An Efficient Authentication Protocol for Wireless Mesh Networks

Peng Zhai[1,2], Jingsha He[1,3], Nafei Zhu[1,*], Peng He[3] and Yao Liang[4]

[1]*Faculty of Information Technology, Beijing University of Technology, Beijing, China*
[2]*Department of Computer Science, Jining University, Jining, Shandong, China*
[3]*College of Computer and Information Science, China Three Gorges University, Yichang, Hubei, China*
[4]*Department of Computer and Information Science, Indiana University-Purdue University Indianapolis, Indianapolis, IN, USA*
E-mail: znf@bjut.edu.cn
[*]*Corresponding Author*

Received 15 September 2020; Accepted 21 October 2020;
Publication 26 December 2020

Abstract

In a wireless mesh network (WMN), how to guarantee safe access to sensitive information has been an issue under research partly because of various hidden attacks and attack vectors. As a network with no need to depend on a fixed infrastructure, WMN is operated over an open and wireless medium. Every user accessing to radio wave may access to the network. Hence, as the first line of defense, authentication for network access can stop illegal users from visiting the network. As an essential mechanism, an authentication program ensures safe access. A reliable handoff protocol on basis of some technologies is put forward in this paper, examples include classical hierarchical network model, Elliptic Curve Cryptography, Strategy evaluation and trust evaluation. The authentication protocol is on basis of Trusted Platform Module (TPM) where the validity of users and terminal devices are verified. Therefore, only reliable terminals applied by legal users can access to a WMN. According

Journal of Web Engineering, Vol. 19_7–8, 1193–1212.
doi: 10.13052/jwe1540-9589.197812

to numerical analysis and simulation outcomes, the switchoff authentication protocol proposed greatly overcomes other authentication protocols with regard to the ratio of authentication success and authentication delay.

Keywords: Wireless mesh network, trusted authentication, network security, key cryptography.

1 Introduction

As a new technique of wireless networks used to set up commercial wireless mobile networks, wireless mesh network (WMN) shall get rid of the restrictions from wireless metropolitan area networks (WMANs), wireless local area networks (WLANs), and wireless personal area networks (WPANs) [1, 2]. By combining with the merits of providing Ad Hoc and Wireless local area networks, WMNs become an increasingly efficient wireless network access approach can offer large capacity, large bandwidth and extensive coverage as a structure of wireless broadband network fully on basis of IP technologies. In some ways, WMNs are characterized by self-organization, decentralized, multiple hops routing and perfect routing, as a network design idea [3]. Security is an important and urgent issue in WMN like other kinds of networks. In a cable network, because data is transmitted to its destination via electric cables, leakage will appear only if physical links are attacked. In the WMN wireless network, information transmission is carried out through the open network, and every covered node is able to receive radio signals. In addition, the external environment will be more dangerous in WMN because of the short of central management. Hence, it is very difficult to detect malicious attacks, and it is necessary to guarantee the credibility of wireless nodes. Before accesses to WMN network, the user's identity must be verified and then determined the relevant permissions [4]. Only authorized users and terminals are allowed to access the network resources. Therefore, access authentication in WMN acts as the basis for safe and credible communication among wireless nodes [5, 6]. Besides, safe access authentication acts as the important gateway preventing malicious behave to unauthorized network access to information [7]. For the switch-over in Wireless Mesh Network, mobile nodes are required to finish access identification within a short delay and play a role in protecting the mobile nodes and the switch-over network [8].

According to the previous practices in the fields of information security, the majority of security problems are from the network terminal nodes [9–13].

Therefore, the trusted computation originally aims to guarantee the safety of network terminals. this paper puts forward the reliable authentication protocols on basis of TPM where both the user's validity and the terminal device's validity are verified. The authentication protocol is on basis of the Trusted Platform Module (TPM) where both the user and the terminal device are verified. Therefore, only reliable terminals applied by legitimate users are permitted to access to a WMN. According to numerical analysis and simulation outcomes, the switchover authentication protocol put forward greatly exceeds other authentication protocol with regard to authentication success ratio and authentication delay.

For the paper, the rest part is organized below. In Section 2, several work of switch protocols in WMNs is reviewed. Section 3 describes the network model applied in the proposed authentication protocol. Section 4 introduces key cryptography and related knowledge. Section 5 discusses Group Key Management. The authentication protocols are displayed in Section 6. In chapter 7, the performance of the authentication protocol is evaluated and validated. In the end, Section 8 summarizes the research contents of this paper and makes a prospect for the future research.

2 Related Work

You and Xie [14] proposed an architecture based on the multi-linear Diffie-Hellman key random exchange protocol [15]. Matsumoto and Diffie [16, 17] put forward the programs of setting up keys on basis of the fundamental Diffie-Hellman key bidirectional exchange protocol [18]. Girault et al. [19] further improved and validated this method. In these studies, different random Numbers are usually exchanged between the two parties communicating on the network for identification and verification. In addition Chatterjee [20], Shi and Gong [21] use the famous ECC constructions to put forward various methods to mutually verify the nodes with each other. The protocol ISA [22] put forward by Li solves the safe key management issue of the WMNs by utilizing EC-IBC. In another aspect, Zhou and Hass [23] put forward a protocol of setting up keys on basis of the traditional public key infrastructure where the effect of the Certification Authority (CA) is shared by a set of nodes through applying ThSS. In their program, any certificate partially signed by k server can be applied to set up a signed certificate similar to a CA-signed certificate. Chai et al. [24] put forward identical methods where the certificate generated by the RSA algorithm is distributed by the certificate Authority node to all nodes in wireless network. Gharib and Moradlou [25] studied

how to distribute private keys generated by the ECC algorithm through a central node authorization authority [23–25] studied authentication private key certificates generated and distributed through TTP.

According to the past practices of information safety, the majority of security problems are from terminal nodes instead of the network. The trusted computation was naturally to guarantee the safety of network terminals. After several years of growth, a lot of technical instructions such as Trusted Platform Module (TPM), Trusted Storage, etc. have been proposed [27] from Trusted Computation Platform Alliance (TCPA) in 1999 to Trusted Computation Group (TCG) in 2003 [26].

Xiao et al. [28] put forward TPM and TNC authentication models, also known as Trusted Platform Module and the Trusted Network Connect, and proposed an authentication protocol based on this research. Users can visit the network normally when the successful measurement of their trust, and their integrity including software, hardware, running systems and shared database is validated. The computing cryptographic chip is integrated into the hardware device, the TPM module is carried out. The access to encryption chip is guarded, and only the TPM can use TPM commands to directly access to the data stored and functions. During the boot, the system measures the consistency of the experimental platform and verifies the setup information and configuration parameters by generating some hash values. The TNC sets up connections on basis of the configurations kept in Trusted Platform Module. Nevertheless, only certification platforms with approved configurations satisfying the safety wireless network demands will be taken into account. The safety configurations of access point must be taken into account by the client. Nevertheless, the proposed protocol carries out the authentication procedures, examples include Elliptic Curve Cryptography algorithm, the system private key, and the public key agreements by utilizing cryptographic methods requiring intensive computations.

In wireless networks, an effective and robust handoff authentication on basis of identity was put forward with a special kind of complex hash function as the network system key [29]. By comparing with other existing identity-based switchoff programs, the program mainly has the advantage of removing the conception that the PKG (private key generator) must be completely reliable, which more safety and simple configuration. Nevertheless, the program is more appropriate for the WMN networks because there may not be any PKG in a more complex environment in a multi-hop WMN.

3 Authentication Methods

3.1 TPM and TNC

The safety of a complete computer system is guaranteed by utilizing trusted computation. First of all, it is assumed that a root of trust constructs a trust chain from certificate root of the hardware device platform for running system processes and then applications. Therefore, certification can be set up for the complete system by graded identifications and trusts. A TPM forms the root of trust which includes one or more Platform Configuration Registers (PCRs) [30] that permit a safe storage and report of relevant security metrics with the BIOS. Changes to previous configurations are detected by applying these metrics, and decisions on how to proceed are produced. In the meantime, hardware devices can be authenticated by TPM. With a RSA key stored in TPM memory is able to perform platform authentication. For instance, whether a system seeking access is the expected system can be verified. Own Attestation Identity Keys (AIKs) is owned by each TPM within a valid certificate CertAIK issued by its producer.

The Trusted Network Connect (TNC) architecture on basis of trusted computation technology sets up associations from the perspective of the integrity of the terminals with policy decision point (PDP), policy enforcement point (PEP) and access requestor (AR) [31]. According to the fundamental concept, it is necessary to check the embedded TPM's information of wireless equipment first, and only those satisfying the security policy of wireless network that can be permitted to visit the network. Therefore, the client device with hidden danger is not permitted to visit the authentication network directly. In the meantime, a terminal can examine its related AP's security and would only connect to a network satisfying its safety demands. Trusted Network Connect is a dynamic forewarning interactive network communication mechanism and its architecture is displayed in Figure 1.

3.2 The WMN Network Topology Model

Figure 2 shows the zone-based hierarchical WMN network model, in which the wireless link is represented by a dashed line and the wired link by a solid line [32]. The WMN network includes only main network, one or multiple zones, namely, local area networks and several decentralized wired or wireless terminals.

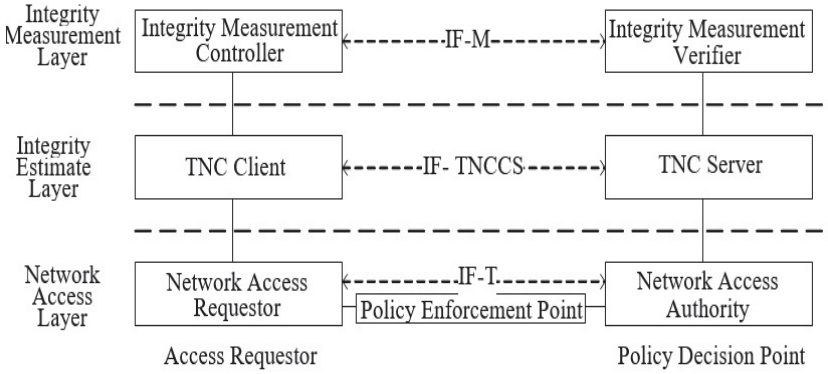

Figure 1 The trusted network connect architecture.

WMN network is a mesh network structure composed of at least two or more routers. This network composed of routers has the capability of self-organizing links, self-repairing and self-configuring. An exclusive database of authorized certificates shared by all major routers in a Certificate Authority (CA). The CA is usually operated and maintained by the Internet Service Providers (ISPs) or other Internet organization. When a new network end user, zone router, or backbone network upgrade is available, the CA begins to work, perform user authentication, and perform user access services [33]. Various types of radio technology can be used to construct the backbone.

Gateways, namely, its border mesh routers are applied to connect each zone to the main network, which integrates mainstream wireless networks, including mobile cellular network, wireless sensor network, Wi-Fi network and so on. Every wireless network zone, there is at least an Access Point (AP), namely, mobile node connecting to the main network such as microwave towers and Mesh Access Points (MAPs) are in the multi-hop networks and cellular networks respectively. Because these Access Points can use various the radio technologies which need to be supported by the backbone border routers. In the WMN Zone network, a variety of user information is stored in the database, usually including user name, user ID, network name, network ID, authentication password and other information value. The Network terminals can idle about from one to another zone or switch from one to another AP in the same or various zones.

Ethernet links can be used to connect traditional terminals to mesh routers regardless of wired or wireless. For traditional terminals with the same radio technology as the mesh routers, mesh routers can be communicated with directly. In case of applying various radio technology, terminals must interact

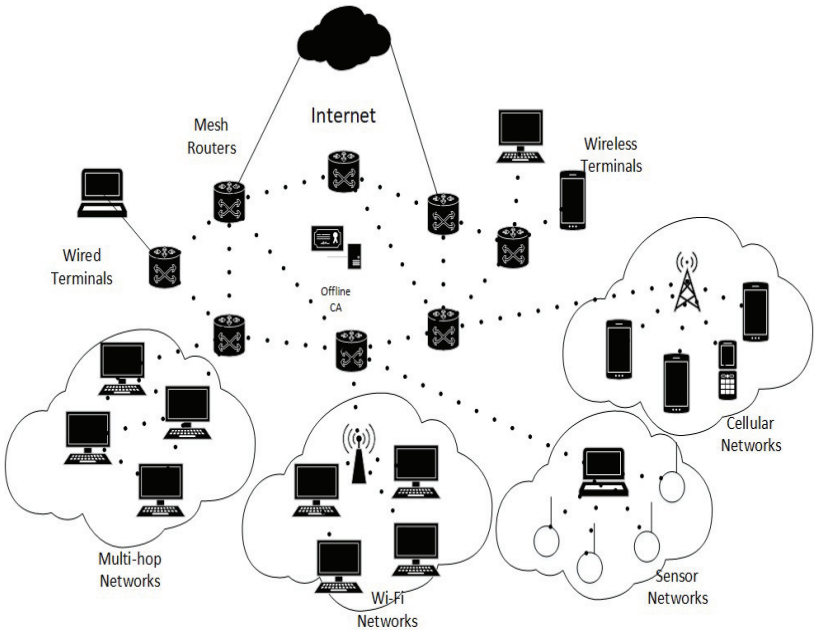

Figure 2 The WMN network model.

with AP in a zone with Ethernet connections to mesh routers. In particular, mesh terminals can visit the network through mesh routers and provide routing capabilities for improved connectivity and coverage by connecting directly to other WMN wireless network terminals.

It is assumed that the communication among terminals in a zone network is made within a relatively shorter scope, and the communication among terminals in a main network is made within a relatively longer scope; the communication efficiency in the main network is much higher than that in the WMN wireless network. In order to construct a trusted network, all devices including backbone routers, APs and terminals should have a TPM in it and each TPM should have its own AIKs with a valid certificate CertAIK issued by its producer.

3.3 Key Cryptography

Certificate: Authentication key generation and key exchange protocols on basis of ECC is adopted in this paper because ECC provides other schemes such as RSA with the smaller key storage space, faster computing speed, higher security level [34].

Cryptography is set up on a appropriately selected elliptic curve E which is defined in a finite field Fq of characteristic p and a base point $P \in E(Fq)$. An integer m meeting $Q = mP$ is sought by the ECDLP (elliptic curve discrete logarithm problem) on $E(Fq)$, while P and Q are brought, which displays an NP-hard intractability problem. According to [35], the definition of some domain coefficients is shown below:

1. The field size q, where q refers to a prime power (in reality, either $q = p$, or odd prime, $q = 2^m$).
2. The instruction *FR* (field representation) of the representation applied for the elements of F_q.
3. a and b in F_q defining the equation of the elliptic curve E over F_q (e.g., $y^2 = x^3 + ax + b$ in the case $p > 3$, and $y^2 + xy = x^3 + ax^2 + b$ in the case $p = 2$).
4. Point $P = (x_P, y_P)$ of the prime order in $E(Fq)$ and $P \neq O$ where the point at infinity is denoted by O;
5. The order n of the point P with $nP = O$ and $n > 2^{160}$ as widely recommended;
6. A cofactor $h = \#E(F_q)/n$ where the number of the F_q rational points on E is denoted by $\#E(F_q)$.

Given an effective set system parameters (p, SK, a, c, Q, m, h), the private key of an entity A is an integer $w_A \in_R [1, n-1]$, while the public key stands for the node $W_A = \omega_A P$. Node A's certification public-key, expressed as $Cert_A$, contains a series of information uniquely identifying A (such as *node* name, location etc), the public key W_A, the system coefficients if the context and a WMN network CA's user signature over the message does not show it. Any other entity B can verify A's client certificate by using his authentic copy which shall be broadcast within the whole network of the CA's public key, so as to obtain Node A's public key authentication copy. All protocols put forward a valid certificate from the offline CA shall be obtained by every entity access to network information resources before.

Two nodes P and Q can finish key exchange:

P chooses $x \in R[1, n-1]$, calculates point $RA = xP$ and sends R_A to B.

Q chooses $y \in R[1, n-1]$, calculates point $R_B = yP$ and sends R_B to A.

The process key is the node $KS = yRA = xRB = xyP$.

In this paper, Elliptic Curve Cryptography (ECC) algorithm is mainly used in key protocol and key pair generation to achieve more efficient and

safe purposes. Because ECC provides others with security comparable while with smaller keystore space and faster validation computations.

Secret Agreement Method: *A* and *B*, two entities can finish the key protocol with key pair (*p, Q*) as follows:

1. *R* chooses $r_A \in_R [1, n-1]$, calculates the node $R_A = r_A P$, and sends R_A to B;
2. *A* chooses $r_B \in R[1, n-1]$, calculates the node $R_B = r_B P$, and then return R_B to R;
3. *R* validates R_B whether R_B is not equal to W, R_B meets the equation of E, and x_B, and y_B are the elements in the Fq. In case of failed validation, *A* will terminate the failed protocol. Otherwise, R calculates $s_A = (r_A + R_A w_A) \bmod m$ and $K = hs_A(R_B + R_B W_B)$. If $R = Q$, then R terminates the failed protocol.
4. *B* makes the same validation above. Meanwhile, in case of failed validation, *B* will terminate the protocol. Otherwise, *S* calculates $s_B = (r_B + R_B w_B) \bmod n$ and $K = hs_B(R_A + R_A W_A)$. If $K = O$, B will terminate the protocol.
5. The point *K* with procedure key.

We can see that, $K = hs_A(R_B + R_B W_B) = hs_B(R_A + R_A W_A) = h(r_A r_B + r_A w_B R_B + r_B w_A R_A + w_A w_B R_A R_B)P$.

3.4 Group Key Management

Because there is no online center to manage the arbiter or the CA authentication center in the main mesh networks, n WMN routers with greater efficiency will administrate the keys applying the (t, n) threshold cryptographic approach by forming a virtual CA and GKM (Group Key Management). The system 's public key PK is published to all, while the private key SK is partitioned into n pieces SK1…SKn which are distributed to the n chosen routers. Then, SK can be reconstructed by any t out of n routers, while SK can't be reconstructed by any p out of the q routers if $p < t$.

There are three parts in $A(t, n)$ threshold secret sharing approach: system coefficients, key distribution and password reconstruction and management algorithm.

Safety coefficient algorithm: as the secret to share, the definition of private key SK is made in a finite field $KF(q)$ where p stands for greater than SK; dj, as random integers defined in $KF(q), d2, \ldots, dn$ are expressed as the system identification of n clients.

Authentication key distribution method: after selecting a $(n-1)$ degree polynomial $f(x) = a_{t-1}x^{t-1} + \cdots + a_1 x + a_0 modp$ in $KF(q)$ where $a_{t-1}, \ldots, a_1$ refer to different integers and $a_0 = SK$, the key blocks $SK_i = f(d_i)modp$ is calculated and moved to each of the components of the participating operation via safe communications link.

Method of password reconstruction: On basis of Lagrange interpolation polynomial. i coordinates $(d_1, SK_1), (d_2, SK_2), \ldots, (d_t, SK_t)$ can be obtained by the cooperation among any p participants.

$$SK = f(0) = \sum_{i-1}^{t} SK_i \prod_{j \neq i, j=1}^{t} \frac{d_j}{d_j - d_i} modp$$

When at least t key pieces are received by a new participant, the secret key can be reconstructed. But what happens if a wrong key piece comes out? Let us consider the confederate matrix

$$\begin{bmatrix} d_1^{t-1} & \cdots & d_1 & 1 & SK_1 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ d_i^{t-1} & \cdots & d_i & 1 & SK_i \end{bmatrix}$$

We collect more than t pieces, which means $i > t$ in the matrix. If the rank of the matrix is bigger than t, there will be no feasible solution in the matrix, and there is surely at least one wrong key pieces received. If so, another t pieces from different participants must be required.

In a wireless mobile context, one key piece holder can be broken through by an attacker within a limited time, and then another key piece holder will be attacked. For enough long time, t holders may be broken through, t key pieces will be acquired; the shared secret key will be calculated. The updating of every key piece shall be made in a defined cycle, so as to avoid this situation. Only t key blocks are gotten within the same circulation. The security process is reconstructable.

3.5 Trusted Authentications

Backbone Router: Before accessing to the network, it is supposed that a new mesh router BR_A shall have a effective certificate $Cert_A$ issued by the offline CA. Besides, it has to be authenticated by at least t routers and obtain their key blocks, and obtain the privatekey SK of network system. The existing main router BR_B exerts an effect as the PEP and PDP in TNC architecture, while BR_A is an AR.

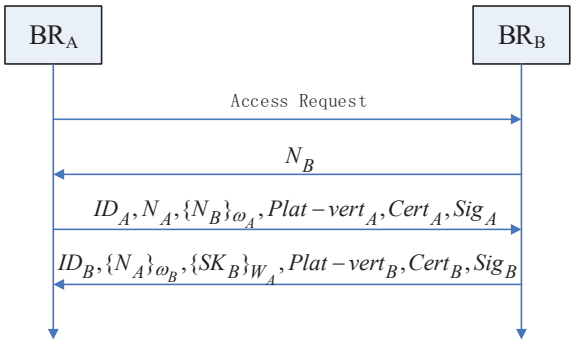

Figure 3 Interactions of backbone router's authentication.

An authentication shall be realized by five procedures as indicated in Figure 3:

BR_A delivers an access request to BR_B.

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

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

After the message is received, both $Cert_A$ and Plat-$vert_A$ are verified by BR_B to guarantee that BR_A is effective under the current safety policy of the network. BR_B will return key block {SKB}WA together with *Blat-vertB*, *CertB* and challenge response {NA}ωB to BR_A only when both verifications are successful.

After the message is received, BR_A will make the same verification as BR_B did. In case of successful verification, BR_A will its private key ωA to obtain SKB.

And after gathering t key blocks, BR_A may reconstruct the privatekey SK of the network and access the network.

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,

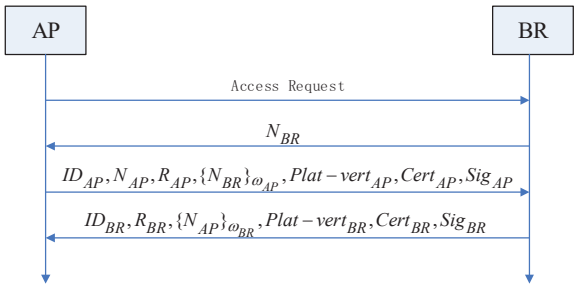

Figure 4 Interactions of AP's authentication.

it can communicate with a border mesh router, and shared a temporary session key with the router. Two entities AP and BR can finish the key protocol with their key pair (w, W) in their certificates according to the description in the section "Key Agreement".

Border mesh router BR exerts an effect as the PEP and PDP in TNC architecture, while AP acts as an AR. When they finish the interaction as illustrated in Figure 3 and exchange RAP and RBR, the AP and BR can share the session key to be applied in their follow-up communication.

Terminal: As depicted in the Section "the Network Model", there are several kinds of terminals in WMN. For those who directly connect to a border mesh router through whatever wired or wireless links, they can access the network in the way as same as an isolated AP, as illustrated in Figure 4.

And for those who must connects the network via an existing AP regardless of what type of zone networks, a three-party authentication with their AP and the border mesh router where the AP has already authenticated before shall be achieved. The existing main router BR exerts an effect as the PDP in TNC architecture, and AP acts as the PEP, while T acts as an AR.

An authentication can be accomplished through seven procedures as indicated in Figure 5:

1. Terminal T delivers its access request to its neighbor AP.
2. AP replies with a challenge NAP to T, which uses a CRM (Challenge/Response Mechanism).
3. T encrypts NAP with its private key ωT as a response, and sends NT as a new challenge for mutual authentication; RT is an integer used for key agreement; T's platform authentication and integrity verification are guaranteed by using Plat-vertT; CertT combined with T's challenge response $\{$NAP$\}\omega$T is used to verify user identity of T's user; the integrity of message is ensured by applying SigT().

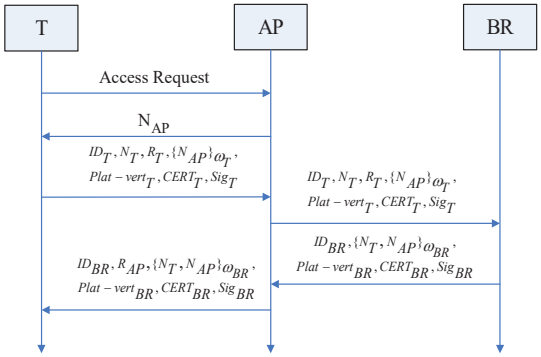

Figure 5 Interactions of terminal's authentication.

4. After the message is received, AP sends it to its related BR for further authentication.
5. After the message is received, BR examines both CertT as well as Plat-vertT to guarantee that T is effective under the current safety policy of the network. BR will send back the challenge response {NT, NAP}ωBR to AP along with its Plat-vertBR, CertBR only when both verifications are successful.
6. After the message is received, AP recognizes T as a valid node, and forwards the message to T along with an integer RAP used for key agreement. And it can calculate the session key with RT.
7. After the message is received, T will make the same verification as BR performed. In case of successful verification, T will obtain the session key with RAP, as described in the Section "Key Agreement".

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 highly secure military zone.

4 Simulation Results and Discussions

Contrast simulations between the protocol TA (Terminal's Authentication) we proposed and TWMAP MN-TAP proposed in [36] are carried out using the simulating software OPNET 14.5 under Windows 10.

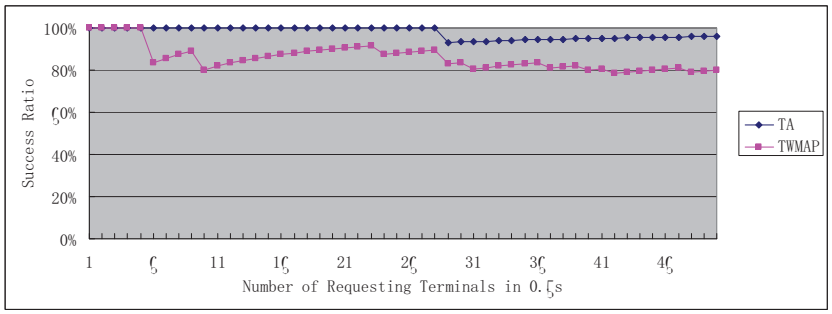

Figure 6 Success ratio of two protocols.

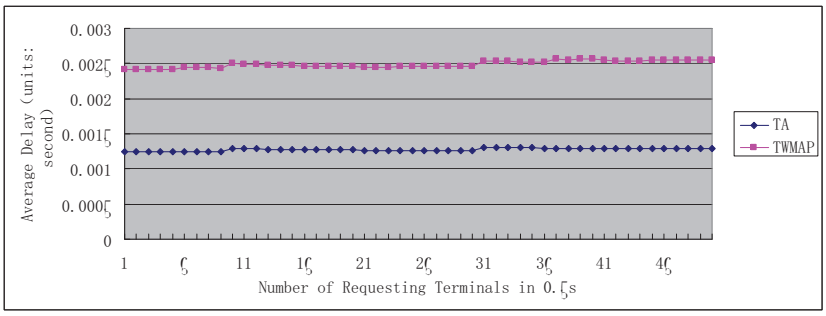

Figure 7 Average delay of two protocols.

We carry out 50 simulations in total, where the quantity of requesting terminals increase from 1 to 50 in 0.5 second. (1) The ratio of successful authentication which stands for the quantity of terminals successfully access to the network divided by the total quantity of requesting terminals in Figure 6 and (2) the average authentication delay which means the total authentication time divided by the successful number in Figure 7 are compared through stimulation.

We can notice 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.

5 Conclusion

Due to the high scalability, convenient access and simple and efficient network structure of WMN network, it becomes a domestic and foreign research

focus with a broad market prospect. This paper puts forward the trusted authentications in WMNs on basis of some technology, such as classical hierarchical network model, ECC, WMN network threshold cryptographic method, and TPM.

Because of the dynamic nature of WMN network nodes and multi-hop network, the network topology is unstable, resulting in long delay of network authentication and low success rate of authentication. In the follow-up work, it is necessary to increase the certification success rate, decrease the authentication delay, and provide security research of WMN with some valuable results. In addition, the authentication method proposed in this paper relies on a trusted authentication center, which brings great hidden danger to system security.With the continuous development of blockchain technology, how to use blockchain decentralization, tamper-proof, traceable and other features to solve WMN network security authentication is the direction of our next research.

Acknowledgements

National Natural Science Foundation of China (61602456) and A Project of Shandong Province Higher Educational Science and Technology Program (J17KA048) have supported the work in this paper.

References

[1] Ma, Z., Ma, J., Moon, S., & Li, X. (2010). An efficient authentication protocol for WLAN mesh networks in trusted environment. IEICE transactions on information and systems, 93(3), 430–437.

[2] Loret, J. S., & Vijayalakshmi, K. (2018). Security enrichment with trust multipath routing and key management approach in WMN. IETE Journal of Research, 64(5), 709–721.

[3] Farash, M. S., Turkanović, M., Kumari, S., & Hölbl, M. (2016). An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment. Ad Hoc Networks, 36, 152–176.

[4] Kumari, S., Khan, M. K., & Atiquzzaman, M. (2015). User authentication schemes for wireless sensor networks: A review. Ad Hoc Networks, 27, 159–194.

[5] Gao,T., Wang, Q., Wang, X., & Gong, X. (2017). An anonymous access authentication scheme based on proxy ring signature for CPS-WMNs. Mobile Information Systems, 201–217.
[6] Chang, C. C., Hsueh, W. Y., & Cheng, T. F. (2016). A dynamic user authentication and key agreement scheme for heterogeneous wireless sensor networks. Wireless Personal Communications, 89(2), 447–465.
[7] Das, A. K. (2017). A secure and effective biometric-based user authentication scheme for wireless sensor networks using smart card and fuzzy extractor. International Journal of Communication Systems, 30(1), 2912–2933.
[8] Guo, P., Wang, J., Geng, X. H., Kim, C. S., & Kim, J. U. (2014). A variable threshold-value authentication architecture for wireless mesh networks. Journal of Internet Technology, 15(6), 929–935.
[9] Choo, K. K. R., Nam, J., & Won, D. (2014). A mechanical approach to derive identity-based protocols from Diffie–Hellman-based protocols. Information Sciences, 281, 182–200.
[10] Kim, W. S., & Chung, S. H. (2015). Interface assignment-based aodv routing protocol to improve reliability in multi-interface multichannel wireless mesh networks. Mobile Information Systems, 768–796.
[11] Jiang, J., Han, G., Wang, H., & Guizani, M. (2019). A survey on location privacy protection in Wireless Sensor Networks. Journal of Network and Computer Applications, 125, 93–114.
[12] Sato, G., Uchida, N., & Shibata, Y. (2015). Resilient disaster network based on software defined cognitive wireless network technology. Mobile Information Systems, 308–319.
[13] Regan, R., & Manickam, J. M. L. (2019). An Optimized Energy Saving Model for Hybrid Security Protocol in WMN. National Academy Science Letters, 42(6), 489–501.
[14] You, Z., & Xie, X. (2011). A novel group key agreement protocol for wireless mesh network. Computers & Electrical Engineering, 37(2), 218–239.
[15] Bresson, E., Chevassut, O., & Pointcheval, D. (2007). Provably secure authenticated group Diffie-Hellman key exchange. ACM Transactions on Information and System Security (TISSEC), 10(3), 101–121.
[16] Matsumoto, T., Takashima, Y., & Imai, H. (1986). On seeking smart public-key-distribution systems. IEICE TRANSACTIONS (1976–1990), 69(2), 99–106.

[17] Diffie, W., Van Oorschot, P. C., & Wiener, M. J. (1992). Authentication and authenticated key exchanges. Designs, Codes and cryptography, 2(2), 107–125.
[18] Hoffmann, L. (2016). Q&A: Finding New Directions in Cryptography. Communications of the ACM, 59(6), 112–123.
[19] Girault, M. Self-certified public keys. In Workshop on the Theory and Application of of Cryptographic Techniques, Springer, 490–497.
[20] He, D., Kumar, N., & Chilamkurti, N. (2015). A secure temporal-credential-based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks. Information Sciences, 321, 263–277.
[21] Shi, W., & Gong, P. (2013). A new user authentication protocol for wireless sensor networks using elliptic curves cryptography. International Journal of Distributed Sensor Networks, 9(4), 730–831.
[22] Jurkiewicz, P., & Niemiec, M. (2016). Implementation of a new cipher in openssl environment the case of indect block cipher. International Journal of Computer and Communication Engineering, 5(1), 41–55.
[23] Zhou, L., & Haas, Z. J. (1999). Securing ad hoc networks. IEEE network, 13(6), 24–30.
[24] Chai, Z., Cao, Z., & Lu, R. (2007). Threshold password authentication against guessing attacks in Ad hoc networks. Ad Hoc Networks, 5(7), 1046–1054.
[25] Gharib, M., Moradlou, Z., Doostari, M. A., & Movaghar, A. (2017). Fully distributed ECC-based key management for mobile ad hoc networks. Computer Networks, 113, 269–283.
[26] Yu, Z., Zhang, W., & Dai, H. (2017). A trusted architecture for virtual machines on cloud servers with trusted platform module and certificate authority. Journal of Signal Processing Systems, 86(2–3), 327–336.
[27] Liu Yonglei, Wang Peng, Jin Zhigang. (2017). Novel universal security mechanism for energy internet based on trusted platform module. Journal of Jilin University, 47, 933–938.
[28] Xiao, P., He, J., & Fu, Y. (2014). An access authentication protocol for trusted handoff in wireless mesh networks. Computer Standards & Interfaces, 36(3), 480–488.
[29] Usman, A. B., & Gutierrez, J. (2018). Toward trust based protocols in a pervasive and mobile computing environment: A survey. Ad Hoc Networks, 81, 143–159.

[30] Furtak, J., & Chudzikiewicz, J. (2015). Secure Transmission in Wireless Sensors Domain Supported by the TPM. In International Conference on Innovative Network Systems and Applications, 129–148.
[31] Cong, P., Ning, Z., Xue, F., Liu, H., Xu, K., & Li, H. (2017). Trusted connection architecture of Internet of Things oriented to perception layer. International Journal of Wireless and Mobile Computing, 12(3), 224–231.
[32] Devaraj, D., & Banu, R. N. (2019). Genetic algorithm-based optimisation of load-balanced routing for AMI with wireless mesh networks. Applied Soft Computing, 74, 122–132.
[33] Mahto, D., & Yadav, D. K. (2018). Performance Analysis of RSA and Elliptic Curve Cryptography. IJ Network Security, 20(4), 625–635.
[34] Rao, A., Sujatha, K., Deepthi, A., & Rajesh, L. (2017). Survey paper comparing ECC with RSA, AES and Blowfish Algorithms. International Journal on Recent and Innovation Trends in Computing and Communication, 5(1), 44–47.
[35] Law, L., Menezes, A., Qu, M., Solinas, J., & Vanstone, S. (2003). An efficient protocol for authenticated key agreement. International Journal of Network Security, 28, 119–134.
[36] Dai, Y., Ma, C., Yang, Y. (2016). Threshold secret sharing based on Lagrange insert value. Journal of Beijing University of Posts and Telecommunications, 27, 24–28.

Biographies

Peng Zhai was born in China in 1978. He is currently a doctoral candidate in the Faculty of Information Technology at Beijing University of Technology and an associate professor with Jining University, china. He received his M.S. degrees in Shandong University of Science and Technology, China in 2005. His research interests include network security and blockchain.

Jingsha He is currently a Professor in the Faculty of Information Technology at Beijing University of Technology (BJUT), Beijing, China. He received his Ph.D. degree from the University of Maryland at College Park in 1990. Prior to joining BJUT in 2003, he worked for IBM, MCI Communications and Fujitsu Laboratories engaging in R&D of advanced networking technologies and computer security. Prof. He's research interests include methods and techniques that can improve the security and performance of the Internet. He has published nearly 260 papers in the above areas.

Nafei Zhu received her B.S. and M.S. degrees from Central South University, China in 2003 and 2006, respectively, and her Ph.D. degree in computer science and technology from Beijing University of Technology in Beijing, China in 2012. From 2015 to 2017, she was a Postdoc and an Assistant Researcher in the Trusted Computing and Information Assurance Laboratory, State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences in China. She is now on the Faculty of Information Technology in Beijing University of Technology. Dr. Zhu has published over 20 research papers in scholarly journals and international conferences (16 of which have been indexed by SCI/EI/ISTP). Her research interests include information security and privacy, wireless communications and network measurement.

Peng He was born in China in 1965. He received his B.Sc. degree in computer application from Hefei University Of Technology, China in 1986, and his M.Sc. degree in measurement and control from Chinese Academy of Sciences, China in 1989. Currently, he is a professor with China Three Gorges University. His research interests include deep learning and network security.

Yao Liang is currently a Professor in the Department of Computer and Information Science, Purdue University School of Science, Indiana University Purdue University, Indianapolis (IUPUI), USA. His research interests include wireless sensor networks, Internet of Things, cyberinfrastructure, multimedia networking, adaptive network control and management, machine learning, neural networks, data management and integration, data engineering, and distributed systems. His research projects have been funded by NSF.