Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Engineering 29 (2012) 4091 – 4095

Procedia Engineering

www.elsevier.com/locate/procedia

2012 International Workshop on Information and Electronics Engineering (IWIEE)

The Research of Access Control in the Application of VANET Based on UCON

Zhang Guoping[a]*, Gong Wentao[b]

[a]*School of Computer and Communication Engineering in China University of Petroleum, Dong Ying, China*
[a]*Internet and Education Technology Center in China University of Petroleum, Dong Ying, China*

Abstract

vehicle network is regarded as an important kind of the internet of things, and the application of vehicle network has attracted more and more attention by researchers, and the applications of vehicle network, such as how to download the date files in the high-speed car by collaborative cars becomes a new hot research topic, the existing researches focus on a single vehicle for a specific task, without taking the related access control strategy into consideration, this paper discusses the usage control of the vehicle network, using UCON control model to express the download task for its powerful expression and flexible authorized strategy, and the paper also proposes access control framework and usage control process in vehicle network, the paper gives the compositions of usage control model such as the subject and the object and the related attributes, and the conditions and the obligations and so on, which enhances the strategy to solve the continuity authorization during downloading the data files.

Key words—the internet of things; vehicle network, usage control, process.

1. Introduction

The concept of IOT (the internet of things) means the network, which contains radio frequency identification (RFID) [1], infrared sensors, global positioning systems, laser scanners and other information sensing device. Everything in IOT can be connected to internet according to the certain protocols, and exchange the information, thus to achieve intelligent identification, location, tracking,

* Corresponding author. Tel.: +1-867-894-3352;
E-mail address: zhanggp@upc.edu.cn.

1877-7058 © 2011 Published by Elsevier Ltd. Open access under CC BY-NC-ND license.
doi:10.1016/j.proeng.2012.01.625

monitoring and management of the network. IOT is also known as “the sensor network” in the international area, which is the concept of sensor networks in an expansion of things[2].

As ubiquitous network connectivity and mobile access become important parts of people’s lives, there is an increasing demand to access the internet for clients on cars. Although the goal can be achieved using 3G or 4G networks, high cost and poor performance become barriers. With large scale deployment of roadside access points (APs) using IEEE 802.11, researchers have paid more attention on helping cars access the Internet via APs. The feasibility has been demonstrated in recent research work [1]. The problem is that the communication range of APs is limited and Dark Areas (DAs) between APs can cause intermittent connectivity. A mobile client has to continue its download tasks within the next AP transmission range if it leaves an AP coverage area without finishing its downloading. The delay is unacceptable, especially in highway scenarios, where APs are deployed at gas stations or service areas anywhere from 8km~16km. The communication range of APs is about 300m~1300m and production phase is 1000m [2], which means if the speed of a mobile client is 100km/h, it will lose touch with the Internet for about 5 minutes~10 minutes. Furthermore, when a client just leaves the range of APs and has a demand of accessing the internet, it has to wait 5 minutes to 10 minutes for the next AP. That really slows the user down, and many date file couldn’t be downloaded due to the high speed and dark areas, thus the paper proposes the a scheme of cooperative downloading based on dynamic slot which could improve the total amount of data downloaded due to the collaboration of the cars, while vehicle network also raises many security issues, such as authorization security and authorization flexibility. IN order to solve the problem, the paper proposes the usage control used in the vehicle network, and also gives the usage control process between the cars when downloads the data files. Thus the rest of paper comes as following: the architecture of vehicle network and abstract of each part has been proposed in section 2, and the architecture and abstraction of usage control model in vehicle network are given in section 3, and the overall access process of access control are also proposed in the section, and the small examples are given in section 4, and the whole paper is summarized in section 5.

2. Framework and process of vehicle network based on UCON

2.1. Related research

In the industry, IOT has generally been recognized as three layers: the top is the application layer, it provides the people with the application services; the middle layer is data transmission network layer, it changes the date between the devices; the third layer is sensing layer. The application layer in vehicle network is much more complex, the numbers of subject and object becomes much more, and how to download data files in the high-speed cars is one of the application, and in order to solve the problem, the cooperative downloading in vehicular networks is first introduced by Nandan et al. [2] as a part of the protocol-SPAWN for cooperative content retrieval and sharing among users aboard vehicles. As far as cooperative downloading service and method is concerned [3].

Our work differs from this approach in that our work pays more attention on usage control of cooperative car selection algorithm in highway scenarios [4]. The new access control model [5] name UCON [6] model is proposed to solve the complex access control problem due to the powerful expression and security control strategy. The control model was first proposed in 2003 by professor sandhu, the model includes the subject [7] and the object of the access control, and conditions [8] and obligations and the various factors authorization policy.

In IOT access control, in particular, having relatively long-term continuous service to immediately revoke the usage or application service needs permission. The attributes of the subjects and the attributes of the objects are only changed after the access control in the traditional access control models [8]. The

attributes of the subjects and the attributes of the objects are only changed after the access control in the traditional access control models, thus the UCON model introduces the concept of mutability[10], it means the value of subject's attributes and the value of object's attributes could be changed not only after access control, but also during the access control, and the changes in the attributes will affect the permission in the subject's next access behavior [11,12], thus could meet the needs for the strict and secure control in vehicle network access contro.

2.2. Architecture of vehicle network

Our framework is based on a network layer design between application layer and sensing layer, and in the access control of vehicle network, there are several major objects such as vehicles customer whose want to download the data files, and the data files which can be downloaded, and the task vehicle which should download for the other cars, and roadside access points and so on.

The subject(S) of UCON in vehicle network is the car client (CC), which is the control of the application service, such as cars and some other moving devices which contain the sensor to indent the information.The attribute(S) of UCON in vehicle network is the Att(CC), which contains the information about the trust value of the car client, and the honest usage times of the application services, and speed of car ,and the id of the car ,and the direction of the car, and dishonest usage time of the application services, and some other properties and so on.The subject(O) of UCON in vehicle network is the Date File(DF), which lays in the application layer and requests the service information provided by the access points locates the wireless sensor network along the road.The attribute(O) of UCON in vehicle network is the Att(DF), which contains the service information such as the digital sources for the car, the length of the data file and the kinds of the data file and so on.The condition(C) of UCON in vehicle network is decided by the policies according to the wireless sensor network, such as the trust value of the car client, and the speed and direction of the car and other decision factors and so on. The condition(C) is the constraints according to the actual situation in wireless sensor network, such as limits of geographical location for the access point and so on.The oBligation(B) of UCON in vehicle network is according to the needs of the access points in the wireless sensor network. The obligation of the device should be done before or during the downloading the data file in high road.The Authorization (A) of UCON in vehicle network is set by the needs of usage control, and decided by the car client and the data file. The Authorization(A) is the functional predicates should be evaluated for usage control, and then returns whether the car clients have rights to download the certain data files.

2.3. The changes of state in vehicle network based on UCON

There are several important states in the vehicle network based on UCON as the following: Initial: the car client (CC) just on his car, and never asks for the downloading in the high speed car. Requesting downloading by itself: the car client (CC) requests for downloading the data file (DF) in the vehicle network, and ask for the access point (AP) along the road. Denied downloading: the car client denied its needs for the downloading the data file, due to the reason itself. Requesting downloading by others: the car client (CC) could not download the data file which supported by the access point due to all kinds of the reasons, such as the car's speed is too fast or access point could not connect to the car and so on. Downloading: the car client (CC) could download the data file (DF) with the help of access point. Revoked: the car client (CC) denied downloading the data file (DF) due to the condition could not meet, all the data file has been downloaded is make no use of. End: the car client (CC) has downloaded the data file (DF). All kinds of the states in the vehicle network based on UCON can be shown in Fig 2 as following.

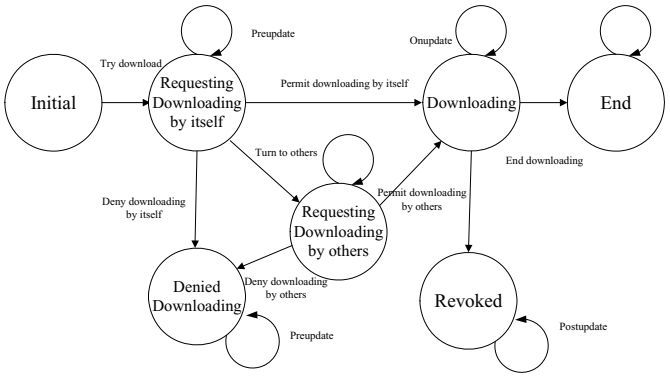

Fig.1. The states in vehicle network based on UCON

The car client should request downloading just after the authorization has been given by the access point, and the subject of downloading the data file can be the car client itself or by the others car clients.

Thus in the vehicle network, there are mang kinds of the car clients, when the speed of the car is too fast for the certain access point, then the other car client could do it for the other cars. and during the changes of the state in the vehicle network, the attributes of the car client could not only be changed after the downloading ,but also can be changed before the downloading or during the downloading .there are three kinds of the change functions as following:

Preupdate(atrr(CC)):the attributes of the car client and date files(DF) change before the downloading.

Onupdate(atrr(CC)):the attributes of the car client and date files(DF) change during the downloading the data files.

Postupdate(atrr(CC)):the attributes of the car client and date files(DF) change after the data files has been downloaded.

3. Access control process simulation

Suppose there are the devices and the application service in the certain wireless sensor network along the road, and there are only one car client and one data file in this simulation, and both of them have the properties about trust value, giving the explanation about the access process and the usage control functions, and formal logic description of this case are as follows:

Subject of UOCN in vehicle network: CC (car client)

Object of UCON in vehicle network: DF (data file)

Attributes (CC): { trust degree, money, honest times, dishonest times}

Attributes (DF): {threshold, number, money}

Obligation: {feedback the data file's information}

Condition :{ CC.money$\geqslant$0$\cap$CC.trustdegree$\geqslant$DF.threshold}

Times: CC's usage times using data file

OLTime: CC's online time using data file

Expense: CC's expense each time using data file

Punish: the punishment for data file's trust degree after each dishonest access control

Allowed(CC,DF,R)=>(CC.money$\geqslant$0$\cap$CC.trustdegree$\geqslant$DF.threshold)$\cap$(Max (speed) $\geqslant$ CC.speed0 $\cap$ Max (length) $\geqslant$DF.length))

PreUpdate (CC. money):CC.money = CC.money- OLTime *
Expense

PostUpdate (DF.money): DF.money = DF.money+OLTime * Expense

PostUpdate (CC.dishonest times): CC.dishonest times =
CC.dishonest times +1
PostUpdate (CC.trustdegree): CC.trust degree = CC.trust degree- Punish

In this case, the control of vehicle network, the car clients using the AP network resources to download the specific data files. In this case gives an honest file download process, we suppose that for the different direction's car couldn't cooperate due to their high speed which the access points and car client couldn't connect. And only certified authorized vehicle clients can download the resources, the registration of access control during downloading can be delivered, can be recovered, thus ensuring the flexibility to download authorized certification; and the authorization process conditions between car client between the data files have been restricted, thus authorization of usage control can be more flexible, and more strictly enforce the security of the access control in vehicle network.

4. Summary

In this paper, the collaborative of vehicle network during the downloading data files are discussed, and the architecture of usage control model in vehicle network is given, and the process of the access control when the car client downloads the data files is proposed , and the small instance is given in the end to prove the flexibility of authorization, thus the authorization for the usage control in vehicle network becomes easy and feasible.

5. Reference

[1]J. Ott and D. Kutscher. A Disconnection-Tolerant Transport for Drive-thru Internet Environments. In Proceedings of IEEE INFOCOM,Miami, March 2005.

[2] T. Kriplean, E. Welbourne, N. Khoussainova, V. Rastogi, M. Balazinska, G. Borriello, T. Kohno, D. Suciu: "Physical Access Control for Captured RFID Data", IEEE Pervasive Computing, vol . 6, no. 4, pp. 48-55, 2007.

[3] A. Juels, "RFID Security and Privacy: A Research Survey", IEEE Journal of Selected Areas in Communications, vol. 24, pp. 381 - 394, 2006.

[4] J. Park, R. Sandhu. The UCONABC usage control model . ACM Transactions on Information and Systems Security, 7 (1) :128-174, 2004.

[5] Xinwei Zhang. Formal Model and Analysis of Usage Control [D]. Virginia: George Mason University, 2006.

[6] J. Park, R. Sandhu. Towards usage control models: beyond traditional access control . ACM Symposium on Acesscontrol Models and Technologies, 2 (3) :57-64, 2002.

[7] J. Park, R.Sandhu.Security Architecture for Controlled Digital Information Dissemination, Proceedings of the Sixteenth Annual Computer Security Applications Conference (ASSAC) ,224-233, 2000.

[8] Fengying Wang,Fei WangThe Research and Application of Resource Dissemination Based on Credibility and UCON2007 International Conference on Computational Intelligence and Security, pp. 584-588, 2007

[9]R. Sandhu, E. Coyne, H. Feinstein, C. Youman. Role-Based Access Control Models . Computer, 1996.

[10] Kollmann, K.: Das„“Internet of Things“.Der kurze Weg zur kollektiven Zwangsentmündigung.Telepolis, www.heise.de/tp/r4/artikel/30/30805/1.html (2009)

[11]Ahn GH, Arvisandhu.Role-based Authorization Constrans Specification [L]. ACM Transcactions on Information and System Security, pp. 207-226, 2002.

[12] A. Jsang, R. Ismail, and C. Boyd. A survey of trust and reputation systems for online service provision . Decision Support Systems, 43(2): 618-644, 2007.