A Novel Access Control Scheme to Construct Fresh Database of Ambient Information in Internet of Things

A Novel Access Control Scheme to Construct Fresh Database of Ambient Information in Internet of Things

Yuichi Kawamoto[†], Hiroki Nishiyama[†], Nei Kato[†], Yoshitaka Shimizu[‡], Atsushi Takahara[‡], and Tingting Jiang[§]
[†]Graduate School of Information Sciences, Tohoku University, Sendai, Japan
[‡]NTT Network Innovation Laboratories, NTT Corporation, Yokosuka, JAPAN
[§]Virginia Polytechnic Institute and State University, Blacksburg, VA, USA
E-mails: [†]{youpsan, bigtree, kato}@it.ecei.tohoku.ac.jp
[‡]{shimizu.yoshitaka, takahara.atsushi}@lab.ntt.co.jp, [§]virjtt03@vt.edu

***Abstract*—The development of technologies for realizing “Internet of Things” inspire many applications which utilize the things’ network. Additionally, the ambient information of the things including various information collected via the network has attracted much attention as useful data for novel applications. By collecting the ambient information from things and constructing databases of them, it is expected to make our lives smarter and more convenient. On the other hand, to maximize the advantage of such a database, it is important to keep the information in the database as fresh as possible. However, in order to keep the freshness of the database, periodically collecting data with short interval is needed, which causes heavy traffic congestion when we use the traditional access control schemes in the existing communication network technologies. Thus, in this paper, we propose a novel access control scheme to keep the freshness of the database while avoiding traffic congestion. Additionally, an optimization to improve the efficiency of our proposed method is provided with mathematical expressions. Moreover, numerical results verify the effectiveness of our proposal.**

***Index Terms*—Ambient information, Internet of Things (IoT), Access control scheme, and Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA).**

I. Introduction

In recent years, the development of communication devices and wireless network technologies accelerates the spread of the concept of “Internet of Things (IoT)” [1]–[3]. Many “things” will be connected to the network by using different wireless communication technologies and many applications using the information collected from the things’ network will be available [4]–[8]. Especially, the ambient information, which is collected from large quantity and variety of things, has attracted much attention to be utilized for controlling the numerous things in many applications. Among many different approaches, user participatory sensing was considered as an efficient way to collect the ambient information. As shown in Fig. 1, by collecting the ambient information that each user observed, it is possible to construct various databases, which can be used in many applications. However, due to the large number of the things, which increase drastically day by day, it is unsatisfactory to collect the ambient information and control the things by using existing communications schemes. Although almost all traditional communications schemes have aimed to increase the network performance such as high throughput, low delay, and so forth, there are still some limitations that make it difficult to satisfy all requirements of IoT. Thus, it is needed to flexibly utilize network technologies to satisfy different the requirements from different applications in IoT. In this paper, we focus on technology utilizing ambient information observed from surrounding network environment as an example of the applications in IoT.

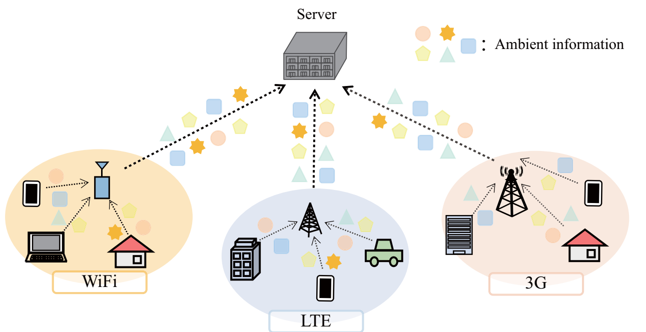


Fig. 1. An example of a system where each user sends the collected ambient information to a server to construct a database.

One of the technologies using the ambient information and user participatory sensing is a novel security system, which uses the ambient information observed from surrounded network environment to realize security enhancement for mobile users in wireless networks [9]–[11]. In this technology, ambient radio signals are utilized to make a user’s fingerprint, which certifies the location of the user. Nowadays, there are many radio signals around us such as LTE, 3G, WiFi, Bluetooth, and Zigbee signals, which are available to be observed. Additionally, the aspects of the signals such as the strength of signals are different from each user’s location. Thus, they can be used as the certification of user’s fingerprint at a certain place at a certain time. In this system, each user sends the collected ambient information to a server to construct a database for the security system. Moreover, the database is updated in realtime by collecting the information at regular interval to keep the database fresh. When some

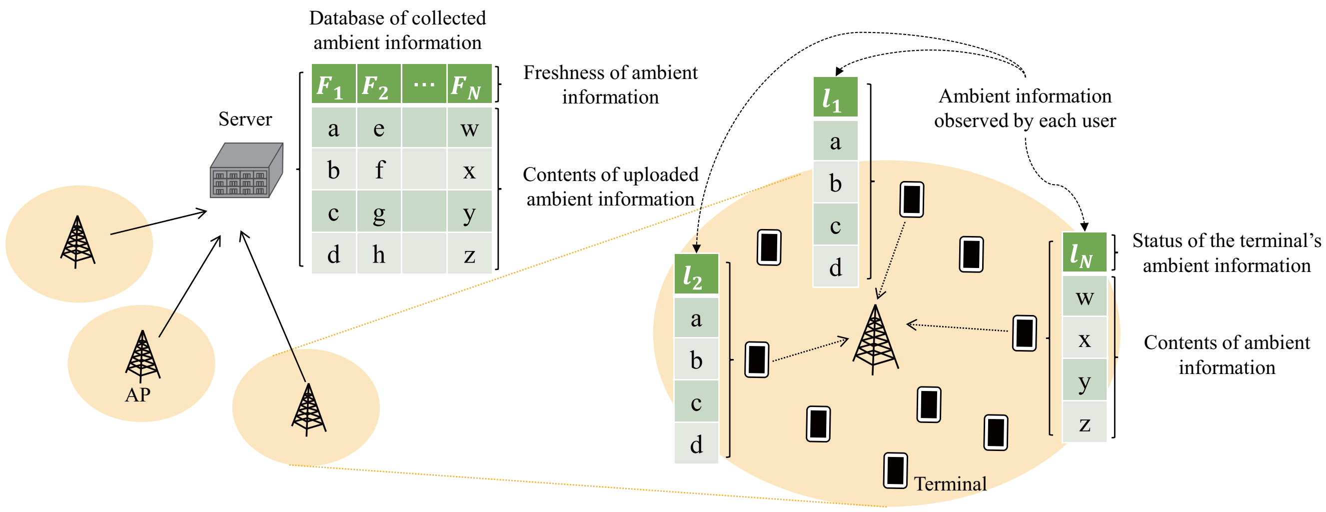


Fig. 2. Assumed network model.

authentications of users' location are required, the server runs the ambient information from the users with the information in the database. In this way, it is considered that novel systems using ambient information and such a database will be available with the spread of IoT technologies. In addition, in such systems, it is understood that the freshness of the database is very important.

However, as mentioned above, since the number of the "things" (including users' devices, from hereon, we call them as terminals) increases day by day and the ambient environment is changing all the time, it is difficult to keep the database fresh by using existing wireless communication technologies due to the limitation of the network capacity. Therefore, we propose a novel access control scheme to achieve fresh database of ambient information from numerous terminals in the wireless communication networks. In this proposal, the timing of sending data by each terminal is controlled by considering how fast the ambient environment at each terminal changes. As a result, it achieves to avoid traffic congestion while keeping the database fresh.

The remainder of this paper is organized as follows. The assumed network model is presented in Section II. Additionally, an existing access control method, namely Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA), is introduced in this section. Section III provides our proposed scheme to collect data from numerous terminals in IoT. Section IV introduces the results of numerical analysis. Finally, concluding remarks are provided in Section V.

II. Assumed Network Model and Access Control Scheme

In this section, we show the network model assumed in this paper. In the assumed network, as shown in Fig. 2, each AP collects the ambient information from the terminals covered by the AP and sends them to the server which constructs the database of the terminals' ambient information. Indeed, since the ambient environment of each terminal change continuously, the freshness of the database constructed at the server decreases momentarily. In order to keep the freshness, the database is updated regularly by the uploaded ambient information from the APs. Thus, each AP needs to periodically collect the ambient information of the terminals with a certain interval.

On the other hand, as the access control scheme used between the APs and terminals in the assumed network, CSMA/CA is supposed to be used. Additionally, it is assumed that the terminals covered by the same AP are close enough to each other to succeed the carrier sense. In the process of CSMA/CA, each terminal checks the usage condition of the channel and starts sending data if the terminal does not sense the usage of the channel for a random period of time called "backoff time". On the other hand, if the terminal senses the other terminal's usage of the channel, it stops the data sending process and wait until next interval. After waiting, the terminal starts retransmitting if the channel is free at that time. In the case where the data collision occurs by the data sending from multiple terminals at the same time, the terminal chooses the random backoff time again. At this time, the range of the chosen backoff time is increased in the process of CSMA/CA. By increasing the range in an exponential fashion each time when the terminal, it decreases the probability that the collision occurs again. In this process, the backoff time, BT, is calculated as the following expression:

$$BT = r \cdot t, \tag{1}$$

where r and t represent a random number and the length of a time slot. Additionally, the value of r is chosen from the range between 0 and CW, which is called contention window. The value of CW is decided from the following expression.

$$CW = (CW_{\min} + 1) \cdot 2^m - 1, \tag{2}$$

where $CW_{\min}$ and m shows the minimum value of the contention window and the number of retransmissions. The value of contention window increases along with the number of retransmission as shown in Eq. 2, and stops when the value exceeds the value of $CW_{\max}$, which denotes the maximum value of the contention window. After that, the random value, r, is chosen from the range between 0 and $CW_{\max}$ repeatedly.

III. Proposed access control scheme

In this section, at first, the summary of the proposed scheme, where the timings of sending traffic from terminals are optimized by considering the freshness of the database, is represented. Secondly, the optimization problem described by using mathematical expressions. Thirdly, the freshness of the two databases constructed by using the proposed scheme and existing scheme, respectively, is analyzed.

A. Summary of the proposed scheme

At first, we introduce the summary of the proposed access control scheme. As mentioned in previous section, keeping the freshness of the database is very important. However, in order to keep the freshness, it is necessary to periodically collect the ambient information from many terminals with a short interval, which causes heavy traffic congestion in the existing communication networks. Thus, in our proposal, the timing of sending traffic is controlled by considering the difference in the changing rapidity of each terminal's ambient information. For example, in the case of the security system that we introduce in Section I, the changing rapidity of each terminal's ambient radio signals is considered to be totally different from that the other terminals. The ambient radio signals around the terminals in crowded places may change continually. However, they usually do not change much in areas with sparse population of users. Thus, in the case of crowded places, the ambient information should be repeatedly collected to keep the database fresh while it is not necessary to collect the ambient information very often in uncrowded places. Therefore, we set the data sending interval of each terminal dynamically according to the rapidity of change of the terminal's ambient information.

To decide the data sending timing, each terminal regularly checks the changed ratio between its current ambient information and the information that the terminal sent to the server last time. We define the status of the current terminal's ambient information as l_i where i denotes the identification number of each terminal. l_i satisfies the following formulation:

$$0 \leq l_i \leq 1. \tag{3}$$

When the information is sent to the server, l_i equals to 1. It decreases with the changing ratio of the terminal's ambient information, and becomes 0 when the current ambient information becomes totally different from the information that the terminal sent to the server. Additionally, we define changing rapidity of the terminal's ambient information as x_i per slot.

In our proposal, each terminal starts the data sending process when l_i falls below a predetermined threshold, denoted by θ. The value of θ is set for each AP according to the condition of the area where the AP covers such as the number of terminals and the changing rapidity of the ambient information. Additionally, the value of θ is broadcasted from each AP to the terminals covered by the AP. Moreover, the value of θ needs the following condition:

$$0 \leq \theta < 1. \tag{4}$$

Thus, the interval from the previous data sending to the start of the next data sending process, Δ_i, is expressed as follows:

$$\Delta_i = \frac{1 - \theta}{x_i}. \tag{5}$$

If θ is set to a high value, the terminals have to periodically send its ambient information with a short interval, and thus traffic congestion may occur. On the other hand, the freshness of the database may decrease with the lower value of θ. Therefore, it is required to optimize the value of θ to keep the database fresh while avoiding traffic congestion.

B. Optimizing the value of θ

We analyze the optimal value of θ to keep the database as fresh as possible by using mathematical expressions. In this analysis, nonpersistent CSMA [12] is assumed to be used in the network. Additionally, the number of terminals in the area, which is covered by an AP, is defined as N. Then, we have following expression.

$$1 \leq i \leq N. \tag{6}$$

As noted previously, each terminal, i, starts the data sending process according to the interval Δ_i. Thus, when the proposed method is used, the rate of occurring traffic including the retransmission data from the terminals in to an AP, G (packets/slot), is expressed as follows:

$$G = \sum_{i=0}^{N} \frac{1}{\Delta_i}. \tag{7}$$

When the proposed method is not used, the value of G may be set by considering other network conditions such as throughput and delay.

On the other hand, the probability that the data sending of a terminal succeed, p_s, is introduced in [13] as follows:

$$p_{\mathrm{s}} = \frac{e^{-aG}}{G \cdot (1 + 2a) + e^{-aG}}, \tag{8}$$

where a denotes the ratio of propagation delay to packet transmission time. Additionally, the traffic occurring rate G is assumed to follow a Poisson distribution. Moreover, the throughput, S (packets/slot), is expressed as follows:

$$S = G \cdot p_{\mathrm{s}} = \frac{G \cdot e^{-aG}}{G \cdot (1 + 2a) + e^{-aG}}. \tag{9}$$

From the analysis on the throughput in previous researches [14], [15], it is shown that the function of S is convex upward with the value of G. Thus, there is the value of G that achieves the maximum value of the throughput. Therefore, we define the optimal value of θ, θ_{opt}, as the value that achieves the maximum throughput. Hence, the value of θ_{opt} is expressed as follows:

$$\theta_{\text{opt}} = \arg\max_{\theta} S. \tag{10}$$

C. The freshness of database

The guaranteed freshness of database in two cases where the proposed method is used or not is analyzed by using mathematical expressions. Here, we define the freshness of the ambient information of i^{th} terminal in the database at the server when the proposal is used or not as F_i^{prop} and F_i^{exist}, respectively. In addition, these values are needed to satisfy the following expression:

$$0 \leq F_i^{\text{prop}}, F_i^{\text{exist}} \leq 1. \tag{11}$$

Since the database at the server is updated every time when new ambient information is collected from terminals, the freshness depends on the expectation value of the time required to finish sending the data from the previous data sending. Thus, when the proposed method is not used, the expectation value of the required time, E_{exist}, is expressed as follows:

$$E_{\text{exist}} = \frac{N}{G_{\text{random}}} + A, \tag{12}$$

where G_{random} and A represent the rate of occurring traffic where the proposed method is not used and the expectation value of the required time when the data sending is missed and the retransmission is carried out in several occasions. On the other hand, $\frac{N}{G_{\text{random}}}$ denotes the average required waiting time from the previous data sending to start next data sending process. Moreover, the value of A is expressed in Eq. 13 where ω denotes the number of retransmissions when the value of contention window reaches $CW_{\max}$. Using Eq. 2, the value of ω can be calculated as follows:

$$\omega = \frac{1}{\log 2} \cdot \log\left(\frac{CW_{\max}+1}{CW_{\min}+1}\right). \tag{14}$$

Thus, the average freshness of database at the server when the proposal is not used is expressed as follows:

$$\begin{aligned} F_i^{\text{exist}} &= 1 - \frac{E_{\text{exist}} \cdot x_i}{2} \\ &= 1 - \frac{1}{2} \cdot \left(\frac{N \cdot x_i}{G_{\text{random}}} + A \cdot x_i\right). \end{aligned} \tag{15}$$

On the other hand, when the proposed method is used, each terminal starts the data sending process when the status of the terminal's ambient information, l_i, falls below the value of θ_{opt}. Thus, the required time depends on the value of the changing rapidity of the terminal's ambient information, x_i. Therefore, the expectation value of the required time when the proposed method is used, E_i^{prop}, is expressed as follows:

$$E_i^{\text{prop}} = \frac{1-\theta_{\text{opt}}}{x_i} + A. \tag{16}$$

Hence, the freshness of the ambient information of each user in the database, when the proposal is used, is expressed as follows:

$$\begin{aligned} F_i^{\text{prop}} &= 1 - \frac{E_i^{\text{prop}} \cdot x_i}{2} \\ &= \frac{1}{2} \cdot (1 + \theta_{\text{opt}} - A \cdot x_i). \end{aligned} \tag{17}$$

From Eqs. 15 and 17, it is understood that the freshness of the database provided in the case where the existing access control method is used depends on the data occurring rate from the terminals. On the other hand, when the proposed method is used, it is controlled by the value of θ_{opt} which is calculated in the proposed method. Thus, it is clearly shown that we can control the freshness of the database of ambient information of terminals by adequately setting the value of the threshold in our proposal.

TABLE I
PARAMETER SETTINGS

Number of terminals (N)	10, 30, 50
Maximum value of contention window ($CW_{\max}$)	15
Minimum value of contention window ($CW_{\min}$)	1023
Length of a time-slot (t)	20μs
Ratio of propagation delay to packet transmission time (a)	0.5

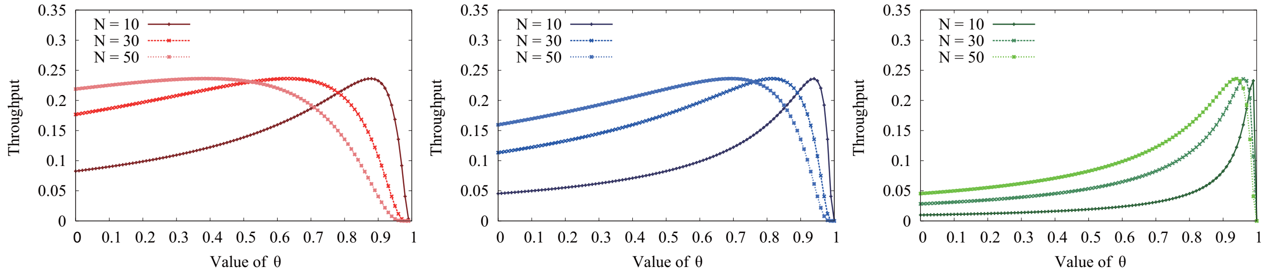
IV. Numerical analysis

In this section, we confirm the existence of the optimal value of θ by analyzing the relationship between the throughput and the value of θ. The numerical calculation results are provided to verify the analysis. Additionally, the effectiveness of the proposed method is also shown in the analysis on the minimum guaranteed freshness of the database of ambient information and the standard deviation of the freshness.

A. Parameter settings

The parameter settings are summarized in Table I. In this numerical analysis, for the simplicity, it is supposed that an AP collects the ambient information from the terminals in the coverage of the AP to construct the database at the server. The number of the terminals in the coverage of an AP is set to 10, 30, and 50, respectively, to evaluate multiple situations where the number of terminals are different. Additionally, the

$$A = \sum_{k=0}^{\omega-1} p_s \cdot (1-p_s)^k \cdot \frac{2^k \cdot CW_{\min} \cdot t}{2} + \sum_{l=\omega}^{\infty} p_s \cdot (1-p_s)^l \cdot \frac{CW_{\max} \cdot t}{2}. \tag{13}$$



(a) x = 0.01. (b) x = 0.005. (c) x = 0.001.

Fig. 3. Value of θ vs. throughput.

terminals are deployed randomly in the coverage of the AP. The AP collects the ambient information from the terminals by using CSMA/CA with or without the proposed method. As the parameters used in the process of CSMA/CA, the maximum and minimum values of the contention window are set to 15 and 1023, respectively. Moreover, the length of a time-slot and the ratio of propagation delay to packet transmission time are set to $20\mu s$ and 0.5, respectively. On the other hand, three situations to reflect the difference in the changing rapidity of ambient information are supposed in this numerical analysis. In the three situations, the average value of the changing rapidity of ambient information, x_{ave}, is set to 0.01, 0.005, and 0.001, respectively. Additionally, in each case, the changing rapidity of ambient information is randomly chosen from the value at up to 5% above or below the average value. Furthermore, we assumed that the retransmission from the terminals can only occur maximum three times.

B. Existence of the optimal value of θ

At first, the existence of optimal value of θ which maximizes the freshness of the database of ambient information is proved. Fig. 3 shows the change of throughput at the AP in the network when the value of θ is changed. Fig. 3a, 3b, and 3c show the different cases where the changing rapidity of ambient information is set to different values. Additionally, each figure shows the case where the number of terminal is set to 10, 30, and 50, respectively. From Fig. 3, it is clearly shown that there is an optimal value of θ which maximizes the throughput in each case where the changing rapidity of ambient information and the number of terminals are different. This is because the set value of θ has an effect on the interval of data sending in the network. If the value of θ is set to a high value, data from each terminal will occur often, which causes traffic congestion at the AP. On the other hand, a low value of θ avoids the traffic congestion but decreases the throughput. Since the high throughput can help to update the database of ambient information at each terminal with a short interval, it can increase the freshness of the database. Moreover, it is understood that the optimal value of θ should be set to a high value when the changing rapidity of ambient information is low and the number of terminals in the network is few.

C. The minimum guaranteed freshness of ambient information

Fig. 4 shows the result of the minimum guaranteed freshness of ambient information of each user in the database of the server in the two cases where the proposed method is used or not. Fig. 4a, 4b, and 4c show the different cases where the value of the changing rapidity of ambient information is set to different values. From Fig. 4, it is understood that the proposed method achieves higher freshness of the database in the server than when the proposal is not used. Additionally, the proposed method provides a significant improvement when the changing rapidity of ambient information and the number of the terminals are high. In such situations, existing access control scheme cannot avoid traffic congestion, which causes lower freshness of the database.

D. Standard deviation of the freshness of database

Furthermore, we show the results of standard deviation of the freshness of database in the two cases where the proposed method is used or not. The standard deviation of the freshness of database is expressed as follows:

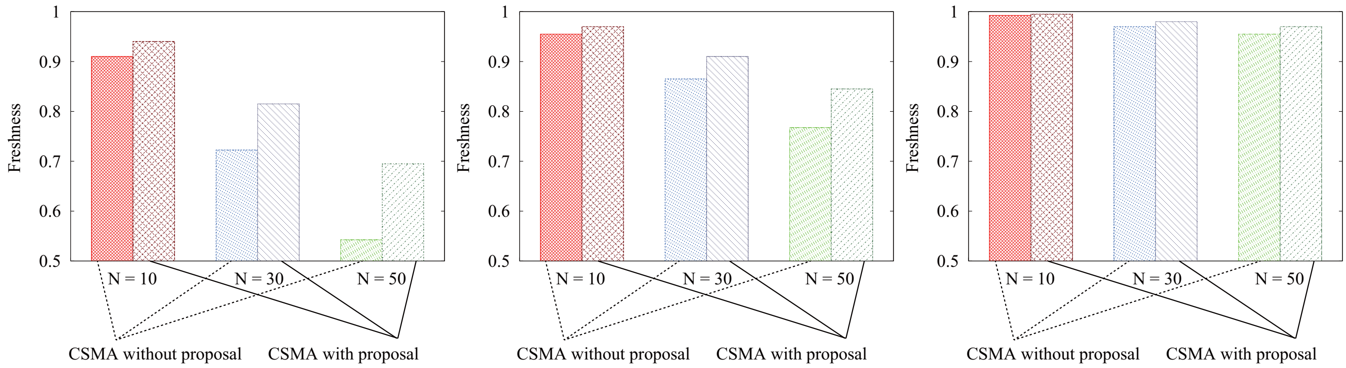
$$\sigma = \sqrt{\frac{1}{N} \cdot \sum_{i=1}^{N} (F_i - \overline{F})^2}, \tag{18}$$

where $\overline{F}$ denotes the average value of F_i.

From Fig. 5a and Fig. 5b, it is clearly shown that when the proposed method is used, the standard deviation of the freshness is significantly lower than when our proposal is not used. This is because in the proposal, each terminal sends its data while considering the freshness of the ambient information of itself. A low standard deviation of the freshness implies that the provided database of ambient information is stable.

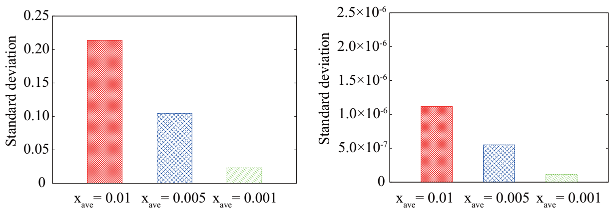
V. Conclusion

In this paper, we proposed a novel access control scheme to construct fresh database of ambient information of terminals. To keep the freshness of the database, it is needed to collect the ambient information from many terminals adequately while avoiding traffic congestion. Thus, in our proposal, the interval for sending data by each terminal is controlled with the changing rapidity of the ambient environment surrounding the terminal. By considering the changing rapidity of the



(a) x = 0.01. (b) x = 0.005. (c) x = 0.001.

Fig. 4. The minimum guaranteed freshness of ambient information of each user in the database at the server.



(a) Without the proposed method. (b) With the proposed method.

Fig. 5. Standard deviation.

ambient environment, it is possible to keep the difference between the realtime information and the information stored in the database at the server as small as possible while avoiding traffic congestion. Additionally, an optimization was introduced to improve the efficiency of the proposed access control scheme by setting a threshold to control the timing of sending data. Mathematical analysis and numerical results represented the existence of the optimal threshold and show the effectiveness of the proposed method on keeping the freshness of the database in the assumed network. Therefore, our proposed method can be considered to achieve the efficient data collecting for constructing the fresh database of the ambient information of terminals while avoiding traffic congestion. As the future works, we analyze the effect of the density of the terminal under an AP on the data collecting. Additionally, the difference of QoS requrirements and types of generated data will be considered.

Acknowledgement

This research was partially funded by the project, "Cognitive Security: A New Approach to Securing Future Large Scale and Distributed Mobile Applications," of Japan-US Network Opportunity: R&D for "Beyond Trillions of Objects" supported by National institute of Information and Communications Technology (NICT), Japan. Additionally, this research was supported in part by US NSF grant CNS-1405747.

References

[1] Y. Kawamoto, H. Nishiyama, N. Kato, N. Yoshimura, and S. Yamamoto, "Internet of Things (IoT): Present State and Future Prospects" *IEICE Transactions on Information and Systems,* Accepted. (Invited Paper)

[2] Y. Kawamoto, H. Nishiyama, Z. M. Fadlullah, and N. Kato, "Effective Data Collection via Satellite-Routed Sensor System (SRSS) to Realize Global-Scaled Internet of Things," *IEEE Sensors Journal,* vol. 13, no. 10, pp. 3645-3654, Oct. 2013.

[3] I. F. Akyildiz and J. M. Jornet, "The Internet of nano-things," *IEEE Wireless Communications,* vol. 17, no. 6, pp. 58-63, Dec. 2010.

[4] S. Balasubramaniam and J. Kangasharju, "Realizing the Internet of Nano Things: Challenges, Solutions, and Applications," *Computer,* vol. 46, no. 2, pp. 62-68, Feb. 2013.

[5] S. Tozlu, M. Senel, W. Mao, A. Keshavarzian, "Wi-Fi enabled sensors for internet of things: A practical approach," *IEEE Communications Magazine,* vol. 50, no. 6, pp. 134-143, Jun. 2012.

[6] L. Xu, L. Rongxing, L. Xiaohui, S. Xuemin, C. Jiming, and L. Xiaodong, "Smart community: an internet of things application," *IEEE Communications Magazine,* vol. 49, no. 11 pp. 68-75, Nov. 2011.

[7] P. Vlacheas, R. Giaffreda, V. Stavroulaki, D. Kelaidonis, V. Foteinos, G. Poulios, P. Demestichas, A. Somov, A. R. Biswas, K. Moessner, "Enabling smart cities through a cognitive management framework for the internet of things," *IEEE Communications Magazine,* vol. 51, no. 6, pp. 102-111, Jun. 2013.

[8] G. Kortuem, F. Kawsar, D. Fitton, V. Sundramoorthy, "Smart objects as building blocks for the Internet of things," *IEEE Internet Computing,* vol. 14, no. 1, pp. 44-51, Jan.-Feb. 2010.

[9] J. D. Nielsen, J. I. Pagter, M. B. Stausholm, "Location privacy via actively secure private proximity testing," *2012 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops),* pp. 381-386, 19-23 Mar. 2012.

[10] L. Xiao, Q. Yan, W. Lou, Y. T. Hou, "Proximity-based security using ambient radio signals," *2013 IEEE International Conference on Communications (ICC),* pp. 1609-1613, 9-13 Jun. 2013.

[11] L. Xiao, Q. Yan, W. Lou, G. Chen, Y. T. Hou, "Proximity-Based Security Techniques for Mobile Users in Wireless Networks," *IEEE Transactions on Information Forensics and Security,* vol. 8, no. 12, pp. 2089-2100, Dec. 2013.

[12] Y. Yang, T. S. P. Yum, "Delay distributions of slotted ALOHA and CSMA," *IEEE Transactions on Communications,* vol. 51, no. 11, pp. 1846-1857, Nov. 2003.

[13] L. Kleinrock, F. A. Tobagi, "Packet Switching in Radio Channels: Part I–Carrier Sense Multiple-Access Modes and Their Throughput-Delay Characteristics," *IEEE Transactions on Communications,* vol. 23, no. 12, pp. 1400-1416, Dec. 1975.

[14] F. Wang, D. Li, Y. Zhao, "Analysis and Compare of Slotted and Unslotted CSMA in IEEE 802.15.4," *5th International Conference on Wireless Communications, Networking and Mobile Computing, 2009. WiCom '09,* pp. 1-5, 24-26, Sep. 2009.

[15] Y. Cheng, H. Li, P. J. Wan, X. Wang, "Wireless Mesh Network Capacity Achievable Over the CSMA/CA MAC," *IEEE Transactions on Vehicular Technology,* vol. 61, no. 7, pp. 3151-3165, Sep. 2012.