A Study about weight grant of Authentication level in USN environment

Bae-young Choi*, Byung-Ryul Ahn, Tai Myoung Chung****
*bychoi@imtl.skku.ac.kr
**anbr0305@skku.edu
**tmchung@ece.skku.ac.kr

Abstract. The objects, which can be personal digital assistants, eleetronic rings, doors or even clothes, offer embedded chips with computation facilities and are generally called artifacts. I later realized that this was not so the real problem is actually authentication.. Recent results indicate scalability problems for flat ad hoc networks. Sensor network achieves function that handle surrounding information perception through sensor and sensed information to network that is consisted of sensor nodes of large number. Research about new access control techniques and height administration techniques need authentication information persons' certification assurance level classification in sensor network environment which become necessary different view base with authentication information at node for application of AAA technology in USN environment that must do authentication process using information that is collected from various sensor mountings. So, get base authentication information in sensor type and present weight grant model by security strength about authentication information through information who draw. In this paper collected information of sensor nodes model who give weight drawing security reinforcement as authentication information by purpose present be going to. and Must be able to can grasp special quality of each sensor appliances in various side and use this and decide authentication assurance level for value estimation as authentication information elements. Therefore, do to define item that can evaluate Authentication information elements thus and give simple authentication assurance level value accordingly because applying weight. Present model who give authentication assurance level value and weight for quotation according to security strength.

Keywords: Sensor network,Authentication Level,weight,USN,Authenticaton information,Sensor node, Authentication weight.

1 Introduction

1.1 Sensor network Abstract

Sensor network achieves function that handle surrounding information perception through sensor and sensed information to network that is consisted of sensor nodes of large number. Sensor network is network that is consisted of the amount, many sensors of that electric power first watch of the night to base network for ubiquitous computing. Number of sensor to compose network is very much and each sensor nodes have military strength and computing ability that is limited, and have insertion and property that Topology of sensor network can change easily by exclusion of frequent sensor nodes. Sensor network processes user's authentication information sensing information through sensor, because dependence for system rises, research about security of user's authentication information must consist together.

Examine about characteristic of sensor network in 2 chapter of these treatise. 3 chapter recognize about characteristic of security techniques about authentication information of sensor network. Examine about element characteristic about authentication information in sensor network in 4 chapter. Examine about method to decide weight about element of authentication information in sensor network in 5 chapter. Recognize about characteristic on security about authentication element weight in sensor network in 6 chapter. Refer about conclusion of treatise and forward research direction that see in 7 chapter

2 Sensor network Characteristic

Sensor nodes that compose sensor network are consisted of part that have sensor function and network function part for wireless data communication. Sensor nodes that have these structure is available limited radio communication, but the function is much lacking than general radio nodes. Sensor nodes must have peculiar environment than nodes that compose and appropriate existent radio network and use restrictive resources. Therefore, sensor nodes must keep Rauting route to use available resources maximum and pass data. Though sensor network means network that consist of sensor nodes of existence and nonexistence, each nodes use own processing ability for data transmission to interior chain of mountains and outside. It may say that is the most important technology that that electric power actions of network by many researches that is consisting present regarding sensor network, arrangement of fast node, jar improve propensitys such as composition, kickback prevention technology. Because detection of node position information, data transmission between each node is broth cast way system that is used by addition of program/variation military affairs/security that is executed at each sensor node or system that use expensive sensor node, contents of transmission data are passed to each nodes.

2.1 Sensor network Security

Sensor network surrounding environment information collection / in very sensitive applications as tool that analyze use . Very unique special quality of only sensor network need perfectly new quest in terms of the threat element or attack method, and security countermeasure for this than existent all other networks.

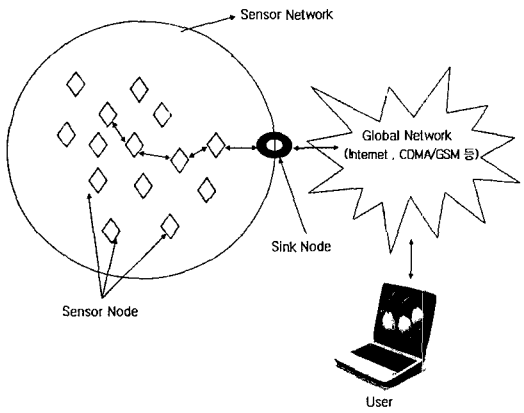

Figure 1. Senser Network structure

Can lift multi unit of measure Rauting and date aggregation etc. that main characteristic of sensor network that become head of a family issue in vantage point on security does limited ability of sensor node, vulnerability of physical security for sensor nodes, and broadcasting by main means of communication. Because can have chain of mountains, communication, save ability and source of energy that sensors are limited very for effectiveness of sensor network, restriction of security function as well as protocole for normal action follows.

End-to-end properties are usually considered as the highest level of security achievable, since all potential intermediaries are elimited. But end-to-end properties are nullified if an endpoint is compared and in sensor networks,every node is an endpoint.

Possible failure of nodes should be designed into algorithms for sensor network as it is highly likely that a certain percentage of them will fail during normal operation. A sensor network should be able to tolerate a cedrtain number of malicious node as well.

sensor network is established in area that person's access is difficult, is very weak in physical attack because is operated in long term state that is allowed. Special quality that limited ability of sensor and communication ability must do to add difficulty on more vulnerabilitys and security than one to one communication because do so that may use broadcasting that is limited by contiguity node by main communication method, and do partial processing for light oil message of middle nodes for electric power or efficient use of important duty width specially creates Security still more hardly..

2.1 Security requirement of sensor network

Important item in side that is security enemy in sensor network must do so that can not see sensitive information except node in permission that is quoted according to continual stream of data between node and when this encrypts data to secret height, data exchange must consist. That is, must guarantee secret department of data. There is important security requirement in application that quotation of message is many in sensor network. Because attacker can insert message easily, it is thing which must confirm whether is that data that listener is used at policy direction decision process comes originally from user. Authentication of data can consist through pure symmetry height mechanism in case of communication anyway. Sender and listener do to share secret height to create message authentication code (Message Authentication Code: MAC) cost about all data communications. In case correct MAC value is received, listener verifies truth of message that is sent by sender. .but must do Broadcasting communication. But, late height exposure and only direction function height chain are proposal by way that open height way solves these problems because actual computing power or resources need is big. Data integrity secures data integrity through data authentication in SPINS by thing to confirm upside of data/variation availability that listener receives in communication.

It is security service that secures that integrity of data is data that send most recently as technology to prevent ashes use about data that send before.

3. Sensor network authentication element

3.1 Authentication level abstract

Kinds of existed various sensor appliance have created authentication information of different form for authentication.

For example, fingerprint awareness, wide-open door awareness, face awareness, hand shape awareness in case of living body awareness .There is iris/retina awareness, cleaned barley awareness etc. Various awareness ways, has created peculiar authentication information of each single person using actuality such physical characteristic. Must be able to can grasp special quality of each sensor appliances in various sides and use this and decide authentication assurance level for value estimation as certification benevolent person. Therefore, do to define item that can evaluate authentication element thus and give simple authentication assurance level value accordingly because applying weight. Do to give authentication assurance level value

3.2 Authentication level importance

Authentication element have different security importance according to that have some input route to in formativeness that is used in user certification and apply to AAA that even if do different identification, information it is ultimate purpose finally, between authentication element information according to relation mutually change be able to must .

Authentication information that is inputs from various sensor devices compose user's identification chisel paper through Mapping and convergence between authentication element and authentication is achieved with this information.

Authentication can grasp right and user's state by user can be given competence and grasp user's service utilization time after competence is given being achieved.

Can grasp special quality of each sensor appliances in various sides for value estimation as authentication element and must be able to decide authentication assurance level that use this.

Therefore, do to define item that can evaluate authentication element simple authentication assurance level value accordingly

because applying weight? Assurance level that is defined by this method may aid in security talk between various authentication elements.

4.Authentication power importance

4.1 Authentication power difference by authentication element

Sensor network technology promise a vast increase in automatic data collection capabilities through efficient deployment of tiny sensing devices. Sensor networks use numerous small, inexpensive nodes that can sense,compute, and communicate with each other to interact with the physical world. Sensors must be small and inexpensive to make it reasonable so that there can be many of them. Many are needes to allow them to be physically present throughout the environment.
We will now take a look at the security of this authentication mechanism. The goal of a person trying to break the systyem is to authenticate as a legitimate user.
Can decide security grade of authentication information with peculiar information of each single person which accept from node of sensor appliances.
and,Authentication information of sensor nodes that appear according to security strength is appearing to differ.
Can grasp and decide assurance level of authentication for special quality of sensor equipments in number of various case through authentication estimation and danger about strength and height of security according to grade of various authentication information and security strength of information are decided.
Evaluating value of authentication seal at sensor node, present simple authentication assurance stage because deciding security strength for quotation and give grade and give authentication element weight for quotation and apply the weight.Therefore, the importance of security about authentication element that sensor nodes according to weight get passing through the authentication assurance step is refered

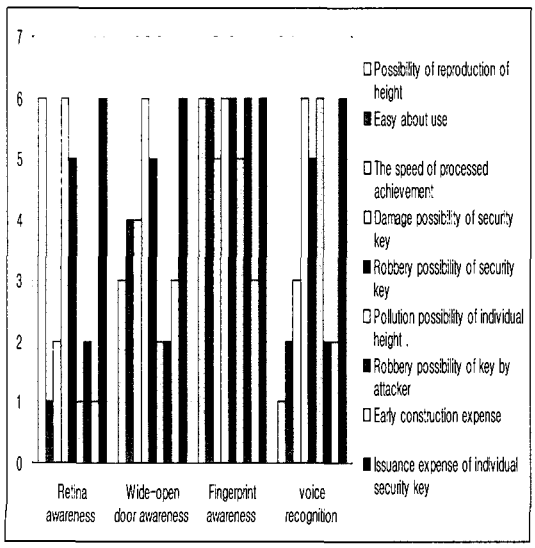

Figure 2.Authentication element security power

4.2 Authentication power difference by authentication element analysis

It is thing which consider confidentiality and integritys of data about authentication information judging robber of security to authentication information at sensor node and do to give element weight about authentication information.
Examined what characteristic according to security authentication element of figure 2 each authentication information have.
And such element information overcoming vulnerability of security in sensor network fundamental plan what it is investigate decide to .
Satisfy authentication and integrity that is security requirement in sensor network through information that recognize in user's body who come figure 1 and approach to network together.
And, is going to present model who put authentication element level according to this security importance and give weight authentication element prices of authentication information of sensor network that is consisted of hundreds several thousands sensor nodes have importance of different security according to input path of sensor strings.
As see in a ticket specially over, deduction of authentication element information that take advantage of living body awareness technology can guarantee secret department of security information that easy of support and different authentication element acquisition in different living body awareness of do various authentication chairman are done special quality Tuesday.
Also, it need limited ability of sensor node, grant of authentication level for authentication element cost of information that is collected in this sensor network in vulnerabilitys of physical security for sensor nodes and research about weight that is main characteristic of Senseon network that become head of a family problem if see from viewpoint on security.
Because giving weight about authentication element price of authentication information, is seeing that can establish system about security of authentication element price and establish basis of solution about vulnerability of sensor network security.

5.Authentication element weight

5.1 Authentication element weight Model

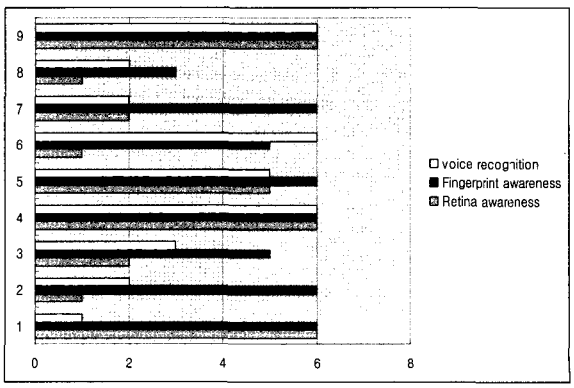

Figure 3 .Authentication element weight models

With figure 3, authentication information's of sensor network through various living body recognition description have high security strength.
Therefore, reproduction or that is returned to life of authentication element through nodes in sensor network is that authentication information impossible can keep security in sensor network.
Also, living body awareness technology is state that an experiment about security robber finishes already with figure 3, it is step practical practicality in been developing USN environment now.
It thinks Security of network of wide meaning that sensor network that is in living body recognition technology is not that this ticket means and grant about weight of authentication information of living body recognition technology is that is going to make standard of weight grant of authentication information that is netted in other sensor devices.
Now security reinforcement in sensor network to repeal and give authentication level of authentication information by weight grant by security strength user's authentication level give must .
Also, with above picture, development of encryption techniques through weight grant was available about authentication information of other sensor appliances that is not living body recognition technology.

6.Authentication weight Advantage

Various kinds authentication mode is used in USN environment.
Various authentication ways compose safe authentication mode combining each other.
Technology of living body awareness is becoming one method that can have peculiar authentication element in sensor network and do efficiency of security greatest.
Is going to be giving authentication level by various methods with shame which is authenticity that is becoming differentiation
It is current password or sensor of way such as card security in sensor network is connoting fair problem about danger of the security.
Have user's diagnostic mechanism and estimation about variety of authentication way should be achieved for deduction of various authentication information
That is, can enhance more level of trust all according to user's case which quote through authentication method more than one to seek information that authenticity is and receive authentication element value through grant about weight
It is classification by level for authentication element quotation that become this background to develop into techniques about techniques of new access control and key administration technique with authentication information for authentication technology or AAA technology application used in existent network environment in USN environment.
Therefore, weight grant research through classification of authentication level may talk that is the most excellent plan solidifies security in sensor network.

7.Conclusions

Authentication in sensor network has created one authentication information with peculiar recognition information of individual during fingerprint recognition such as recognition of various sensing data that is living body or face recognition. Hand shape awareness, iris/retina awareness various recognition ways.
That is, pass through process that have this authentication element and create peculiar authentication information for single quotation and give authentication level and give simple authentication assurance level value giving weight and do authentication of appliance
Information for quotation in sensor network has peculiar awareness information and does each single person's authentication.
This paper executes authentication recognizing position information of node and the position information is integrated by sensor information between nodes.
Recognize information by tag and recognize authentication information of each appliance according to the information.
Quote information that have realized information between node
Therefore, authentication element user who accepts to secure safety of information that is netted at nodes in sensor network of give level voluntarily and give weight according to security strength must.
And research that continuous research reactor completes weight grant of authentication information in various sensor network and present systematic model of authentication information via encryption process may have to be continued.

8. References

[1] Sencun Zhu, Sanjeev Setic, and Sushil Jajodia. LEAP:Efficient Security Mechanisms for Large-Scale Networks. In Proceedings of the 10th ACM Conference on Computer and Communications Security(CCS),pages 62-72.ACM Press, 2003.

[2] L.Eschenauer and V. D. Gligor. A Key-Management Scheme for Distributed Sensor Networks. In CCS'02. ACM, 2002.

[3] Chrisx Karlof and David Wagner. Secure Routing in Wireless Sensor Networks Elsevier Ad Hoc Networks, 1(2-3):295-315. September 2003.

[4] H.Chan and A.Perrig, Security and privacy in sensor networks, IEEE Computer, October 2003, PP.103-105.

[5] L.Eschenauer and V.D.Gligor, A key-management scheme for distributed sensor networks, ACM CCS 2002, Nov.2002.

[6] F.Hu, J.Ziobro, J.Tillet and N.Sharma, Secure wireless sensor networks :Problems and solutions ,J.of SCI,to appear,2004

[7] D.Liu and P.Ning, Efficient distribution of key chain commitments for broadcast authentication in distributed sensor networks, NDSS' 03,2003.