Research on Trusted Certification Mechanism of Sensing Layer of the Internet of Things

CHEN Chunzi

Department of computer, Beijing University of Technology, Beijing 100124, China

504922294@qq.com

Keywords: Internet of things; Sensing network; Trusted computing; Trusted certification

Abstract: The trusted certification scheme is an effective means to solve the network security problems. However, the existing scheme does not consider the trusted problems of the network and nodes of the sensing layer. Based on this, this paper proposes a trusted certification mechanism of Sensing Layer of the Internet of Things. This mechanism combines certification and trusted computing, and realizes the mutual identity certification and platform integrity certification of sensing nodes. Compared with the existing scheme, the scheme proposed in this paper has a great improvement in security.

Introduction

With the rapid development of wireless communication technology, micro manufacturing technology, and various sensors thereafter, Internet has become the emerging network, is a new research direction in the field of information technology. [1] The Internet of things mainly consists of three layers: the sensing layer, the network layer and the application layer.[2] The sensing layer network can be called the sensing network. Each sensor node can only handle a limited amount of processing, which is characterized by limited resources and limited energy. [3]

Wireless networks are more vulnerable to privacy and security than wired networks.[4] Although there have been many researches on trusted certification mechanism of sensing layer of Internet of things, but there are not really aware of the trusted solution of nodes and the network. Based on this, this paper puts forward a trusted certification mechanism of Sensing Layer of the Internet of Things, in order to ensure that the node's identity is trusted and the transmission of data is reliable.

Trusted Certification Mechanism of Sensing Network

Two-Way Identity Certification When the Sensing Node Joins the Cluster Network. (1) The sensing node N identifies its identity ID_N, the type of the sensing node type, and requests the information Req to be sent to TCN, requesting to join the cluster network.

(2) After TCN receives the information, check the type of the sensing node. If the type of the sensing node N conforms to the cluster network requirement, TCN uses the identity ID_N of the sensing node N to obtain the certification keys K_{CN} of both parties. TCN selects random numbers r_C and serial numbers T_C and calculates $\{r_C \| T_C \| ID_N\}_{K_{CN}}$,TCN sends $\{r_C \| T_C \| ID_N\}_{K_{CN}}$ and r_C to the sensing node N .

(3) The sensing node uses the identity ID_C of TCN to obtain the certification keys K_{CN} of both parties. The sensing node N decrypts $\{r_C \| T_C \| ID_N\}_{K_{CN}}$ to verify the correctness of the signature. The sensing node N selects the random number r_N and the serial number T_N and computes $\{r_N \| T_N \| ID_N\}_{K_{CN}}$, the sensor node N send $\{r_N \| T_N \| ID_N\}_{K_{CN}}$, r_N to TCN.

(4) TCN decrypts $\{r_N \| T_N \| ID_N\}_{K_{CN}}$ to verify the correctness of the signature.

At this point, TCN and sensing node N use the shared communication key $\hat{k}_{CN} = \{r_C, r_N\}_{K_{CN}}$ to establish secure channels.

Platform Integrity Certification. (1) the trusted root TPM N of the sensing node N will send its platform integrity signing certificate AIK_N, $\{ID_N, \hat{r}_N\}_{AIK_N}$ to TCN. In which, $\hat{r}_N$ is anti - replay random number.

(2) TCN's trusted root TPM C will send its own certificates AIK_C, $\{ID_C, \hat{r}_C\}_{AIK_C}$ and AIK_N, $\{ID_N, \hat{r}_N\}_{AIK_N}$ to trusted certification center of the Internet of things (TC-IOT). In which, $\hat{r}_N$ is anti-replay random number.

(3) TC-IOT verify the validity of the certificate AIK_C and AIK_N. TC-IOT decrypts $\{ID_N, \hat{r}_N\}_{AIK_N}$ and $\{ID_C, \hat{r}_C\}_{AIK_C}$ to verify the correctness of the signature. TC-IOT uses its shared key K_C, K_N with TPM C and TPM N to calculate $\{\hat{r}_C + 1, k_{CN}\}_{K_C}$, $\{\hat{r}_N + 1, k_{CN}\}_{K_N}$, and send then to TPM C and TPM N separately.

(4) TPM C and TPM N use the shared key to decrypt $\{\hat{r}_C + 1, k_{CN}\}_{K_C}$, $\{\hat{r}_N + 1, k_{CN}\}_{K_N}$ and obtain the certification key k_{CN} of the platform integrity of both parties respectively.

(5) TPM C sends the integrity request information $Req\{i_1, ..., i_r\}$ to TPM N, In which, $\{i_1, ..., i_r\}$ is the PCR integrity identification corresponding to the sensing node.

(6) TPM N sends the integrity information $\{nPCR_1, ..., nPCR_r\}_{k_{CN}}$ and the integrity request information $Req\{j_1, ..., j_s\}$ to TPM C, in which $\{j_1, ..., j_s\}$ is the PCR integrity identification for TCN.

(7) TPM C verify integrity information $\{nPCR_1, ..., nPCR_r\}_{k_{CN}}$, and according to the value of completeness information $\{nPCR_1, ..., nPCR_r\}_{k_{CN}}$, judge if the sensing node N is trusted, if the judge result is not trusted, refuse sensing nodes to join the cluster network. TPM C sends TCN integrity information $\{cPCR_1, ..., cPCR_r\}_{k_{CN}}$ to TPM N.

(8) TPM N verify integrity information $\{cPCR_1, ..., cPCR_r\}_{k_{CN}}$, and according to the value of completeness information $\{cPCR_1, ..., cPCR_r\}_{k_{CN}}$, judge if TCN is trusted, if the judge result is not trusted, the sensing node N refused to join the cluster network.

At this point, the mutual identity certification and platform integrity certification between the trusted cluster head node TCN and the sensing node N are completed.

This article uses BAN logic to make inference to ensure the correctness of the key generated in the process of trusted identity certification and platform integrity certification.

Inference rules:

(1) rules of message meaning.

$$\frac{P \mid\equiv Q \xleftrightarrow{K} P, P \lhd \{X\}_K}{P \mid\equiv Q \sim X} \tag{1}$$

(2)temporary value validation rules.

$$\frac{P \mid\equiv \#(X), P \mid\equiv Q \mid\sim X}{P \mid\equiv Q \mid\equiv X} \tag{2}$$

(3) arbitration rules

$$\frac{P \mid\equiv Q \mid\Rightarrow P, P \mid\equiv Q \mid\equiv X}{P \mid\equiv X} \tag{3}$$

(4) belief rules

$$\frac{P \mid\equiv X, P \mid\equiv Y}{P \mid\equiv (X, Y)} \quad \frac{P \mid\equiv (X, Y)}{P \mid\equiv X} \quad \frac{P \mid\equiv Q \mid\equiv (X, Y)}{P \mid\equiv Q \mid\equiv X} \tag{4}$$

(5) sending rules

$$\frac{P \mid\equiv Q \mid\sim (X,Y)}{P \mid\equiv Q \mid\sim X} \tag{5}$$

(6) receiving rules

$$\frac{P \lhd (X,Y)}{P \lhd X} \quad \frac{P \lhd < X >_Y}{P \lhd X} \quad \frac{P \mid\equiv Q \overset{K}{\longleftrightarrow} P, P \lhd \{X\}_K}{P \lhd X} \tag{6}$$

$$\frac{P \mid\equiv Q \overset{K}{\longrightarrow} P, P \lhd \{X\}_K}{P \lhd X} \quad \frac{P \mid\equiv Q \overset{K}{\longrightarrow} P, P \lhd \{X\}_{K^{-1}}}{P \lhd X} \tag{7}$$

(7) fresh rules.

$$\frac{P \mid\equiv \#(X)}{P \mid\equiv \#(X,Y)} \tag{8}$$

Initialization hypothesis according to BAN logic:

$$TCN \mid\equiv TCN \overset{K_{CN}}{\longleftrightarrow} N \tag{9}$$

$$N \mid\equiv TCN \overset{K_{CN}}{\longleftrightarrow} N \tag{10}$$

$$\text{TPM TPM}\, C \mid\equiv C \overset{K_C}{\longleftrightarrow} TC - IOT \tag{11}$$

$$\text{TPM TPM}\, N \mid\equiv N \overset{K_N}{\longleftrightarrow} TC - IOT \tag{12}$$

$$TCN \mid\equiv \#(r_C) \tag{13}$$

$$N \mid\equiv \#(r_N) \tag{14}$$

$$\text{TPM}\, C \mid\equiv \#(\hat{r}_C) \tag{15}$$

$$\text{TPM}\, N \mid\equiv \#(\hat{r}_N) \tag{16}$$

$$\text{TPM TPM}\, C \mid\equiv TC - IOT \mid\Rightarrow C \tag{17}$$

$$\text{TPM}\, N \mid\equiv TC - IOT \mid\Rightarrow \text{TPM}\, N \tag{18}$$

Logical reasoning:

(a) proof $TCN \mid\equiv N \mid\equiv TCN \overset{\hat{k}_{CN}}{\longleftrightarrow} N$:

$TCN \lhd \{r_C \parallel r_N \parallel ID_N\}_{K_{CN}}$

From the initialization hypothesis (9) and rule (1) can get:

$TCN \mid\equiv N \sim \{r_C \parallel r_N \parallel ID_N\}$

From the initialization hypothesis (13) and the rule (5) can get:

$TCN \mid\equiv \#\{r_C \parallel r_N \parallel ID_N\}$

By rule (2) can get:

$TCN \mid\equiv N \mid\equiv \{r_C \parallel r_N \parallel ID_N\}$

so

$TCN \mid\equiv N \mid\equiv TCN \overset{\hat{k}_{CN}}{\longleftrightarrow} N$

(b) proof $N \mid\equiv TCN \mid\equiv TCN \overset{\hat{k}_{CN}}{\longleftrightarrow} N$:

$N \lhd \{r_N \parallel ID_C\}_{K_{CN}}$

From the initialization hypothesis (10) and rule (1) can get:

$N \mid\equiv TCN \sim \{r_N \parallel ID_C\}$

From the initialization hypothesis (14) and the rule (5) can get:

$TCN \mid\equiv \#\{r_N \parallel ID_C\}$

By rule (2) can get:

$N \mid\equiv TCN \mid\equiv \{r_N \parallel ID_C\}$

so

$N \mid\equiv TCN \mid\equiv TCN \overset{\hat{k}_{CN}}{\longleftrightarrow} N$

(c) proof $\text{TPM}\, C \mid\equiv C \overset{k_{CN}}{\longleftrightarrow} N$:

Note that TPM C and TPM N interactions are encrypted using the communication key generated in the previous step, which ensures the privacy of the interaction and the efficiency of the interaction.

TPM $C \triangleleft \{AIK_N, \hat{r}_C, k_{CN}\}_{K_C}$

From the initialization hypothesis (11) and the rule (1) can get:

TPM $C \mid\equiv IOTTC \sim \{AIK_N, \hat{r}_C, k_{CN}\}$

From the initialization hypothesis (15) and the rule (5) can get:

TPM $C \mid\equiv \#\{AIK_N, \hat{r}_C, k_{CN}\}$

By rule (2) can get:

TPM $C \mid\equiv IOTTC \mid\equiv \{AIK_N, \hat{r}_C, k_{CN}\}$

so

TPM $C \mid\equiv IOTTC \mid\equiv C \xleftrightarrow{k_{CN}} N$

From the initialization hypothesis (17) and the arbitration rule (3) can get:

TPM $C \mid\equiv C \xleftrightarrow{k_{CN}} N$

(d) proof TPM $N \mid\equiv C \xleftrightarrow{k_{CN}} N$:

TPM $N \triangleleft \{AIK_C, \hat{r}_N, k_{CN}\}_{K_N}$

From the initialization hypothesis (12) and the rule (1) can get:

TPM $N \mid\equiv IOTTC \sim \{AIK_C, \hat{r}_N, k_{CN}\}$

From the initialization hypothesis (16) and the rule (5) can get:

TPM $N \mid\equiv \#\{AIK_C, \hat{r}_N, k_{CN}\}$

By rule (2) can get:

TPM $N \mid\equiv IOTTC \mid\equiv \{AIK_C, \hat{r}_N, k_{CN}\}$

so

TPM $N \mid\equiv IOTTC \mid\equiv C \xleftrightarrow{k_{CN}} N$

From the initialization hypothesis (17) and the arbitration rule (3) can get:

TPM $N \mid\equiv C \xleftrightarrow{k_{CN}} N$

The interaction between TPM C and TPM N can be obtained:

TPM $C \mid\equiv N \mid\equiv C \xleftrightarrow{k_{CN}} N$

TPM $N \mid\equiv C \mid\equiv C \xleftrightarrow{k_{CN}} N$

Scheme Comparison

The table below gives a comparison of the schemes proposed in this paper and the existing scheme.

Table 1 scheme comparison

	Solutions in this paper	Existing scheme[5]
Expandability	good	It costs more to expand.
Certification	Has the identity and the platform integrity double authentication mechanism, has the good security.	There is only an certification mechanism.
Key distribution	A key distribution scheme based on vector space is adopted, and the key distribution efficiency and computational efficiency are high.	The key of all nodes is saved by the base station, and the key distribution efficiency is low.
Amount of calculation	The calculation is small and fixed.	big

Conclusion

The trusted certification mechanism proposed in this paper realizes the mutual identity certification and platform integrity certification between the sensing node and the cluster head node, and the analysis shows that the proposed scheme is superior to the traditional one.

Acknowledgements

First of all, I want to sincerely thank my mentor, Prof. Shen Changxiang. He gave me a lot of help in learning, the environment and other aspects, which made me make great progress in learning and research. I also want to thank the teachers of trusted computing laboratory, teacher Gong Bei and teacher Ning Zhenhu, for their guidance and help in writing my essay. Their profound knowledge, rigorous scholarship, approachable charisma, tireless teacher style, working style of improvement, tireless education and optimistic and open-minded attitude of life have deeply influenced me.

Reference

[1]M. Junaid, M. A. Shah and I. A. Satti, "A survey of internet of things, enabling technologies and protocols," 2017 23rd International Conference on Automation and Computing (ICAC), Huddersfield, 2017, pp. 1-5.doi: 10.23919/IConAC.2017.8082058

[2]A. G. Dinker and V. Sharma, "Attacks and challenges in wireless sensor networks," 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, 2016, pp. 3069-3074.

[3]Y. Liu, C. Zhu and P. Yan, "An energy-saving spectrum sensing scheme with combined clustering and censoring in cognitive wireless sensor networks," 2017 9th International Conference on Wireless Communications and Signal Processing (WCSP), Nanjing, China, 2017, pp. 1-6.

doi: 10.1109/WCSP.2017.8170892

[4]H. Wu, F. Yao, Y. Chen, Y. Liu and T. Liang, "Cluster-Based Energy Efficient Collaborative Spectrum Sensing for Cognitive Sensor Network," in IEEE Communications Letters, vol. 21, no. 12, pp. 2722-2725, Dec. 2017.doi: 10.1109/LCOMM.2017.2758376

[5]M. El-hajj, M. Chamoun, A. Fadlallah and A. Serhrouchni, "Analysis of certification techniques in Internet of Things (IoT)," 2017 1st Cyber Security in Networking Conference (CSNet), Rio de Janeiro, Brazil, 2017, pp. 1-3.doi: 10.1109/CSNET.2017.8242006