Research Journal of Applied Sciences, Engineering and Technology 5(11): 3069-3073, 2013
DOI:10.19026/rjaset.5.4535
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: August 11, 2012 Accepted: September 17, 2012 Published: April 05, 2013

Research Article

Distributed Access Control Based on Proxy Signature in M2M Sensor Networks

[1, 2, 3]Lingyu Lee, [3]Yunsheng Zhang, [1, 2]Ying Jiang, [1, 2]Yingli Liu
[1]Yunnan Key Lab of Computer Technology Application, Yunnan, China
[2]Faculty of Information Engineering and Automation,
[3]Faculty of Mechanical and Electrical Engineering, Kunming University of Science and Technology,
Yunnan, China

Abstract: In this study, we have a research of the distributed access control based on proxy signature in M2M sensor networks M2M sensor networks. As M2M sensor networks are usually deployed in hostile environment, the global communication security of M2M sensor networks is and will continue to be a major concern. Although there are many related works on access control in WSNs (Wireless Sensor Networks), Ad-hoc networks, MANETs (Mobile Ad-hoc Networks) and etc., they cannot be applied to M2M sensor networks directly. Motivated by this consideration, we develop a secure and distributed access control scheme based on proxy signature for M2M sensor networks, which provides strong authentication and achieves efficiency. Moreover, security of the proposed technique does not rely on availability of a secure channel.

Keywords: Access control, M2M sensor networks, proxy signature, security, trapdoor hash function

INTRODUCTION

With the development of WSNs, RFID and pervasive computing technology, M2M (Machine to Machine) sensor networks, which consist of M2M servers and terminals, both of which are connected together by sensor networks to form a collaborative computing environment, have been more and more widely applied to intelligent applications and services. M2M sensor networks cover various technologies including sensing, communication; computing, data processing and feedback control technologies and support massive heterogeneous smart devices to communicate with each other (Chang, 2012). M2M sensor networks aim to involve associating communications (e.g., between smart devices) with each other via wireless sensor networks, while limiting of (even without) human intervention.

Similar to conventional networks, access control is a critical security service in M2M sensor networks to prevent sensitive data and services from unauthorized internal and external accessing. On one hand, the access control scheme must be able to authorize and grant users the right to access to the network; on the other hand, the scheme must organize data collected by sensors in such a way that an unauthorized device cannot make arbitrary queries. This restricts the network access only to eligible users and devices, while queries from outsiders will not be responded.

As conventional network, two approaches access control schemes in M2M sensor networks, namely, centralized and distributed approaches. In the centralized case, sensed data are collected from individual sensor devices and transmitted back to a central location. In the other case, after a sensor device has generated some data, it stores the data locally or at some designated devices within the network instead of immediately forwarding the data to a centralized location out of the network. The stored data later on can be accessed in distributed manner by the users of the sensor network.

Since sensed data are no longer transmitted to a centralized location out of the network, distributed data storage and access, comparing with the centralized case, consumes less bandwidth. In addition, distributed data storage and access can avoid weaknesses such as single point of failure, performance bottleneck, which are inevitable in the centralized case. These advantages together have led to the recent increasing popularity of distributed data storage and access (Girao *et al*., 2007; Newsome and Song, 2003).

As a large amount of sensed data is distributed storage in individual M2M terminals, data security naturally becomes a serious concern. Actually, in many application scenarios, data sensed by M2M sensor network are closely related to security and/or privacy issues and should be accessible only to authorized devices.

Similar to the distributed access control protocols of conventional wireless network, a secure distributed

Corresponding Author: Yunsheng Zhang, Faculty of Mechanical and Electrical Engineering, Kunming University of Science and Technology, Yunnan, China

access control scheme of M2M sensor networks should satisfy the following requirements:

- **Distributed:** After deploying, multiple authorized network devices are able to access data on different devices simultaneously without involving human intervention. Additionally, the scheme should prevent unauthorized devices from accessing
- **Authentication:** security of authentication needs to be enforced for sensor data in M2M sensor networks so that the information will not be obtained by unauthorized devices
- **Confidentiality:** The query command can be only processed by the target device
- **Integrity Protection:** It must be possible to ensure that a query command has not been modified by adversaries or malicious intermediate modes during its transmission
- **Freshness security:** To avoid vulnerable to replay attack the target device can always ensure that the query command is new
- **Liveness:** any query command will be processed at least by one or each device of the set of devices which form a collaborative computing environment (Youssou Faye and Thomas, 2011)

To satisfy the above requirements, we propose a practical secure and distributed access control scheme in this study, which is built on the secure proxy signature using trapdoor hash function

In this study, we have a research of the distributed access control based on proxy signature in M2M sensor networks M2M sensor networks. As M2M sensor networks are usually deployed in hostile environment, the global communication security of M2M sensor networks is and will continue to be a major concern. Although there are many related works on access control in WSNs (Wireless Sensor Networks), Ad-hoc networks, MANETs (Mobile Ad-hoc Networks) and etc., they cannot be applied to M2M sensor networks directly. Motivated by this consideration, we develop a secure and distributed access control scheme based on proxy signature for M2M sensor networks, which provides strong authentication and achieves efficiency. Moreover, security of the proposed technique does not rely on availability of a secure channel.

LITERATURE REVIEW

M2M access control: Several access control policies have been proposed in M2M. Among these policies Chakraborty and Ray (2006) etc. propose an access control model called Trust BAC (Chakraborty and Ray, 2006), which extend RBAC model based on trust. However, the model has often been found to be inadequate for scalability and decentralization. In Ray and Toahchoodee (2007) propose a formal spatio-temporal model based on RBAC model that is suitable for commercial WSNs applications, which can determine whether a user has access to a given object. Next year, in Ray and Toahchoodee (2008) the authors extend the model to incorporate environmental contexts. However, the different features of a spatio-temporal access control model may interact in subtle ways resulting in conflicts. It is important to detect and resolve access control conflicts (Chen and Chang, 2012). In Shucheng *et al.* (2009), Yu *et al.* propose fine-grained data access control problem, which applies and tailors KP-ABE to WSNs. However, the scheme is statically defined before the CPS application deployed and cannot be adjusted according to the change of system environment dynamically. In He *et al.* (2012), He proposed a secure and distributed code dissemination protocol named DiCode, which is built on the proxy signature by warrant (PSW) technique. DiCode can resist denial-of-service attacks. However, the protocol relies on availability of a secure channel.

Trapdoor hash-based proxy signature: In this study, the proxy signature is introduced into the design of our proposed scheme. Dozens of schemes have focused on developing new proxy signatures by enhancing the security and efficiency, since the proxy signature was introduced by Mambo *et al.* (1996). However, some proposed schemes take long time to verify a signature. In Shamir and Tauman (2001), the trapdoor hash function was introduced to signature scheme and then, in Mehta and Harn (2005) the author built one-time signatures by exploiting the key-exposure property of trapdoor hash functions. Although many secure and effective proxy signature techniques can be applied in access control, we choose the proxy signature scheme that was introduced by Chandrasekhar *et al.* (2010) for several reasons. Firstly, the technique allows the choice of primitives open to policy specifications. Secondly, security of the proposed technique does not rely on availability of a secure channel. Last but not lest, the proposed technique inherently provides the efficiency of online/offline signature schemes (Chandrasekhar *et al.*, 2010).

MODELS

Network model: M2M sensor networks consist of a large number of resource-constrained devices with sensor, the servers (applications) and a Certificate Authority (CA). Devices (or terminals) sense conditions in their local surroundings, report their observations to the servers or other devices, which collaborate with it, based on query command. Servers (Applications) pass data through various application services. Wireless network furnishes connection both devices and servers (applications). The network model is a public key infrastructure. The CA is responsible for signing a unique public key certificate to an authenticated device, which binds the device's identity.

Adversary model: The adversary is given access to standard and proxy signing oracle. The adversary can interact with the honest entity multiple times playing the role of different entities each time. The adversary can eavesdrop, copy or replay the transmitted messages in the M2M sensor network. With compromising legal devices, the adversary can inject forged false messages or ephemeral keys. Additionally, the adversary may launch adaptive chosen message attack in the random oracle model under the DL assumption.

OUR PROPOSED PROTOCOL

In this section, the proposed scheme is presented in detail. Before giving the detailed description, we first give an overview of the proposed scheme.

Overview proposed scheme: In our proposed scheme, three kinds of participants are involved, a delegator (specific server), proxies (devices) and a Certificate Authority (CA). The delegator generates a trapdoor hash of the warrant, signs the hashed warrant and sends the (warrant, signature) pair to the proxy over an insecure channel. The proxy signature uses its trapdoor key, known exclusively to it, to find a collision between the trapdoor hash of the warrant and the given message. The proxy tags the result of the collision along with the delegator signature, warrant and query to collectively generate the proxy signature.

The proposed scheme consists of six phases: system initialization, delegator signature generation, delegator signature authentication, device query generation, target device verification, new devices joining phase.

System initialization: The servers and devices execute the following steps before they are deployed:

- The specific server chooses p and q, which denote 1024-bit and 160-bit primes, respectively, $q| (p - 1)$. α is an element of order q in Z_p^* and $H_1, H_2 : \{0, 1\}^* \rightarrow Z_q^*$ are cryptographic hash functions. Consequently, the system public parameters PA is a tuple $< p, q, \alpha, H_1, H_2$
- The servers choose their long-term private key $x \in_R Zq^*$ and computes the corresponding long-term public key as $X = \alpha^x \in Z_q^*$
- The devices choose their long-term trapdoor key $y \in_R Z_q^*$ and computes the corresponding long-term hash key as $Y = \alpha^y \in Z_q^*$
- Both the servers and the devices submit their (public, identity) pairs or (hash identity) pairs to CA, respectively. The CA verifies the identity upon registration. The CA sends back certificates to them, respectively. The certificates bind their identity with their public keys or hash keys
- The CA keeps all (public. Identity) pairs of servers and (hash, identity) pairs of the devices into a directory which can be access publicly by all the legal servers and devices in the M2M sensor network
- Both servers and devices preload the public directory, the system public parameters PA $< p, q, \alpha, H_1, H_2>$ into their memory respectively before they are deployed

Delegator signature generation: The delegator signature is generated by the following steps:

- When a device D_i wants to access data in another device, it makes a request to the specific server (delegator). The form of a request is depicted in Table 1

  Here, the request of device records *source ID*, which indicates the identity of itself, *target ID*, which the device wants to access and *type*, the data type, which the device wants to access.
- The server confirms that the device is legal by check it's identity in its memory. If the check fails, the server looks up the public directory of CA. If the check fails, the server aborts the request. Otherwise, the server writes the identity into its memory and chooses a big prime k, $(k \in_R Z_q^*)$ and generates the ephemeral (private, public) key pair as $(k, r = \alpha^k \in Z_q^*)$
- The server generates a warrant w, the format of w is depicted in Table 2

  Here, Timestamp means valid period of the warrant, which the device can be a proxy, to allow to access data
- The server compute $TH_Y (w, r) = \alpha^{hw} Y^{r} (mod q)$, where $h_w = H_1 (w ||Y)$.
- The server solves for t in $t \equiv k + xH_2(TH_Y(w, r)|| w ||r) (mod q)$
- The server form a proxy signature key $s= <t, r, w>$ and send s to the device, say D_i

Delegator signature authentication: After receiving the delegator signature s from the server, the device D_i performs the following operations:

Table 1: Format of the warrant request

Source ID (16)	Target ID (16)	Type (6)	Server ID (2)

Table 2: Format of the warrant w

Target ID (16)	Timestamp (8)	Type (6)	Server ID (2)

Table 3: Format of the query command

Target ID (16)	Timestamp (16)	Type (6)	Reserved (2)	Source ID (8)

- The device checks whether warrant w conforms to one of the ID of servers. If the check fails, the device aborts it.
- The device compute $TH_Y\ (w,\ r) = \alpha^{hw}\ Y^r$ (mod q) and $h = H_2(TH_Y(w,\ r)||w\ ||r\ )$
- If $r = \alpha^t X^{-h\ (}mod\ q)$, the signature $s = <t,\ r,\ w>$ on h is valid under the public key X of the server. Otherwise, the device rejects the signature key

Device query generation: When the device D_i wants to access data after it authenticates the proxy signature, he does the following steps:

- The device D_i constructs a query command QU_i at first. An example format of QU_i is depicted in Table 3
- D_i generates the ephemeral (trapdoor, hash) key pair as $(\ z \in_R Zq^*,\ Z{=}\alpha^z\ \in Zq^*)$
- D_i solve for c in $c{=}\ z^{-1}\ (\ h_w\ -\ h_m\ +\ yr\ )\ ($mod q), where $h_m = H_1\ (m\ ||Z\ )$
- The proxy signatures PS_i is the tuple $<s,\ QU_i\ ,\ c\ ,\ h_m>$ on the query QUi conforming to warrant w
- D_i send PS_i to the target device, say

Target device verification: D_j can verify the delegation agreement, identify the proxy and verify the proxy signature on the query QUi conforming to warrant w as follows:

- D_j checks whether the query QUi conforms to warrant w. If check fails, D_j aborts it
- D_j checks the *timestamp* segment in w to make sure the w is not overtime
- D_j checks whether the hash key Y_i of D_i in its memory. If D_j find Y_i, then D_j executes the next step, otherwise D_j looks up the hash key Y_i of D_i from the publicly available directory of CA. If D_j finds Y_i in CA, then D_j executes the next step. Meanwhile D_j adds Y_i into its memory
- D_j computes $TH_Y\ (w,\ r) =\alpha^{hw}\ Y^{\ r}(\ mod\ q)$ and $h = H_2(TH_Y\ (w,\ r)||\ w||\ r\ )$.
- Dj computes $r' = \alpha^t X^{-h\ (}mod\ q)$. If $r' \neq r(\ mod\ q)$, D_j aborts it
- D_j computes $Z' = \alpha\ (\ h_w\ -\ h_m\ )\ c^{-1} Y^{rc-1}\ (mod\ p)$. Check whether $h_m = H\ (m||\ Z')$. If the check passes, D_j authenticates as a legal device and provides the data that D_i wants. Otherwise, D_j aborts the query

New devices joining phase: The underlying network of M2M is extremely dynamic in nature. A new device may need to join the M2M sensor network after deployed. A device D_{new} which wants to join in the M2M sensor network after the network is deployed. D_{new} must register in a specific server firstly. Once the server accepts the request from D_{new}, it will assign an identity for it. Then D_{new} computes its hash key, as described in system initialization phase and submits it to the server. The server sends the (hash, identity) pair to the CA. The CA sends back a certificate which binds the identity with the hash keys to the server. The server sends the certificate to $D_{new.}$

SECURITY ANALYSIS

So far, we have elaborated the procedures of our protocol. By the protocol, we can achieve M2M sensor network access control. In the following, we will discuss the security of our proposed scheme to verify whether the security requirements have been satisfied.

Distributed: The authorized devices are able to access data in a distributed manner.

Authentication: In order to access data, each device has to register to not only the specific server to obtain a delegator signature but also the CA to achieve the certificate of its hash key. To send a query command, a server needs to sign the query command with delegator signature and warrant. Therefore, the server enforces strict access control by devices registration.

Integrity protection: An authorized device uses a proxy signature technique to authenticate the query command. The target devices know the public keys, thus can verify the query command. Therefore, an adversary cannot modify the query command and then pass the verification of the sensor nodes.

Confidentiality: The query command can be only processed by the target device.

Freshness security: The timestamp included in the query command can ensure the freshness of the query command. Moreover, the timestamp can resist replay attack by adversary.

Liveness: Any query QUi posted by a legitimate device will be processed at least by one or each sensor of the set of sensors which must process the query command in order to give the required answer to the user other than meeting the above requirements, the proxy signature based on trapdoor hash, which we introduce in our proposed scheme, can also satisfy collision-forgery-resistant, ephemeral-collision-forgery-resistant and key-exposure resistant. Moreover, the scheme is secure against adaptive chosen message attack in the random oracle model under the DL assumption. The proofs of aforementioned security are given in Youssou Faye and Thomas (2011) and Chandrasekhar *et al*. (2010).

CONCLUSION

In this study, we have proposed a novel access control scheme for M2M sensor network. The security analysis show that the technique guarantees strong unforgeability, verifiability, strong identifiability, strong undesirability and prevention of misuse. Moreover, security of the proposed technique does not rely on availability of a secure channel.

ACKNOWLEDGMENT

This research is sponsored by the Subject Direction Team of Software Quality Assurance of Kunming University of Science and Technology.

This research is also sponsored by Department of Education of Yunnan Province Scientific Research Fund grant 2012Y552.

REFERENCES

Chakraborty, S. and I. Ray, 2006. TrustBAC: Integrating trust relationships into the RBAC model for access control in open systems. Proceedings of the 11th ACM Symposium on Access Control Models and Technologies, ACM, pp: 49-58.

Chandrasekhar, S., S. Chakrabarti, M. Singhal and K.L. Calvert, 2010. Efficient proxy signatures based on trapdoor hash functions. IET Inform. Secur., 4(4): 322-332.

Chang, G., 2012. M2M Architecture: Can it realize ubiquitous computing in daily life? KSII T. Inte. Inform. Syst., 6: 24-45.

Chen, D. and G. Chang, 2012. A survey on security issues of M2M communications in cyber-physical systems. KSII T. Inte. Inform. Syst., 6(1): 24-45.

Girao, J., D. Westhoff, E. Mykletun and T. Araki, 2007. Tinypeds: Tiny persistent encrypted data storage in asynchronous wireless sensor networks. Ad Hoc Networks, 5: 1073-1089.

He, D., C. Chen, S. Chan and J. Bu, 2012. DiCode: DoS-resistant and distributed code dissemination in wireless sensor networks. IEEE T. Wirel. Commun., 11: 1946-1956.

Mambo, M., K. Usuda and E. Okamoto, 1996. Proxy signatures for delegating signing operation. Proceedings of the 3rd ACM Conference on Computer and Communications Security, ACM, pp: 48-57.

Mehta, M. and L. Harn, 2005. Efficient one-time proxy signatures. IEE P- Commun., 152: 129.

Newsome, J. and D. Song, 2003. GEM: Graph EMbedding for routing and data-centric storage in sensor networks without geographic information. Proceedings of the 1st International Conference on Embedded Networked Sensor Systems. ACM, pp: 76-88.

Ray, I. and M. Toahchoodee, 2007. A Spatio-temporal Role-Based Access Control Model. In: Barker, S. and G.J. Ahn (Eds.), Data and Applications Security. Springer Berlin, Heidelberg, pp: 211-226.

Ray, I. and M. Toahchoodee, 2008. A Spatio-temporal Access Control Model Supporting Delegation for Pervasive Computing Applications Trust, Privacy and Security in Digital Business. Furnell, S., S. Katsikas and A. Lioy (Edn.), Springer Berlin, Heidelberg, pp: 48-58.

Shamir, A. and Y. Tauman, 2001. Improved online/offline signature schemes. CRYPTO Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology, Springer, London, UK, pp: 355-367.

Shucheng, Y., R. Kui and L. Wenjing, 2009. FDAC: Toward Fine-Grained Distributed Data Access Control in Wireless Sensor Networks. INFOCOM, IEEE. Worcester, MA, pp: 963-971.

Youssou Faye, I.N. and N. Thomas, 2011. A survey of access control schemes in wireless sensor network. World Acad. Sci. Eng. Technol., 59: 814-823.