# Journal of Applied Sciences

ISSN 1812-5654

science alert

ANSInet
an open access publisher
http://ansinet.com

Journal of Applied Sciences 13 (16): 3320-3324, 2013
ISSN 1812-5654 / DOI: 10.3923/jas.2013.3320.3324


# Application of Direct Anonymous Attestation to the Ad Hoc Networks Security

[1]Tao Zhang and [2]Shuai Ren
[1]School of Electronic and Control Engineering, Chang'an University, Xi'an, 710064, China
[2]School of Information Engineering, Chang'an University, Xi'an, 710064, China

**Abstract:** As Ad Hoc networks own characteristics, the existing fixed network security strategy can not be effectively implemented. Direct Anonymous Attestation theory will be imported into Ad Hoc networks based on researching the Ad Hoc network. To optimize authentication link of the Ad Hoc networks, we make use of trusted computing platform module in hardware level and Direct Anonymous Attestation theory. The application effectively solves the Ad Hoc nodes security issues, thus raising the Ad Hoc network against attacks.

**Key words:** Network security, ad hoc network, direct anonymous attestation, zero-knowledge proof

## INTRODUCTION

Ad Hoc Network provide mobile devices with a wireless communications network. In Ad Hoc network, there is no fixed infrastructure such as base stations and mobile switching center. The mobile node which within the scope of communication can direct communicate with each other through a wireless connection, for those who are far from the nodes will rely on the other nodes for routing message.

Mobile nodes in Ad Hoc network certainly lead to the Network topology constantly changing. The node security can not be certified. It easily makes the Ad Hoc network invaded and attacked by illegal nodes (Zheng and Kravets, 2005). Therefore, this study will introduce trusted computing theory (Shen and Tong, 2010) to the Ad Hoc network, play the advantages of trusted computing on node authentication, use of Direct Anonymous Attestation theory (Othman *et al*., 2010)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, 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, capture, thus falling into the attacker's control (Li and Wang, 2007). At the same time, as the handling capacity and computing power of mobile nodes are limited, making a number of mobile nodes can not 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 (Kale *et al*., 2013).

**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 (Cho *et al*., 2010). As a non-central and self-organizing network, finding routing and maintain of Ad Hoc network need to mutual cooperation between the nodes. On the other hand, node mobility let its own resources and capacity limited and lack effective network physical protection. All these have made Ad Hoc network routing mechanism face a variety of security threats. It can generally be divided into the following categories.

**Routing forging:** Routing forged is that attacker tamper, forging routing information and faking a number of identity nodes to make false routing information.

**Routing hiding:** Routing hiding is that an attacker hide 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.

**Corresponding Author:** Tao Zhang, School of Electronic and Control Engineering, Chang'an University, Xi'an, 710064, China

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 fundamental resolved. It will introduce the trusted computing theory in the following article. The application of trusted computing is to achieve the purpose of high-security authentication under the low transmission costs in mobile Ad Hoc network.

## BASED ON THE TRUSTED COMPUTING OF AD HOC NODES CREDIBLE SECURITY SOLUTIONS

### Overview of trusted computing

**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 up network nodes and TPM by physical means to provide hardware basis to the construction of trusted environment. TPM tamper-proofing secure chip provide terminal "trust roots" function. At present, TCG has offered two versions of the TPM solution.

Based on the feature of TPM "trust roots", the use of Direct Anonymous Attestation in TPM1.2 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 that can be achieved 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 (Day *et al*., 2013). 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 v1.2 is shown in Fig. 1.

DAA use Camenisch-Lysyanskaya signature scheme (Xue and Ding, 2012; Chim *et al*., 2011; He *et al*., 2011; Yeh *et al*., 2011) on the TPM to generate public key of the certification. Following is Camenisch-Lysyanskaya signature scheme of four 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 $c^e = a^x b^s d \bmod n$;

**Step 2:** TPM sign the public key of TPM DAA = $a^x \bmod n$, when x is the key of TPM

**Step 3:** Get random number S', alculate the $c' = cb^{s'} \bmod n$ and send c' to the verifier

**Step 4:** Verifier calculates s+es' = s'', bring it into $d = c'^e a^{-x} b^{-s''}$. If the equation was establish, 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 1990s. In zero-knowledge proof, a person (or devices) do 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 tow programmes of Zero-knowledge proof (Catalano *et al*., 2011; Gros *et al*., 2012):

- **Schnorr authentication:** It is based on the difficulty of discrete logarithm. System parameters are p and q which are two prime numbers, q is p-1's the prime factor, $g \neq 1$ and $g^p = 1 \bmod q$. Prover chooses $x_p$ and calculates $yp = g^{x_p} \bmod p$

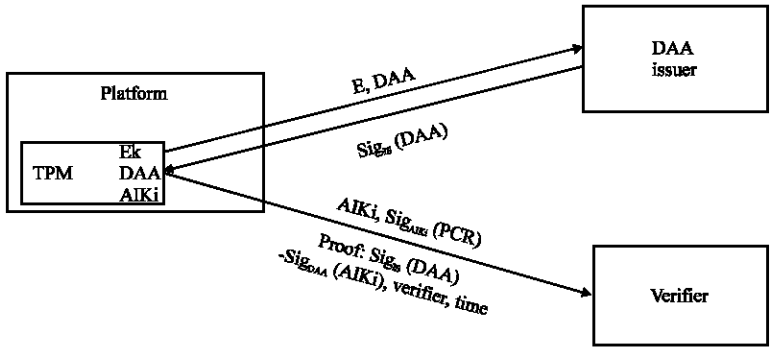


Fig. 1: Step of TPM v 1.2

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

**Step 1:** Prover get random number $r1 \in GF(p)$, $r1 \neq 1$, calculate $S \equiv g^{r_1} \bmod p$ and send ($y_p$, S) to verifier
**Step 2:** Verifier gets random number $r_2$ and send it to Prover
**Step 3:** Prover calculate $v = r_1 + r_2 x_p \bmod p$ and send v to verifier
**Step 4:** Verifier checks $g^v = S(y_p)^{r2}$. If equation is equal, Verifier accept the Prover, or reject:

$$g^v \equiv g^{(r_1+r_2x_p)} \bmod p \equiv g^{r_1} \cdot (g^{x_p})^{r_2} \bmod p$$
$$\equiv g^{r_1} \cdot (y_p)^{r_2} \bmod p \equiv S \cdot (y_p)^{r_2}$$

- **Fiat-shamir:** In fiat-shamir, prover's identity has k secret numbers $x_{p1}$, $x_{p2}$,$\cdots$,$x_{pk}$. Order n = pq and calculate $y_{pi} \equiv x^2_{pi} \bmod n$, public document's ID: $y_{p1}$, $y_{p2}$,$\cdots$, $y_{pk}$, concrete steps are as follows:

**Step 1:** Prover gets random select number of calculations, Prover sent to Verifier;
**Step 2:** Verifier sent $b = (b_1, b_2,\cdots b_k)$ to P, $b_i$ is randomly number $b_i \in \{0,1\}$, i = 1, 2,$\cdots$, k
**Step 3:** Prover calculate $y = rc_1c_2\cdots c_k$ 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:

$$y^2 = r^2 \prod_{i=1}^{k} y_{pi}^{bi} \bmod m$$

accepted, if not is rejected

**Security solutions of ad hoc nodes based on the 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, so as to solve Ad Hoc network nodes trusted problem.

**Alteration of ad hoc network based on the trusted computing:** According to trusted computing theory, the paper transforms the original the Ad Hoc network in three 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 sent DAA key signatures to the network nodes
- **Adding authentication server in Ad Hoc:** As there is a possibility of the DAA private key x may have be taken from the TPM, so in order 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:

**Step 1:** Request the certified to calculate $NV = \zeta^x \bmod \Gamma$ which P is called the pseudonym (have the same $NV = \zeta^x \bmod \Gamma$ 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 use certain frequency to change the different, also give the verifier opportunities of analysing based on NV. So the permits server should be separated into tow servers, one is authorized check verifier and other is access verifier.

According to the above three transformations, the structure of Ad Hoc network based on the Trusted Computing is shown in Fig. 2.

**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 produce a DAA group signature key and apply for public key
**Step 2:** Second, DAA issuer sent key to the node of Ad Hoc after the public key been verified by DAA publisher

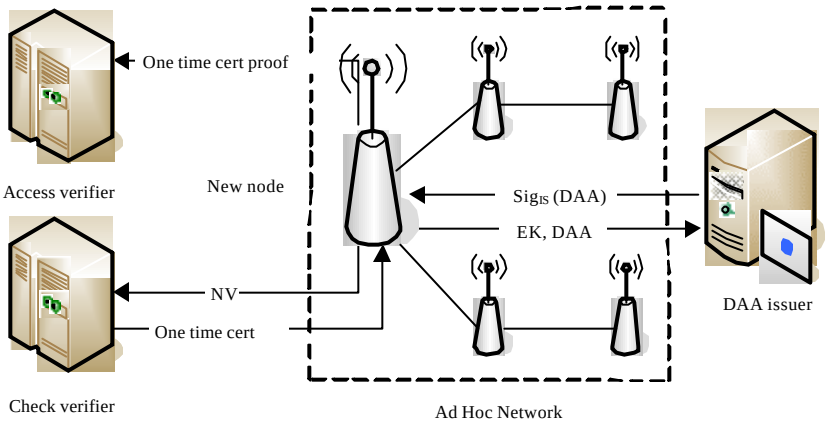


Fig. 2: Structure of Ad Hoc network based on the trusted computing

**Step 3:** Finally, node apply to the adjacent nodes to proved its own generate the AIKi, verify and signature by time; to proved its own have key signature on DAA issuer

## SECURITY ANALYSIS AND VERIFICATION CONCLUSION

**Safety analysis of ad hoc nodes based on the trusted computing:** network nodes use daa public key ek (identifier) to apply certification only ones.

The entire system uses a group signature, making a number of the same group user (TPM) have the same DAA public key. Thus DAA publisher can only determine whether the applicant be a trusted nodes and a legitimate DAA key through EK public key and direct anonymous proof.

The most fundamental 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 resolve the issue of key reversal and prove 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 make 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 use random $f^{\hat{e}}$ to decide whether to allow TPM access services based on frequency certification

**Conclusion verify:** According to above analysis, Ad Hoc network based on the Trusted Computing can be an effective mechanism to meet the network nodes trusted. The advantage lies:

- No one 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 certificate issued only once, so there is no bottleneck. This quality is very suitable for the characteristics Ad Hoc networks
- DAA certificate can be issued to manufacturers, can also be issued to the purchase of the platform. It is easily to promote the Ad Hoc network security based on Trusted Computing
- The separation of Check-verifier and Access-verifier eliminate the appearance of a fake TPM and greatly enhanced the security system

## CONCLUSION

If Ad Hoc technology abuse, will lead to a lot of Internet crime which can not 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 trusted of network node, making Ad Hoc network more comprehensive and security. Future work 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.

**ACKNOWLEDGMENTS**

The project was supported by the Special Fund for Basic Scientific Research of Central Colleges, Chang'an University. The Grant No. is 2013G1241118. And the National 863 plans projects and The Grant No. is 2012AA112312. The project was supported by the Ministry of Transport of the People 's Republic of China projects and The Grant No. is 2012-364-208-600, 2012-364-208-200, 201231849A70. The project was supported by the Jilin Association for International Exchange of Personnel projects and The Grant No. is 2012-7-102-2.

**REFERENCES**

Catalano, D., M. Di Raimondo, D. Fiore and M. Messina, 2011. Zero-knowledge sets with short proofs. IEEE Trans. Inform. Theory, 57: 2488-2502.

Chim, T.W., S.M. Yiu, L.C. Hui and V.O. Li, 2011. PASS: Privacy-preserving authentication scheme for smart grid network. Proceedings of the IEEE International Conference on Smart Grid Communications, October 17-20, 2011, Brussels, Belgium, pp: 196-201.

Cho, J.H., A. Swami and I.R. Chen, 2010. A survey on trust management for mobile ad hoc networks. IEEE Commun. Surv. Tutorials, 13: 562-583.

Day, J.N., T.T.H. Chau, M. Wolbers, P.P. Mai and N.T. Dung *et al*., 2013. Combination antifungal therapy for cryptococcal meningitis. N. Engl. J. Med., 368: 1291-1302.

Gros, J., R. Ostrovsky and A. Sahai, 2012. New techniques for noninteractive aero-knowledge. J. ACM, Vol. 59. 10.1145/2220357.2220358

He, D., J. Bu, S. Chan, C. Chen and M. Yin, 2011. Privacy-preserving universal authentication protocol for wireless communications. IEEE Trans. Wireless Commun., 10: 431-436.

Kale, M.R.A., S.R. Gupta and R.B. Prmit, 2013. An overview of manet ad hoc network. Int. J. Comput. Sci. Appl., 6: 223-227.

Li, F. and Y. Wang, 2007. Routing in vehicular ad hoc networks: A survey. IEEE Veh. Technol. Mag., 2: 12-22.

Othman, H., H. Hashim and J.L. Ab Manan, 2010. A conceptual framework providing Direct Anonymous Attestation (DAA) protocol in trusted location-based services (LBS). Proceedings of the International Conference on Internet Technology and Secured Transactions, November 8-11, 2010, London, UK., pp: 1-7.

Shen, Z. and Q. Tong, 2010. The security of cloud computing system enabled by trusted computing technology. Proceedings of the 2nd International Conference on Signal Processing Systems, Volume 2, July 5-7, 2010, Dalian, China, pp: V2-11-V2-15.

Xue, X. and J. Ding, 2012. LPA: A new location-based privacy-preserving authentication protocol in VANET. Secur. Commun. Networks, 5: 69-78.

Yeh, L.Y., Y.C. Chen and J.L. Huang, 2011. PAACP: A portable privacy-preserving authentication and access control protocol in vehicular ad hoc networks. Comput. Commun., 34: 447-456.

Zheng, R. and R. Kravets, 2005. On-demand power management for ad hoc networks. Ad Hoc Networks, 3: 51-68.