang Liping
Department of Computer Science and Technology
Shandong Yankuang Technician Institute
ZouCheng, China
e-mail: 6232908@qq.com

Han Ke
Department of Information
LiaoCheng City People's Hospital
LiaoCheng, China
e-mail: Hanke@hotmail.com

***Abstract*—WMNs (Wireless Mesh Networks) are a new wireless broadband network structure based completely on IP technologies and have rapidly become a broadband access measure to offer high capacity, high speed and wide coverage. WMN is such a network that doesn't need to rely on fixed infrastructure and is operated over an open, wireless medium. Any user within the covered area of radio wave may access the network. Therefore, authentication for network access is the first line of defense that can prevent unauthorized users from accessing the network. An authentication scheme is thus a key mechanism to ensure secure access. In this paper, we propose a trusted authentication protocol based on Trusted Platform Module (TPM) in which the validity of both the user and the terminal device is verified. Thus, only trusted terminals used by legal users are allowed to access a WMN.**

Keywords- Wireless mesh network; Trusted Authentication; network security;Key cryptography

I. INTRODUCTION

Wireless Mesh Network (WMN) is becoming a hot topic in the research of wireless networks. WMN is a special form of mobile AD HOC network, a new broadband wireless network architecture, and an integration of wireless local area network (WLAN). The WMN technology can be acted as "the last mile" in the communications network, wireless metropolitan area networks, wireless sensor networks, and wireless LAN network. WMN integrates various existing wireless technologies, such as the IEEE 802.11 WLANs[1], IEEE 802.16 Broadband WMANs[2], the IEEE 802.15 WPANs[3], and even cellular phone network. Via WMN technology, the mobile user can connect to the Internet to enjoy the service at any time, from any location. Due to WMN has fixed and sufficient power backbone routers, the issue of mobility and energy consumption is less to consider. In order to allow WMN become an important extension of the wired network or even to replace part of the cable network, improving network communication capacity and communication quality[4,5,6], and providing safe access scheme are WMN research required to solve. The large WMN requires a large number of keys, how these keys are securely generated, updated and revoked is a very complex and difficult problem. It is very important to design a safe WMN authentication model that is responsible for the mobile nodes accessing, identification authentication and key distribution [7,8,9,10,11].

Security is a crucial and urgent problem in WMN as in other types of networks. In a wired network, data are transmitted to its destination through electric cables, so leakage can happen only when the physical links are under attack. In a wireless network, data are transmitted through an open space and any node in the coverage can receive the radio signals. Moreover, in WMN, the external environment can be more serious due to the lack of central administration. Therefore, malicious attacks are more difficult to detect and the credibility of wireless nodes must also be guaranteed. Before a user accesses WMN, the network must verify the user's identity and determine the relevant permissions[12][13,14]. Only users and terminals that are successfully authorized are permitted to access the network and network resources. Access authentication in WMN is thus the foundation for secure and reliable communication between wireless nodes.

In this paper, we propose trusted authentication protocols based on TPM in which not only the user's validity but also the terminal device's validity is verified. Thus, only a trusted terminal belonged to a legal user is allowed to access a WMN.

II. RELATED WORK

Past practice of information security has demonstrated that most security problems result not from the network but more from terminal nodes. The original idea of trusted computing was proposed to ensure the security of network terminals. After years of development, from Trusted Computing Platform Alliance (TCPA) in 1999 to Trusted

© 2014. The authors - Published by Atlantis Press

Computing Group (TCG) in 2003[15,16], a series of technical specifications such as Trusted Platform Module (TPM), Trusted Storage, etc. have been proposed.

Trusted computing is used to guarantee the security of an entire computer system. First, a root of trust is assured to construct a chain of trust from the root to the hardware platform to the operation system and then to applications. Trust can thus be established for the entire system through graded authentications and trusts. Together with the BIOS, a TPM forms the root of trust which contains one or more Platform Configuration Registers (PCRs) that allow a secure storage and reporting of security relevant metrics. TPM can be used to authenticate hardware devices. Since each TPM chip has a unique and secret RSA key burned in when it is produced, it is capable of performing platform authentication. For example, it can be used to verify that a system seeking access is the expected system [17]. Each TPM has its own Attestation Identity Keys (AIKs) within a valid certificate CertAIK issued by its producer.

The Trusted Network Connect (TNC) architecture based on trusted computing technologies establishes connections from the viewpoint of the integrity of the terminals in which there are three types of entities: access requestor (AR), policy enforcement point (PEP) and policy decision point (PDP) [18]. The basic concept is that the embedded TPM's information of wireless devices must be checked first and only those that meet the security policy of the network can be allowed to access the network. So a terminal with potential threat cannot access the network directly. At the same time, a terminal can verify its associated AP's security and would only connect to a network that satisfies its security demands. We assume a zone-based hierarchical network model for WMN in this paper as shown in Fig. 1 in which dashed and solid lines indicate wireless and wired links, respectively [19].

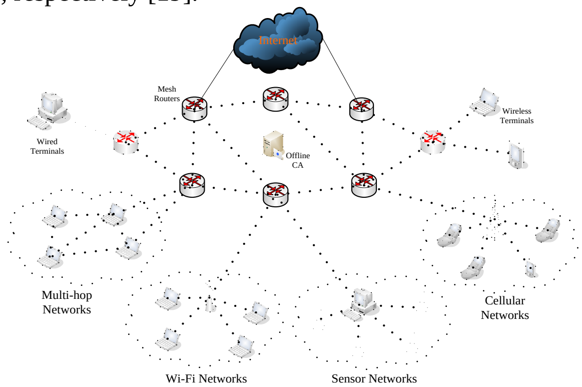

Figure. 1 The Hierarchical WMN Model

III. KEY CRYPTOGRAPHY

A. Certificate

To achieve better security, key pair generation and key agreement protocol adopted in this paper are all based on Elliptic Curve Cryptography (ECC) because ECC offers security comparable to others while with smaller key sizes and faster computation speed.

All cryptography is built on a suitably chosen elliptic curve E defined over a finite field Fq of characteristic p and a base point $P \in E(Fq)$. As described in [20], some domain parameters are defined as follows:

(1) A field size q, where q is a prime power (in practice, either $q = p$, an odd prime, or $q = 2^m$);

(2) An indication FR (field representation) of the representation used for the elements of Fq;

(3) Two field elements a and b in Fq which define the equation of the elliptic curve E over Fq (e.g., $y^2 =x^3+ax+b$ when $p > 3$ and $y^2+xy=x^3+ax^2+b$ when $p = 2$);

(4) A finite point $P = (x_P , y_P)$ of prime order in $E(Fq)$ and $P \neq O$ where O denotes the point at infinity;

(5) The order n of the point P with $nP=O$ and $n > 2^{160}$ as commonly recommended;

(6) The cofactor $h = \#E(Fq)/n$ where $\#E(Fq)$ denotes the number of Fq-rational points on E.

Given a valid set domain parameters (q, FR, a, b, P, n, h), an entity A's private key is an integer $w_A \in_R [1, n-1]$, while its public key is the point $W_A =\omega_A P$. A's public-key certificate, represented as $Cert_A$, contains a string of information that uniquely identifies A (such as A's name and address), its public key $W_{A,}$ the domain parameters if these are not known from context and a certifying authority CA's signature over this information. Any other entity B can use his authentic copy of the CA's public key, which should be broadcasted within the whole network, to verify A's certificate, thereby obtaining an authentic copy of A's public key. In all protocols proposed in this paper, every entity should acquire a valid certificate from the offline CA before accessing the network.

B. Key Agreement

Two entities A and B can complete the key agreement with their key pair (w, W) as follows:

(1) A selects $r_A \in_R [1, n-1]$, computes the point $R_A=r_AP$, and sends R_A to B;

(2) B selects $r_B \in R[1, n-1]$, computes the point $R_B=r_BP$, and sends R_B to A;

(3) A validates R_B whether R_B is not equal to O, R_B satisfies the equation of E, and x_B, y_B are elements in the Fq or not. If the validation fails, then A terminates the protocol run with failure. Otherwise, A computes $s_A=(r_A+R_Aw_A)$ mod n and $K=hs_A(R_B+R_BW_B)$. If $K=O$, then A terminates the protocol run with failure.

(4) B does the same validation above. And if it fails, then B terminates. Otherwise, B computes $s_B=(r_B+R_Bw_B)$ mod n and $K=hs_B(R_A+R_AW_A)$. If $K=O$, then B terminates.

(5) The session key is the point K.

We can see that, $K= hs_A(R_B+R_BW_B)= hs_B(R_A+\mathrm{R_AW_A})=h (r_Ar_B+r_Aw_BR_B + r_Bw_AR_A + w_Aw_BR_AR_B) P$.

IV. Trusted Authentications

A. Backbone Router

Before accessing the network, a new mesh router BR_A is supposed to have a valid certificate $Cert_A$ issued by the offline CA. In order to get the private key *SK* of the system, it needs to be authenticated by at least *t* routers and get their key pieces. As in TNC architecture, the existing backbone router BR_B plays a role as the PEP and PDP, while BR_A is an AR.

There are five steps to accomplish an authentication as illustrated in Fig. 2:

(1) BR_A sends an access request to BR_B.

(2) BR_B replies with a challenge N_B to BR_A, which uses a CRM (Challenge/Response Mechanism).

(3) BR_A encrypts N_B with its private key ω_A as a response, and sends N_A as a new challenge for mutual authentication; $Plat\text{-}vert_A{=}SML_A||\{PCR_A||N_A\}_{AIK,A}||CERT_{AIK,A}$, where SML(Storage Measure Log), PCR and CERT $_{\text{AIK,A}}$ is used to ensure BR_A's platform authentication and integrity verification; $Cert_A$ combined with BR_A's challenge response $\{N_B\}_{\omega A}$ is used to authenticate the identity of BR_A's user. $Sig_A()$ is used to ensure the integrity of the message.

(4) After receiving the message, BR_B verifies both $Cert_A$ as well as $Plat\text{-}vert_A$ to ensure that BR_A is valid under the network's current security policy. Only when both verifications are successful, will BR_B send back its key piece $\{SK_B\}_{WA}$ along with its *Plat-vertB*, *CertB* and challenge response $\{N_A\}_{\omega B}$ to BR_A.

(5) After receiving the message, BR_A will do the same verifications as BR_B did. If successful, BR_A will get SK_B using its private key ω_A.

And after gathering at least *t* key pieces, BR_A can now reconstruct the private key *SK* of the network and access the network.

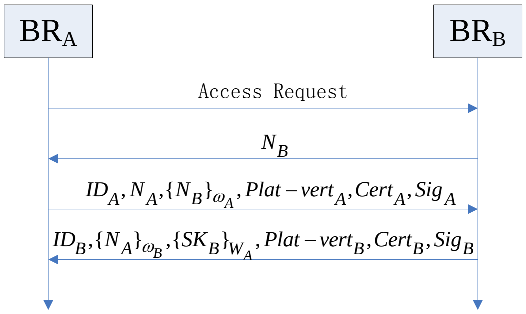
BR_A
BR_B
Access Request
N_B
$ID_A, N_A, \{N_B\}_{\omega_A}, Plat-vert_A, Cert_A, Sig_A$
$ID_B, \{N_A\}_{\omega_B}, \{SK_B\}_{W_A}, Plat-vert_B, Cert_B, Sig_B$

Figure.2 Interactions of Backbone Router's Authentication

.

B. Access Point

Unlike the backbone mesh routers, an ordinary AP in zone networks should not get the private key SK of the backbone network. Instead, it can communicate with a border mesh router, and shared a temporary session key with the router. Two entities AP and BR can complete the key agreement with their key pair (w, W) in their certificates, as described in the section "Key Agreement".

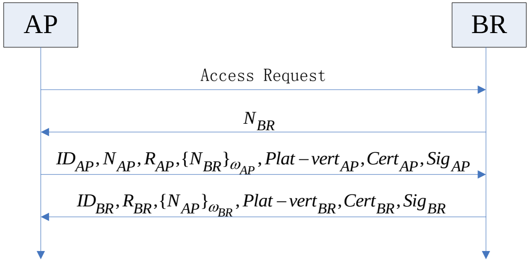
AP
BR
Access Request
N_{BR}
$ID_{AP}, N_{AP}, R_{AP}, \{N_{BR}\}_{\omega_{AP}}, Plat-vert_{AP}, Cert_{AP}, Sig_{AP}$
$ID_{BR}, R_{BR}, \{N_{AP}\}_{\omega_{BR}}, Plat-vert_{BR}, Cert_{BR}, Sig_{BR}$

Figure.3 Interactions of AP's Authentication

As in TNC architecture, the border mesh router BR plays a role as the PEP and PDP, while AP is an AR. When they finish the interaction as illustrated in Fig. 3 and exchange RAP and RBR, the AP and BR can share the session key to be used in their next communication.

C. Roam and Handoff

When a terminal switches a handoff from one zone network to another, or requests a roam service in a foreign zone, compatibility of security policies between different zones or between foreign and home zone needs to be considered. If they are compatible, then the handoff or roam can be processed smoothly. Or else, they must start a negotiation first. For example, a normal personal laptop cannot easily move from his LAN to a high secure military zone.

V. Simulation Results and Discussions

Contrast simulations between the protocol TA (Terminal's Authentication) we proposed and TWMAP proposed in [21,22] are carried out using the simulating software OPNET 10.5A under Windows XP.

We carry out 50 simulations in total, in which the number of requesting terminals increases from 1 to 50 in 0.5 second. Through the simulations, we compare (1) the success ratio of authentication which is the number of terminals successfully access the network divided by the total number of requesting terminals in Fig.4 and (2) the average delay of authentication which is the total authentication time divided by the successful number in Fig5.

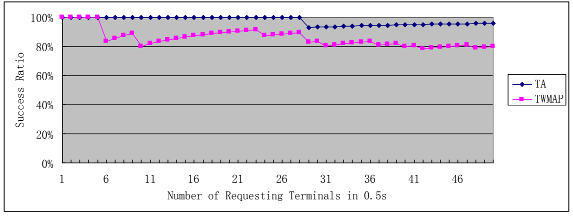

Figure. 4 Success Ratio of Two Protocols

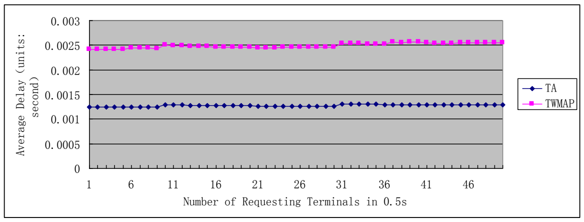

Figure. 5 Average Delay of Two Protocols

We can see that, in both success ratio and average delay, the TA protocol is better than MN-TAP. Since there are more interactions between the PEP and PDP in MN-TAP, it brings a much longer authentication time and a smaller success ratio.

VI. Conclusion

Authentication in wireless networks is very important, which usually is viewed as the first defense of the network. Trusted authentications in WMNs are proposed in this paper based on several technologies, such as hierarchical network model, ECC, (*t*, *n*) threshold cryptographic method, and TPM.

Because of its volatile topology and the characteristics of multi-hop in WMN, authentication success rate is not high enough, and authentication delay is long. In later work, according to its characteristics of WMN, we should increase the success rate and reduce the authentication delay, and provide some valuable results to security research of WMN. Moreover, trusted handoff and roaming in WMNs will be paid more attention to improve our protocol.

Acknowledgment

We thank our college for providing us the practical equipment, so we can do experiment and simulation which tests our model and improve its performance concisely. This work was financially supported by the third batch science and technology plan fund of the education department of Shandong province(J08LJ56) "network measurement research based on network behavior"and "Researches on Ipv4/v6 Internet Measurement Based on User Behaviors" of the Jining University science and technology development project.

References

[1] IEEE 802.11 WG. IEEE Standard 802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. 1999.

[2] IEEE 802.16 Standard Group. IEEE 802.16 TM: Broadband Wireless Metropolitan Area Networks[EB/OL]. http://standards.ieee.org/getieee802/802.16.html, Nov,16,2012.

[3] IEEE 802.15 Standard Group. IEEE 802.15 TM: Wireless Personal Area Networks[EB/OL]. http://standards.ieee.org/getieee802/802.15.html, Nov,16,2012. Proceedings, The 2nd International Conference on Information Technology and Computer Science.423

[4] Shamir Adi. "How to Share a Secret". Communications of the ACM, ACM, vol. 22, no.11, pp. 612-613, 1979.

[5] Blakley G R. "Safeguarding Cryptographic Keys", In Proceedings of the National Computer Conference, pp. 313-317, 1979.

[6] Desmedt Yvo, Jajodia Sushil, "Redistributing Secret Shares to New Access Structures and Its Application"[EB/OL]. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.55.2968, 1997.

[7] Wong Theodore M, Wang Chenxi, Wing Jeannette M. "Verifiable Secret Redistribution for Archive Systems", In Proceedings of the 1st International IEEE Security in Storage Workshop, pp. 94-105,2009.

[8] Feldman Paul. "A Practical Scheme for Non-interactive Verifiable Secret Sharing". In Proceedings of the 28th IEEE Annual Symposium on Foundations of Computer Science, pp.427–437,2011.

[9] Kim Jongtack, Bahk Saewoong. "Design of Certification Authority Using Secret Redistribution and Multicast Routing in Wireless Mesh Networks". Computer Networks, Elsevier, vol. 53, no.1, pp.98–109, 2009.

[10] Zhu Haojin, Lin Xiaodong, Lu Rongxing, Pinhan Ho, Xueming Shen. "SLAB: Secure Localized Authentication and Billing Scheme for Wireless Mesh Networks". IEEE Transaction on Wireless Communications, IEEE, vol.7, no.10, pp.3858–3868, 2008.

[11] Cao Zhenfu, Zhu Haojin, Lu Rongxing. "Provably Secure Robust Threshold Partial Blind Signature", Science in China Series F: Information Sciences, China Science Press, vol. 49, no.5, pp. 604–615, 2006.

[12] Mike Boneh. "Building intrusion tolerant applications", In Proceedings of the 16th USENIX Security Symposium in Washington, pp. 79-91, 2010.

[13] Jing Ji Wu, Tian Yang Zhou. "Intrusion Tolerance Technology on the Internet", Journal of Graduate College of China Science Institute, University of China Science Institute Press, vol.18, pp,119-123, 2010.

[14] Chai Zhenchuan, Cao Zhenfu, Lu Rongxing. "Threshold Password Authentication against Guessing Attacks in Ad hoc networks", Ad Hoc Networks, Elsevier, vol.5, no.7, pp.1046- 1054,2007.

[15] Dong Xiaolei, Wang Liheng, Cao Zhenfu. "EP2DF: an Efficient Privacy-preserving Date- forwarding Scheme for Service-oriented Vehicular Ad Hoc Networks", IEEE Transactions on Vehicular Technology, IEEE, vol.60, no.2, pp.580-591, 2011.

[16] Burrows M, Abadi M, Needham R. Logic of Authentication. ACM Transactions on Computer Systems, 1990, (8):18-36.

[17] TPM:http://en.wikipedia.org/wiki/Trusted_Platform_Module

[18] Zhang Huan-Guo, Chen Lu, Zhang Li-Qiang, "Research on Trusted Network Connection", Chinese Journal of Computers, v 33, n 4, p 706-17, April 2010

[19] Akyildiz, I.F, Xudong Wang, Weilin Wang, "Wireless mesh networks: a survey", Computer Networks, v 47, n 4, p 445-87, 15 March 2005

[20] Fu YF, He JS, Wang R, Li GR. Mutual authentication in wireless mesh networks[C]. Proc.2008 IEEE International Conference on Communications 2008; 2606-2610

[21] L. Law, A. Menezes, et al., "An efficient protocol for authenticated key agreement", Designs, Codes and Cryptography, Vol. 28, No. 2, March 2003, pp 119-134.

[22] Y. Dai, C. Ma and Y. Yang, "Threshold secret sharing based on Lagrange insert value," Journal of Beijing University of Posts and Telecommunications, Vol. 27, No. 2, April 2004, pp. 24-28.