Available online at www.qu.edu.iq/journalcm
JOURNAL OF AL-QADISIYAH FOR COMPUTER SCIENCE AND MATHEMATICS
ISSN:2521-3504(online) ISSN:2074-0204(print)

Models of Trust and Trusted Computations to an Ad-hoc Network Security

*Younis Samir Younis [1], Saad Hussein Abed Hamed [2], Saleem Meften [3],**

[1] Ministry of Education, Nineveh Education Directorate, Nineveh, Iraq.Email: fajirnet1@yahoo.com.

[2] College of Computer Science & Information Technology, Al-Qadisiyah University, Al-Diwaniyah, Iraq.E-mail: shsaadsh2014@gmail.com.

[3] Department of Computer Science and Engineering, Hodeidah University, Al-Hudaydah, Yemen.E-mail: sal.meften@gmail.com.

**** Corresponding author: Saleem Meften:Email address: sal.meften@gmail.com***

ARTICLE INFO

Article history:
Received: 25 /10/2022
Rrevised form: 27 /11/2022
Accepted : 1 /12/2022
Available online: 01 /12/2022

Keywords:
Ad-hoc network , trust computations trusted computations Network security, Cloud computing

ABSTRACT

Ad-hoc networks have unique properties, making it impossible to execute the current existing network security policy successfully. Based on studying the Ad-hoc network, the Cloud Security theory will be applied to it. We apply Direct Blind Authentication theory and trusted computing platform hardware modules to optimize the Ad-hoc networks' authentication links. The program successfully addresses the security concerns of Ad-hoc nodes, strengthening the Ad-hoc network's defenses.

MSC.41A25; 41A35; 41A3

https://doi.org/10.29304/jqcm.2022.14.4.1090

1. INTRODUCTION

Mobile devices have access to a wireless communications network through an ad-hoc network. There is no fixed infrastructure, such as base stations and mobile switching centers, in ad-hoc networks. For those who are far from the nodes, the mobile node, which within the scope of communication can directly interact with each other over a wireless connection, will rely on the other nodes for message routing.

∗ *Corresponding autho :* Saleem Meften

Email addresses: **sal.meften@gmail.com**

Communicated by: Dr. Alaa Taima Albu-Salih

Mobile nodes in Ad-hoc network certainly led to the Network topology constantly changing. The node security cannot be certified. It easily makes the Ad-hoc network invaded and attacked by illegal nodes. Therefore, this study will introduce trusted computing theory to the Ad-hoc network, play the advantages of trusted computing on node authentication, use of Direct Anonymous Attestation theory to increase the links of node security authentication and improve Ad-hoc network security.

Ad-hoc network and security analysis: Mobile Ad-hoc network brought us the ability of wireless access flexibility, while many of its inherent characteristics are also potential vulnerability [5], specific performance.

Node vulnerability: As network nodes are usually formed by many portable mobile devices, which lack the necessary physical protection, it can easily be lost, captured thus, falling into the attacker's control. At the same time, as the handling capacity and computing power of mobile nodes are limited, making several mobile nodes cannot or difficult to make complex public-key cryptography computing. In addition, some attackers can force node reorganization or making complex operation to consume power, which launched a special type of denial-of-service attack.

Lack infrastructure: The lack of infrastructure makes the centralized authentication institutions and e-traditional security solutions no longer applicable to the mobile Ad-hoc network.

Threat of Ad-hoc routing mechanism: Ad-hoc network routing security designed to protect the accessibility of routing information, routing information's integrity and reliable routing for the message. As a non-central and self-organizing network, finding routing and maintaining of Ad-hoc network need to cooperation between the nodes. On the other hand, node mobility lets its own resources and capacity limited and lack effective network physical protection. All these have made Ad-hoc network routing mechanisms face a variety of security threats [6]. It can generally be divided into the following categories:

Routing forging: Routing forged is that attacker tamper, forging routing information and faking several identity nodes to make false routing information.

Routing hiding: Routing hiding is that an attacker hides reliable routing by special way (only formed by internal legitimate routing nodes). It makes the routing protocol can be only controlled by the routing attacker, so that communication network flow to the attacker control.

From the above discussion, it indicates that making mobile Ad-hoc Network so vulnerable and insecure is the wireless node authentication issue, which was not fundamentally resolved. It will introduce the trusted computing theory in the following study. The application of trusted computing is to achieve the purpose of high-security authentication under the low transmission costs in mobile Ad-hoc network.

2. BASED ON THE TRUSTED COMPUTING OF AD-HOC NODES CREDIBLE SECURITY SOLUTIONS

Overview of trusted computing

The concept of trusted computing: In 2003, the Trusted Computing Group (TCG) was officially established and developed a hardware-level Trusted Platform Module (TPM). To connect network nodes and TPM by physical means to provide hardware basis to the construction of trusted environment. TPM tamper proofing secure chip provides terminal trust roots function. At present, TCG has offered two versions of the TPM solution. One is the Privacy CA in the TPM 1.1 version [7] and the other is Direct Anonymous Attestation (DAA) in the TPM 1.2 version [3], [8].

Based on the feature of TPM trust roots, the use of Direct Anonymous Attestation in TPM 1.2 achieve accessing network security authentication and enables network node security and trustworthy in the Ad-hoc network environment.

Direct anonymous attestation: Direct anonymous attestation is a strategy [1] that can be achieved by authorizing identity authentication in the remote authentication, when not to expose their identity. The principle is the certified (TPM) generate the DAA group signature key and get signature (certificate) on DAA key from DAA issuer. That was later, the certified generated signature by DAA key on AKIi, Verifier and Time and show the DAA PKI to the DAA verifier. The step of TPM v 1.2 is shown in Fig. 1.

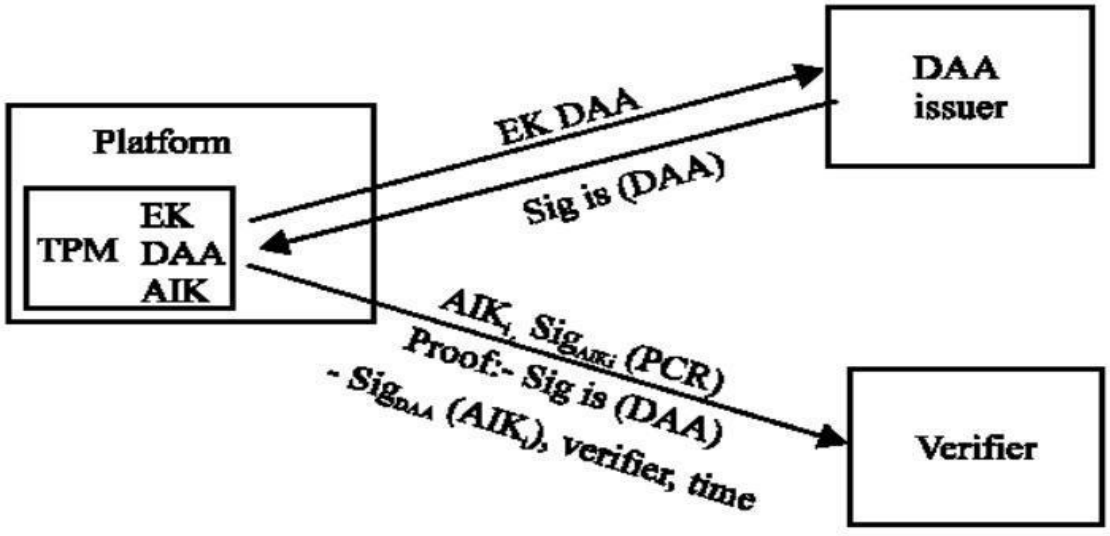

Fig. 1: The step of TPM v1.2

DAA uses Camenisch and Lysyanskaya signature scheme on the TPM to generate public key of the certification [2]. Following is Camenisch-Lysyanskaya signature scheme of 4 steps:

Step 1: Public key of DAA issuer released the public key: (n, a, b, d), where n is an RSA modulus, signature on message x is triple (c, e and s), such that $c^e = a^x b^s d \mathrm{mod} n$.

Step 2: TPM sign the public key of TPM DAA $= a^x \mathrm{mod} n$, when x is the key of TPM.

Step 3: Get random number s', calculate the $c' = cb^{s'} \mathrm{mod} n$ and send c' to the verifier.

Step 4: Verifier calculates $s + es' = s''$, bring it into $d = c'^e a^{-z} b^{-s''} \mathrm{mod} n$. If the Eq. was established, it can prove that TPM master the c, e, s''.

The basis of DAA is the zero-knowledge proof, which is developed by the Bell Labs and the University of Cambridge in the early 1990 s. In zero-knowledge proof, a person (or devices) does not have to expose secrets and can also prove that they really know the secret. The mathematical basis of zero-knowledge proof is the discrete logarithm's difficulties and congruence class problem. There are several specific ways to achieve DAA such as, Schnorr and Fiat-Shamir.

This study will introduce two programs of zero knowledge proof.

Schnorr authentication: It is based on the difficulty of discrete logarithm. System parameters are p and q, which are 2 prime numbers, q is $p - 1$'s the prime factor, $g \neq 1$ and $g^p \equiv 1 \mathrm{mod}$ q. Prover chooses x_p and calculates $y_p \equiv g^x \mathrm{mod} p$.

Prover learns x_p, y_p, p, q, g and verifier learns p, q, g. Following is Schnorr authentication of 4 steps:

Step 1: Prover get random number $r_1, \in \mathrm{GF(p)}, r_1 \neq 0$ calculate $S \equiv g^{r_1}$ and send (y_p, S) to verifier.

Step 2: Verifier gets random number r_2 and send it to Prover.

Step 3: Prover calculate $v = r_1 + r_2 x_p \mathrm{mod} p$ and send v to verifier.

Step 4: Verifier checks $g^v = S(y_p)^{r_2}$?. If Eq. is equal, the Verifier accepts the Prover, or rejects.

$$g^v \equiv g^{(z_1 + \dot{z}_z x_p)} \mathrm{mod} p \equiv g^x \cdot (g^{x_z}) \mathrm{mod} p$$
$$\equiv g^{\frac{k}{1}} \cdot (y_p)^h \mathrm{mod} p \equiv S(y_p)^{h_h^h}$$

Fiat-shamir: In Fiat-Shamir, Prover's identity has k secret numbers, $x_{p1}, x_{p2}, \ldots x_{pk}$. Order $n = pq$ and calculate $y_{pi} \equiv x_{pi}^2 \mathrm{mod} n$, public document's ID: $y_{p1}, y_{p2}, \ldots, y_{pk}$, concrete steps are as follows:

Step 1: Prover gets random select number of calculations, Prover sent to Verifier.

Step 2: Verifier sent $b = (b_1, b_2, \dots b_k)$ to P, b_i is randomly number $b_i \in \{0,1\}, i = 1, 2, \dots, k$.

Step 3: Prover calculate $y = rc_1, c_2 \dots, c_k$ and gave y to Verifier, which $c_i = \begin{cases} 1, & b_i = 0 \\ 0, & b_i = 1 \end{cases}$.

Step 4: Verifier Check y and then if $y^2 = r^2 \prod_{i=1}^{k} y_{pi}^{bi} \text{modm}$, accepted, if not is rejected.

Security solutions of Ad-hoc nodes based on trusted computing: Since there is lack of trusted authentication links in the original Ad-hoc network, making Ad-hoc network security presence hidden dangers. Based on the Trusted Computing theory, transform the original certification system in the aspect of network trusted authentication, to solve Ad-hoc network nodes trusted problem.

Alteration of Ad-hoc network based on trusted computing: According to trusted computing theory, the study transforms the original Ad-hoc network in 3 areas:

Connecting TPM with Internet user's nodes: Introducing TPM into user nodes will be the basis of achieving trusted Ad-hoc. With the TPM terminals, using a single security module and its own signature key (EK) can generate the only independent group DAA signature key. It is the trusted certification's starting point based on the whole trusted computing in Ad-hoc network.

Adding DAA third-party publishers in Ad-hoc: DAA third-party publishers are responsible for verifying the efficiency of network nodes (TPM) and sending DAA key signatures to the network nodes.

Adding authentication server in Ad-hoc: As there is a possibility, the DAA private key x may have been taken from the TPM, so to effectively monitor and detect counterfeit TPM, the node authentication server should be included in Ad-hoc network.

Authentication mechanisms of the Ad-hoc network based on trusted computing are as follows:

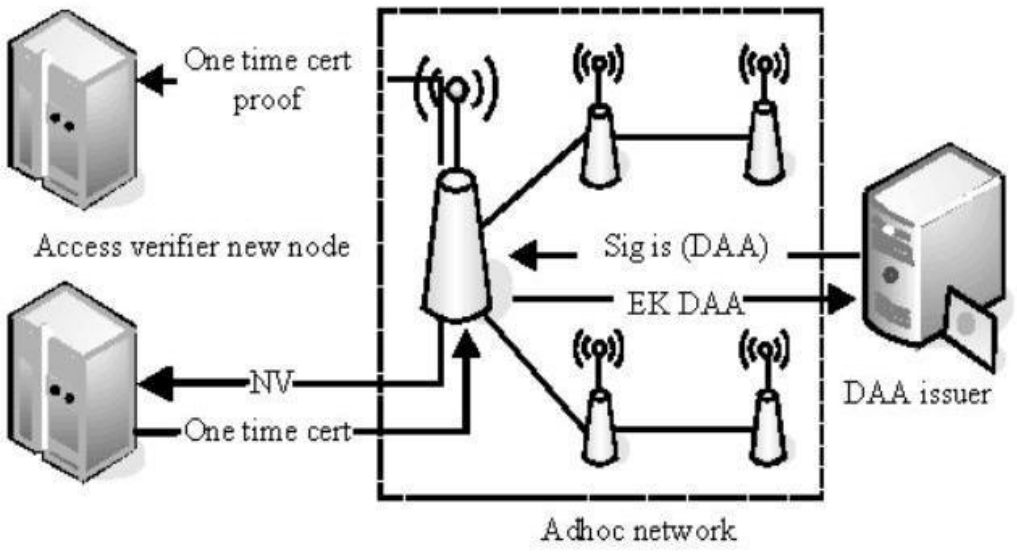

Fig. 2: The structure of Ad-hoc network based on trusted computing

Step 1: Request the certified to calculate NV $= \zeta^{x} \text{mod}\Gamma$, which P is called the pseudonym (have the same $NV = \zeta^{x} \text{ mod}\Gamma$, certified can be distinguished between different P).

Step 2: If x had been published, the verifier calculates NV with invalid x and compares the NV, which calculated by the certified. If the same, which is the counterfeit TPM.

Step 3: At the same time or continuously received a lot of the same certification request of NV, determining whether the certification results are negative in accordance with specific applications and risk management strategies. To handle the x that has not yet been found.

Each the certified uses a certain frequency to change the different, also give the verifier opportunities of analyzing based on NV [4]. So, the permits server should be separated into two servers, 1 is authorized check verifier and other is access verifier. According to the above 3 transformations, the structure of the Ad-hoc network based on Trusted Computing is shown in Fig. 2. The Ad-hoc network certification system based on trusted computing:

Step 1: When TPM access in the Ad-hoc, the node with the only TPM signature key EK produces a DAA group signature key and apply for public key.

Step 2: Second, DAA issuer sends key to the node of Ad-hoc after the public key been verified by DAA publisher.

Step 3: Finally, a node applies to the adjacent nodes to prove its own generate the AIKi, verify and signature by time; to prove its own have key signature on DAA issuer.

4. CONCLUSION

Network nodes use DAA public key EK (identifier) to apply certification only ones. The entire system uses a group signature, making several the same group user (TPM) has the same DAA public key. Thus, DAA publishers can only determine whether the applicant is a trusted node and a legitimate DAA key through EK public key and direct anonymous proof.

The most fundamental aspect of Ad-hoc is protection key reversal of equipment. In DAA-Ad-hoc network, the difficulty of discrete logarithm is the basis of zero knowledge proof. The mathematical resolves the issue of key reversal and proves the Ad-hoc nodes' security.

The security steps based on the authorized check verifier and access verifier in node authentication server are as follows:

Step 1: Firstly, TPM interacts with the Check-verifier. Check verifier makes frequency analysis and detection blacklist, issued the one-time certificate and frequency certificate with DAA.

Step 2: Second, TPM interacts with Access-verifier. Access verifier uses random to decide whether to allow TPM access services based on frequency certification.

According to the above analysis, Ad-hoc network based on the Trusted Computing can be an effective mechanism to meet the network nodes trusted. The advantages are:

- No 1 could use the DAA public key to determine which the specific node is thus, guaranteeing the Ad-hoc nodes trusted.
- In the whole network of Ad-hoc, DAA certificates are issued only once, so there is no bottleneck. This quality is very suitable for the characteristics of Ad-hoc networks.
- DAA certificate can be issued to manufacturers, can also be issued to the purchase of the platform. It is easy to promote Ad-hoc network security based on Trusted Computing.
- The separation of Check-verifier and Access-verifier eliminated the appearance of a fake TPM and greatly enhanced the security system. If Ad-hoc technology abuse, will lead to a lot of Internet crime, which cannot be held responsible to the offenders, so this study raise Ad-hoc network based on trusted computing. Use theory of trusted computing to certificate and monitor the network nodes before accessing network and to ensure the trust of network node, making Ad-hoc network more comprehensive and security. Future research will focus on the comprehensive assessment of Ad-hoc network and certification between TPM and other platforms. As the trusted computing development, the Ad-hoc will achieve a new level.

5. REFERENCES

1) Brickell, E., J. Camenisch and L. Chen, 2004. Direct anonymous attestation. Proc. 11th ACM Conf. Compu. Commun. Security, pp: 132-145.
2) Camenisch, J. and A. Lysyanskaya, 2003. A Signature Scheme with Efficient Protocols. Security in Communication Networks: Third International Conference, SCN 2002, pp: 268-270.
3) Liming, H., X. Sun, Y. Shutang and L. Songnian, 2007. A Method to Implement Full Anonymous Attestation for Trusted Computing Platform. Wuhan Uni. J. Nat. Sci., pp: 101-104.
4) Nützel, J. and A. Beyer, 2006. How to Increase the Security of Digital Rights Management Systems without Affecting Consumer's Security. Emerging Trends in Info. Commun. Security, pp: 368-380.
5) Ping, Y., J. Yichuan, Z. Shiyong and Z. Yiping, 2005. A Survey of Security for Mobile Ad-hoc Networks. Acta Electronica Sinica, pp: 893-899.
6) Tingyao, J., Y. Jinghua and L. Qinghua, 2005. Survey on the Security for Mobile Ad-hoc Networks. Appl. Res. Com., pp: 1-4.
7) Sumrall, Nancy, and Manny Novoa. "Trusted computing group (TCG) and the TPM 1.2 specification." In Intel Developer Forum, vol. 32. Intel, 2003.
8) Zhidong, S., Z. Huanguo, Z. Miao, Y. Fei and Z. Liqiang, 2006. The Mechanism about Key and Credential on Trusted Computing Platform and the Application Study. Wuhan Uni. J. Nat. Sci., pp: 1641-1644.