An Internet of Things System Based on Device-to-Device Communication Technology and Radio-Frequency Identification

https://doi.org/10.3991/ijoe.v14i10.9302

Cheng Huang(✉), Yongbo Lv
Beijing Jiaotong University, Beijing, China
gaffer.c@foxmail.com

Abstract—This paper aims to build a mobile communication system suitable for different application scenarios of the Internet of Things (IoT). For this purpose, an IoT system was developed based on device-to-device (D2D) communication technology and radio-frequency identification (RFID). The D2D-RFID-based IoT system combines the merits of mobile communication (e.g. 4G) and the RFID. The analysis shows that the proposed system boasts good mobility, stable transmission, short time delay, fixed IP, and no need of a central server. The research findings have a great application potential in different IoT scenarios.

Keywords—device-to-device (D2D), radio-frequency identification (RFID), internet of Things (IoT)

1 Introduction

The Internet of Things (IoT) is a technology of the future. It can connect all things [1], create intelligent equipment, and generate a massive amount of valuable data. In the IoT era, network access will not be limited to personal computers or mobile phones, but extended to almost everything, ranging from refrigerator, air-conditioner to smart toilet.

However, the connection speed of the IoT is restricted by the wireless communication technology. At present, the IoT is mainly accessed via Wi-Fi or 4G. With a fixed range of communication, the Wi-Fi fails to support mobile communications; the 4G is designed to connect mobile phone users of the Internet, rather than accommodate the IoT applications. Neither of the two technologies can actually stimulate the development of the IoT.

To solve the problem, this paper proposes an IoT system based on device-to-device (D2D) communication technology and radio-frequency identification (RFID). The D2D-RFID-based IoT system combines the merits of mobile communication (e.g. 4G) and the RFID.

2 Technical Background

As an important component of the IoT, the RFID is a wireless communication technology that recognizes an object through radio signals instead of actual contact. The D2D is also a key element of the IoT. This communication technology mainly accelerates the interaction between things. It should be noted that the D2D operation relies on the 5G system.

The 5G is a landmark communication standard for the development of the IoT [2]. Before the birth of 5G, the IoT functions are severely limited in that the 4G does not support the connection to enough devices, and that the Wi-Fi does not have central control or mobile handover capability. The application of the IoT is fully considered in the design of 5G. This new generation standard 1000 times the number of connections of 4G and reduces the communication delay, without sacrificing the advantages of 4G (e.g. central control and mobility).

2.1 RFID

Currently, the RFID serves as a target recognition method like barcode and two-dimensional barcode [3~5]. The RFID suits the IoT well because it requires no direct contact with the target, works for a long time without replacing the power supply, and uses small and durable tags. Therefore, this technique has been applied in vehicle charging, document recognition and item tracking. On the downside, the strength of the RFID lies in the recognition of items, rather than the big data communication and processing or the security authentication [6, 7]. This is because most RFID devices, originally designed for item recognition, have no power supply or sufficient processing/storage capacity.

2.2 D2D

The D2D communication is an important feature of the 5G [8, 9]. Unlike traditional mobile communication, the D2D devices communicate directly with each other and the data need not to pass through the core network. In this way, the communication quality is improved at the cost of the communication range of short distance devices [10]. Note that short distance wireless communication is commonplace in the IoT.

Besides, the D2D differs greatly from short-range wireless communication like Wi-Fi and Bluetooth. The main differences are as follows: first, the D2D does not need separate access setting and matching; second, the D2D has a wireless resource controller that allocates and transmits wireless resources in a uniform manner, while the short-range techniques often suffer from severe signal interference; third, users of D2D devices can switch to traditional communication methods when the signal is poor, which is impossible if the users have already adopted the traditional means. Taking the Wi-Fi-4G integrated mode for example, when the Wi-Fi is cut off, the device will be switched to 4G and assigned a new IP address, leading to the reestablishment of all TCP and SSL connections.

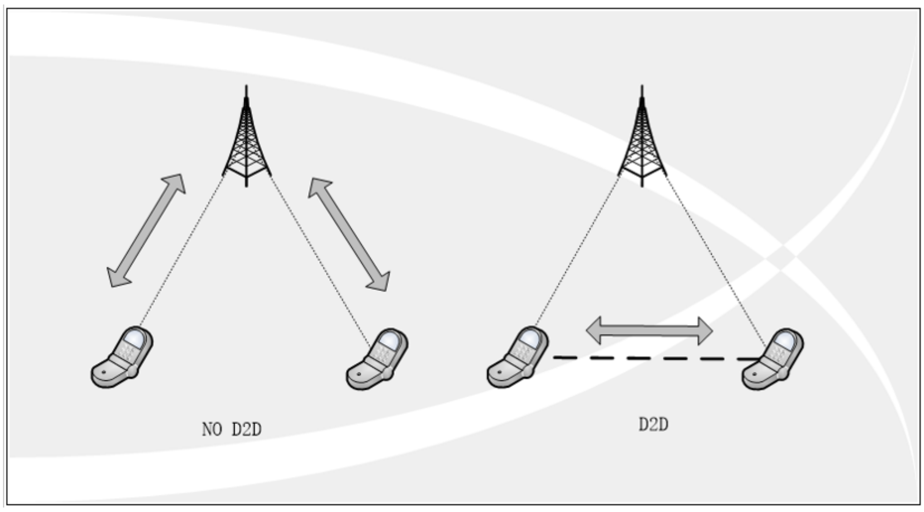

Fig. 1. Diagram of the D2D

According to the diagram in Figure 1, the D2D allows a device to directly send data to a nearby device, instead of the transfer by the mobile network. The direct transmission reduces the pressure on the central network and the network time delay.

Using wireless communication methods, the IoT applications can only be implemented individually in the effective distance of wireless communication, which varies from tens of metres to several hundred metres. The D2D, through direct communication, greatly enhances the communication ability and quality of IoT applications within the distance.

3 Design of RFID-D2D-Based IoT

The development of the D2D makes it possible to further improve the original IoT system. Here, the improvement is realized through integration of the technical features of the D2D and the RFID.

3.1 System design

As shown in Figure 2, the RFID-D2D-based IoT consists of four modules: an item perception module, a data transmission module, an authentication module and a service processing module. In the system, the item perception and recognition are realized using the RFID; then, the items are connected via the D2D to ensure high-quality communication; the security authentication is performed on a middleware; finally, the service of the upper layer application is processed by the service processing module.

The four-module design of the IoT system has the following advantages:

1. The RFID does well in identifying items that are close to each other. In a close distance, it is easy to set up seamless connections with the D2D.
2. The RFID is a completely independent technique that helps an application recognize items in any format. By contrast, the mobile communication is not suitable for application or capable of item identification, although it carries the information for the core network to identify the terminal.
3. With an electric tag or a reader, the RFID is an essential part of smart devices, in addition to the CPU for computing and the chip for communication. Each of these parts answers the intended purpose, forming a simple and reliable whole. Compared with hardware, the Authentication is particularly suitable for software, as RFID does not have to perform computing or processing for security authentication.

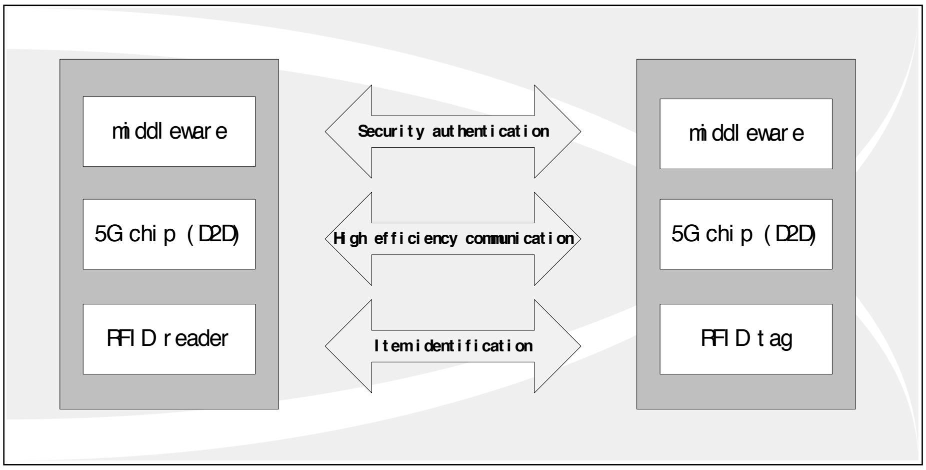

Fig. 2. System components

The above figure shows that the RFID is responsible for recognizing and perceiving the underlying items, the D2D for communicating the data efficiently, and the middleware for authentication through open SSL.

3.2 RFID module design

In the RFID-D2D-based IoT system, the RFID module does not have a strong processing ability. The only function of this module is short-distance recognition by electronic tags powered by a passive supply. The security authentication and data storage duties are transferred to the middleware of the upper layer software. In this way, the RFID module is simplified and blessed with a big storage space, and reliable performance.

3.3 D2D module design

The D2D module has a D2D chip for mobile communication. Without any modification, this chip can establish D2D connections whenever data communication is needed. However, the D2D module must be able to broadcast the received address to the nearby terminals, i.e. all the connectable devices. This is because RFID tags are often not bound to the layer 2 or layer 3 address of the other party, which should be connected to after acquiring the RFID tag information of the peer end. The broadcasting ability eliminates the need to record the correspondence between the RFID tags of the two parties and the layer 2 or layer 3 address through the central server, thereby reducing the number of central nodes and accelerating the establishment of connection. After receiving the broadcast, the peer end will check if its own RFID is requested, and, if yes, respond with its own IP address.

3.4 Authentication module design

The authentication module mainly relies on a middleware that performs CA certificate-based security authentication using the OpenSSL library. The middleware boasts excellent authentication performance, thanks to its low cost, high flexibility, and good CPU processing ability for chips with mobile communication functions. The RFID was not adopted for this module because its encryption algorithms are expensive and hardware-oriented. Below is a brief description of the principle of CA certification.

The CA certificate is a security technology that uses asymmetric encryption algorithms to perform identity authentication. In general, each certificate has a private key and a public key. The former should be kept private, while the latter can be disclosed to others. With the public key, a person can decrypt the encrypted information sent by the private key. As the only holder of the private key, the sender of the information has a reliable identity. Of course, the actual situation is much more complex than the above principle. Sometimes, some people may make their own certificates. To prevent this, the certificate must be issued by a reliable third-party.

3.5 System operation process

Table 1. System operation process

1	RFID recognizes the devices.
2	The owner of the RFID reader obtains the electronic tag from the owner of the RFID tag.
3	The owner of the RFID reader sends a D2D broadcast or multicast message, aiming to establish a connection.
4	After receiving the message, the owner of the RFID tag replies with its own IP address.
5	The two parties set up a TCP connection.
6	The two parties set up an SSL connection.
7	The two parties authenticate each other.
8	Both parties complete the remaining upper-layer services through D2D communication.

Note: The "upper-layer services" refers to the application services to be transmitted after the IoT, namely, the data collected by the current device.

Table 1 gives a clear map of the relationship between the various modules of the system and its process. As described earlier, the owner of the RFID reader first emits a radio frequency signal; after receiving the signal, and the passive RFID tag of the owner of the RFID tag replies with its own tag; after that, the owner of the RFID reader sends a D2D broadcast to obtain the layer 2 and layer 3 addresses of the other party; then, TCP and SSL connections are gradually established. In total, there are 7 interactions, and fewer if both systems support TCP fast start-up optimization. Next, the two parties perform the authentication through the CA certificate. Finally, the upper application services run on the IoT system.

Here, the D2D information is not broadcasted continuously so that the two parties can obtain each other's information without using the RFID module. The reason goes as follows: The D2D, not designed for item recognition, may consume a huge amount of 5G resources and battery power if the communication chip works continuously. By contrast, the RFID is designed for item recognition and the owner of the RFID tag consumes no power. That is why the D2D and the RFID are integrated in this research.

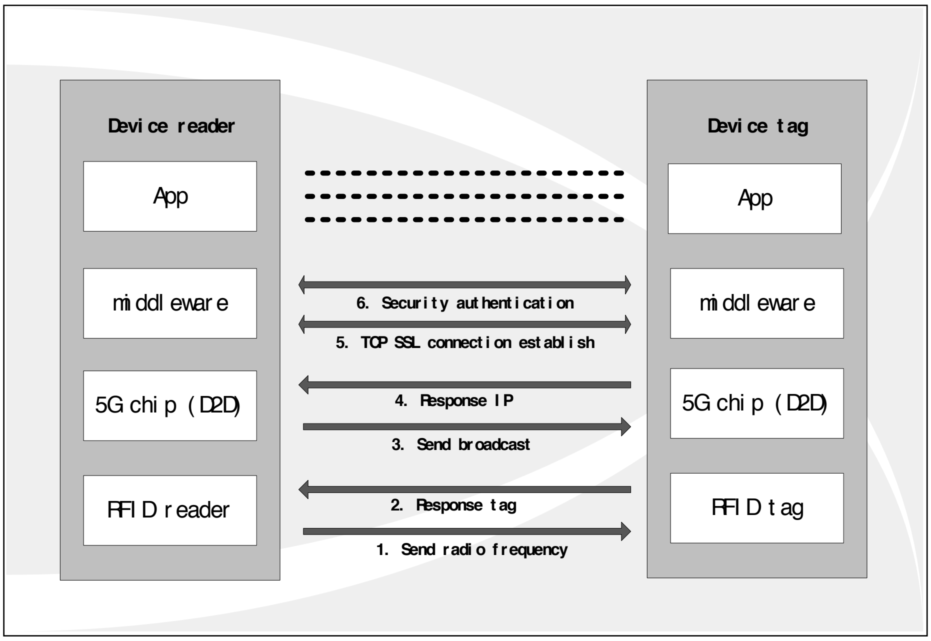

Fig. 3. Flow chart of the system

Note: Device reader is the owner of the RFID reader; Device tag is the owner of the RFID tag.

4 Analysis on the RFID-D2D-based IoT

The proposed RFID-D2D-based IoT has the following advantages over the mainstream IoT systems.

1. Good mobility: Many IoT systems are based on Wi-Fi connections. They have no mobility and only works in a very small range. The connections are lost once the object is out of the range. Compared to these systems, the proposed IoT can automatically switch from the D2D mode to the normal transmission mode and complete the handover between different base stations.
2. Stable transmission: The D2D, as a technical standard of 5G, is managed by a wireless resource management unit. Since all wireless resources are allocated by the base station, the proposed IoT does not have the unstable communication state as Wi-Fi. When there are a few users, Wi-Fi outperforms the proposed IoT because it has no central node to control wireless resource allocation. However, when there are many users, the terminals of Wi-Fi will compete for wireless resources, leading to unstable transmission and up to ten milliseconds-long delay. [11]
3. Unique IP: Considering both short- and long-distance transmission modes, the proposed IoT can assign a fixed IP to each device, which is not possible for the combination of Wi-Fi and mobile communication. The unique IP prevents reconnection of the TCP and improves the communication stability. This feature is very important. Without this feature, the low-starting TCP may be too slow to reach a stable sending speed.
4. Short delay: Because the D2D communication mode does not need to pass through the core network, the proposed IoT enjoys a shorter communication delay than traditional mobile communication network. The short delay reduces the core throughput, which in turn enhances the network performance.
5. Simplicity: The adoption of D2D broadcasting eliminates the need for a third-party server to open a barrier in which neither side knows the other's IP address.

Table 2. Comparison between IoT connection technologies

Communication mode	Mobility	Stability	Unique IP	Time delay	Access to the IP to Peer
Wi-Fi	No	Poor	No	Unstable	Convenient
Traditional mobile communication	Yes	Excellent	Yes	General	Inconvenient
Combination of Wi-Fi and mobile communication	Yes	General	No	Unstable	Inconvenient
RFID-D2D-based IoT	Yes	Excellent	Yes	Excellent	Convenient

From the above table, it can be clearly seen that the comprehensive performance of the Internet of Things connection technology based on RFID-D2D is excellent. But it also needs updated mobile communication technology for support, without the application of 5G technology, it cannot be realized.

5 Conclusions

This paper designs a promising RFID-D2D-based IoT system which adopts both RFID and D2D technologies, integrates middleware functions, and realizes excellent performance. The proposed system combines the merits of mobility and short-distance communication and avoids their disadvantages. It is suitable for scenarios where the device has a certain processing capability, but not for connecting items that have no communication chip and processing capability. With the development of IoT applications and mobile communication techniques, it is believed that more research areas will be opened up in the fields of the IoT and IoT and mobile communication in the future.

6 References

[1] Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M. (2013). Internet of things (iot): a vi-sion, architectural elements, and future directions. Future Generation Computer Sys-tems, 29(7), 1645-1660. https://doi.org/10.1016/j.future.2013.01.010

[2] Osseiran, A., Boccardi, F., Braun, V., Kusume, K. (2014). Scenarios for 5g mobile and wireless communications: the vision of the metis project. Communications Magazine IEEE, 52(5), 26-35. https://doi.org/10.1109/MCOM.2014.6815890

[3] Ferrer, G., Dew, N., Apte, U. (2010). When is rfid right for your service? International Journal of Production Economics, 124(2), 414-425. https://doi.org/10.1016/j.ijpe.2009.12.004

[4] Want, R. (2006). An introduction to rfid technology. IEEE Pervasive Computing, 5(1), 25-33. https://doi.org/10.1109/MPRV.2006.2

[5] Orndorff, C., Dai, W. (2016). Numerical hyperthermia simulation for a 3-d triple-layered skin structure with embedded vascular countercurrent network and nanoparti-cles. International Journal of Heat & Technology, 34(Special Issue 1), S179-S184. https://doi.org/10.18280/ijht.34S124

[6] Feldhofer, M., Dominikus, S., Wolkerstorfer, J. (2004). Strong authentication for rfid systems using the aes algorithm. Ches, 3156, 357-370. https://doi.org/10.1007/978-3-540-28632-5_26

[7] Finkenzeller, K. (2003). Rfid handbook: fundamentals and applications in contactless smart cards and identification / k. finkenzeller. Wiley & Sons(5). https://doi.org/10.1002/0470868023.ch9

[8] Hakola, S., Chen, T., Lehtomaki, J., Koskela, T. (2010). Device-To-Device (D2D) Communication in Cellular Network - Performance Analysis of Optimum and Practi-cal Communication Mode Selection. 29.16:1-6. https://doi.org/10.1109/WCNC.2010.5506133

[9] Sakr, A.H., Hossain, E. (2014). Cognitive and energy harvesting-based d2d communi-cation in cellular networks: stochastic geometry modeling and analysis. IEEE Trans-actions on Communications, 63(5), 1867-1880. https://doi.org/10.1109/TCOMM.2015.2411266

[10] Liu, Z., Peng, T., Xiang, S., Wang, W. (2012). Mode selection for Device-to-Device (D2D) communication under LTE-Advanced networks. IEEE International Confer-ence on Communications (pp.5563-5567). IEEE. https://doi.org/10.1109/ICC.2012.6364738

[11] Banerjee, S., Ghosh, A., Mitra, S.K. (2017). A modified mathematical model for life-time enhancement in wireless sensor network, Mathematical Modelling of Engineer-ing Problems, 4(2): 84-90. https://doi.org/10.18280/mmep.040204

7 Authors

Huang Cheng is a doctoral student, computer engineering. He studies in School of Traffic and Transportation Beijing Jiaotong University, No.3 Shangyuancun Haidian District Beijing 100044 P. R. China.

Lv Yongbo is a system scientist, engineering educator, and Professor of Beijing Jiaotong University. She studies in School of Traffic and Transportation Beijing Jiaotong University, No.3 Shangyuancun Haidian District Beijing 100044 P. R. China.

Article submitted 30 July 2018. Resubmitted 23 August 2018. Final acceptance 09 October 2018. Final version published as submitted by the authors.