Proposal of cooperative operation framework for M2M systems

Fumihito Sugihara*, Katsuhiro Naito†, Hidekazu Suzuki‡, Akira Watanabe‡, Kazuo Mori*, Hideo Kobayashi*
*Department of Electrical and Electronic Engineering, Mie University, Tsu, Mie 514-8507, Japan
†Faculty of Information Science, Aichi Institute of Technology, Toyota, Aichi 470-0392, Japan
‡Graduate School of Science and Technology, Meijo University, Nagoya, Aichi 468-8502, Japan

***Abstract*—This paper presents a new framework for a privacy oriented M2M cooperative system. The proposed framework can realize privacy preservations, short delay cooperation, large scalability by employing an end-to-end communication mechanism. Additionally, it also supports distributed cooperative operations among M2M devices in different vendors. Therefore, users can employ various kinds of M2M devices produced by different vendors and can create own procedures for cooperative operations among M2M devices flexibly. The proposed framework employs Network Traversal with Mobility (NTMobile) that is the IP mobility and accessibility network protocol to realize end-to-end communication between M2M devices. NTMobile provides a seamless overlay network where each M2M device can be recognized by a unique Fully Qualified Domain Name(FQDN). Additionally, it also supports distributed operation between separate domain founded on the DNS mechanism. The prototype implementation demonstrates that the proposed platform can provide cooperative services between M2M device with end-to-end communication based on NTMobile.**

***Index Terms*—M2M, IoT, cooperative operations, framework, end-to-end communication**

I. Introduction

Machine-to-Machine (M2M) systems have been attracting attention as one of the solutions for various issues in environmental problems, energy usages and aging societies in the 21th century [1], [2]. Recently some specific protocols for M2M have been proposed [3], [4], [5]. Conventional M2M systems employ a client-server mechanism even if they assume M2M communication [6], [7], [8]. Therefore, all cooperation services among M2M devices are performed through severs because each M2M device may be difficult to communicate with each other directly due to NAT traversal problems or difference of IP protocol versions. As a result, cooperative operation through the server systems causes large latency due to propagation delay and processing delay. In other words, a client-server mechanism for M2M systems has a poor scalability because the number of M2M devices will be huge in the near future. Additionally, M2M devices generally sense extremely private information such as an entrance door status, an existence in a room, health information etc. These private information should be transferred directly to curb the flow of information from systems even if some devices should cooperate for some purposes.

This paper presents a new framework for a privacy oriented M2M cooperative system. The proposed framework can realize privacy preservations, short delay cooperation, and large scalability by employing an end-to-end communication mechanism. Additionally, it also supports distributed cooperative operations among M2M devices. Therefore, users can employ various kinds of M2M devices produced by different vendors and can create own procedures for cooperative operations flexibly. IP mobility protocols are useful technologies to realize end-to-end communication. On the contrary, a few implementations have been developed to support a NAT traversal and interconnectivity between IPv4 and IPv6 networks [9], [10]. The proposed framework employs Network Traversal with Mobility (NTMobile) that is the authors's original IP mobility and accessibility network protocol to realize end-to-end communication between M2M devices [11], [12]. NTMobile provides a seamless overlay network where each M2M device can be recognized by a unique Fully Qualified Domain Name(FQDN). Additionally, it also supports distributed operation between separate domain based on the DNS mechanism. The prototype implementation shows that the proposed platform can realize privacy oriented cooperative services between M2M devices based on NTMobile.

II. Overview of NTMobile

Fig. 1 shows the overview of NTMobile network. NTMobile is a new IP mobility and accessibility network protocol for IPv4 and IPv6 networks. The system of NTMobile consists of Account server (AS), Direction Coordinators (DCs), Relay servers (RSs) and NTMobile end-nodes. The NTMobile network assigns a virtual IP address pool to each DC, and each DC assigns a virtual IP address in the pool to its NTMobile end-node. Therefore, each NTMobile end-node can be uniquely identified by the virtual IP address in the NTMobile network. Applications use it as a communication IP address because it is also allocated to a virtual interface. Therefore, applications can continue communication by using the virtual IP address even when a real IP address is changed. IP datagrams including the virtual IP address from applications are encapsulated by NTMobile functions, and are exchanged through the UDP tunnel. There are two types of communication paths. One is a direct tunnel path between NTMobile end-nodes, which is typically used in principle. Another is a relay tunnel path via RS when NTMobile end-nodes cannot communicate directly due to NAT traversal problems and difference of IP protocol versions. Fig. 2 shows the tunnel construction process in the NTMobile. Additionally, NTMobile end-nodes

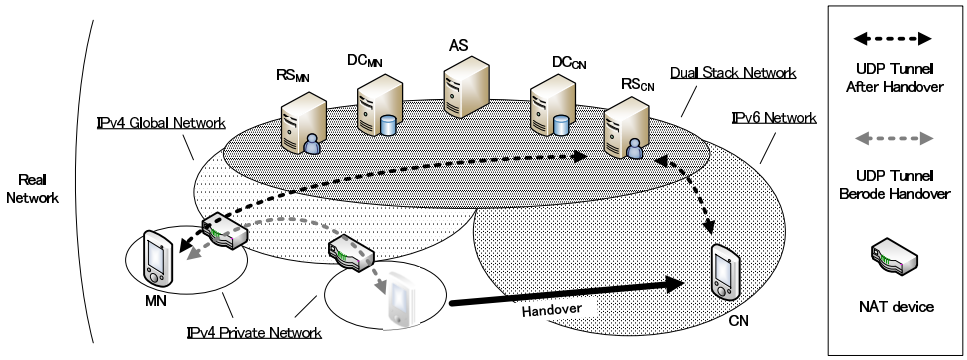

Fig. 1. Overview of NTMobile

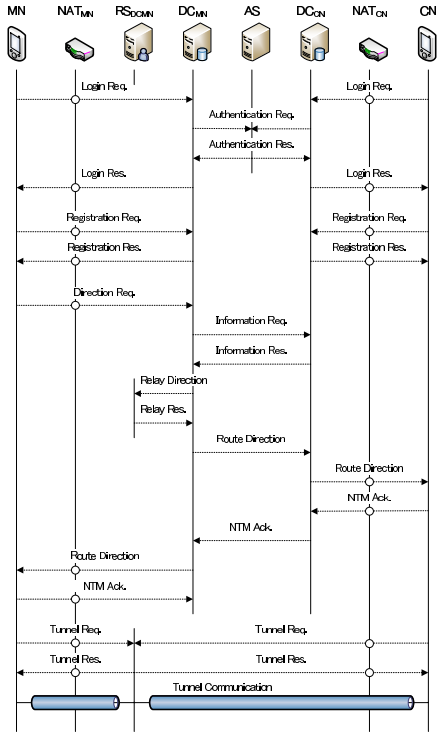

Fig. 2. Tunnel construction in the NTMobile

use the optimum communication path by a route optimization mechanism in NTMobile. Therefore, communication delay can be reduced in typical private networks with NAT routers.

A. Direction Coordinator

Direction Coordinators manage the information of each NTMboile end-nodes and direct a tunnel construction process to them. The NTMobile network assigns a virtual IP address pool to each DC, and each DC assigns a virtual IP address in the pool to its NTMobile end-node. Therefore, each NTMobile end-nodes can be uniquely identified by the virtual IP address in the NTMobile network. Additionally, DC has recorded NTMobile end-node's Fully Qualified Domain Name (FQDN), a real IP address, a virtual IP address and a real IP address and a port number of an out side interface of a NAT in its own database. DC has a function of Domain Name System (DNS) to manage its domain, and to find each DC by using the DNS mechanism. Hence, DC can be decentrally-organized in the NTMobile network due to the use of the mechanism in the DNS. DC is assumed to be installed in a dual-stack network because DC should be responsible for the connectivity from IPv4 and IPv6 networks for NTMobile end-nodes.

B. Relay Server

Relay servers are used for a relay operation of a tunnel between NTMobile end-nodes when communication cannot be performed directly between them due to a NAT traversal and a lack of compatibility between IPv4 and IPv6 networks. Some RSs can be managed by their DC. Therefore, DC can assign an appropriate RS based on a CPU load and network traffics, and directs a tunnel construction process. RSs are also installed in a dual stack network because RS may also perform relay between IPv4 and IPv6.

C. NTMobile end-node

A NTMobile end-node has a virtual interface for applications. A virtual IP is assigned from DC to the virtual interface. Therefore, applications communicate by using the virtual IP address continuously. Additionally, the IP datagrams with virtual IP addresses are concealing the change of a real IP address by UDP capsulation. The NTMobile end-node should register a new real IP address to its DC for IP mobility and accessibility functions when the real IP address changes.

III. Proposed System

A. System model

Fig. 3 shows the overview of the proposed system. The proposed system defines a cooperative operation procedure as a recipe. Users can describe any recipes including procedures in a local device and procedures among some devices. The proposed system comprises of recipe servers, M2M device management servers and M2M devices in addition to the server group of existing NTMobile servers. The M2M device management servers authenticate own M2M devices and configure

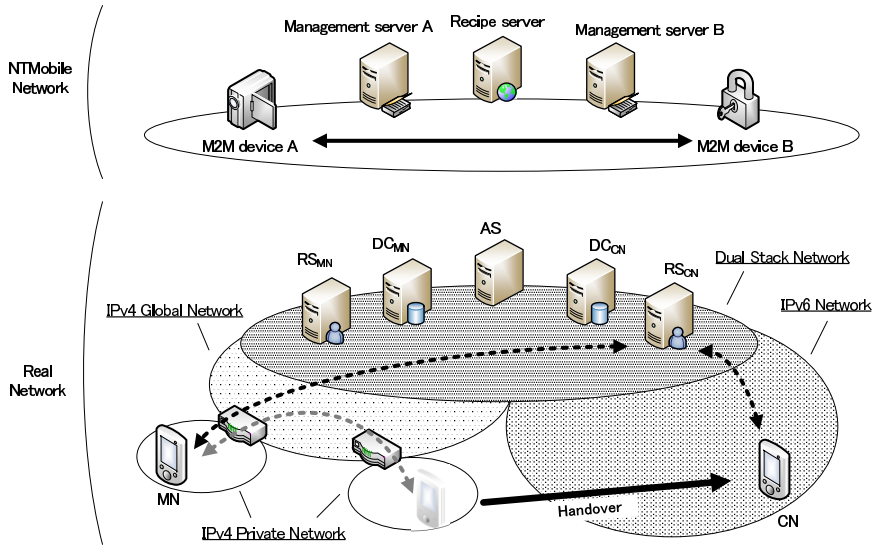

Fig. 3. Overview of proposed system

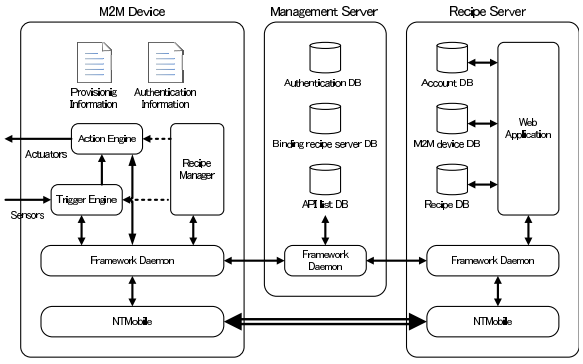

Fig. 4. Implementation design

them. The recipe servers obtain information about the M2M devices and provide functions for recipes to the users. The users can manage their own recipes on the recipe servers. The recipe servers also configure the M2M devices according to the recipes. Fig. 4 shows the implementation design of the proposed system. We believe that we can implement a proposed system by designing it in this way.

- Recipe server
  The function of Recipe server is to manage recipes, M2M devices and user accounts. Recipe server has the function of NTMobile, and it is assumed to be installed in a dual-stack networks because M2M devices may use IPv4 and IPv6 protocols. In addition, the recipe server obtains information about M2M devices from their M2M management servers to support various vendors' devices. Then, it also binds the registered M2M devices to own system.
- M2M device management server
  M2M device vendors manage their own M2M device management servers. The M2M device management server manages the functional information of each M2M device. It also authenticate its M2M device by an authentication scheme such as a digital certificate.
- M2M device
  A M2M device implements the function of NTMobile and applications on the proposed framework. Applications that use the proposed framework realize the cooperative operations by the acquired information from external sensors, the control of external devices and communication with the recipe server and other M2M devices.

A cooperative operation between M2M devices in the proposed framework performs by end-to-end communication. NTMobile provides the end-to-end communication function to the proposed framework. A recipe is performed between M2M devices according to the following trigger and action by using NTMobile end-to-end communication.

- Trigger
  Users define some conditions to trigger a cooperative operation according to information of external sensors connected to M2M devices and services according to a recipe. A users' recipe manages these conditions as a trigger.
- Action
  Users define some operational actions associated with the trigger. The actions include operations of peripheral equipments or notification to another services.

B. Provisioning Process

The following procedure in Fig. 5 shows the provisioning process of the M2M device to bind to user's recipe servers.

1) M2M device venders provide unique information to their M2M devices as an identifier.
2) A user obtains the identifier of the M2M device and registers it to the user's recipe server to bind to the M2M device. The recipe server accesses the M2M device

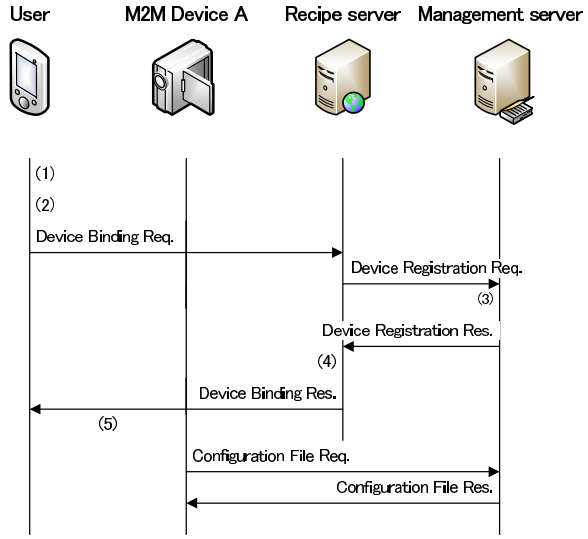

Fig. 5. Provisioning process

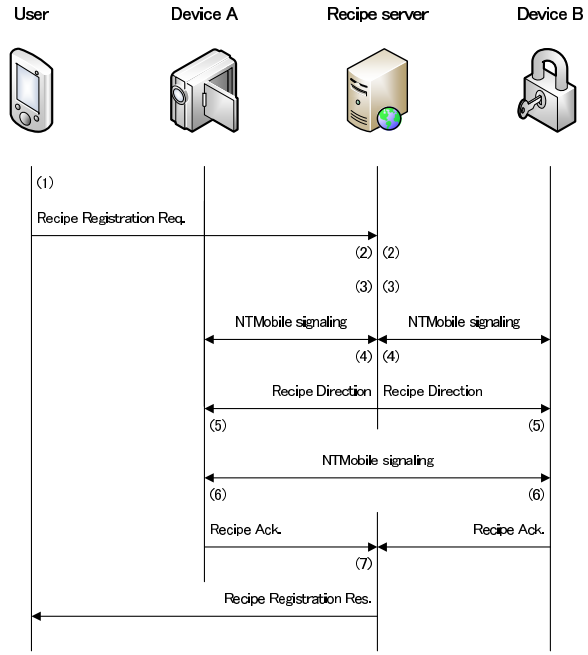

Fig. 6. Registration process of recipes

management server of the M2M device based on the identification information.

3) The M2M device management server completes the registration process for the M2M device and replies the API lists of the M2M device to the recipe server.
4) The recipe server notifies the completion of the M2M device registration to the user.
5) The user switches on the M2M device after the M2M device registration. The M2M device accesses to its own M2M device management server and obtains the provisioning information.

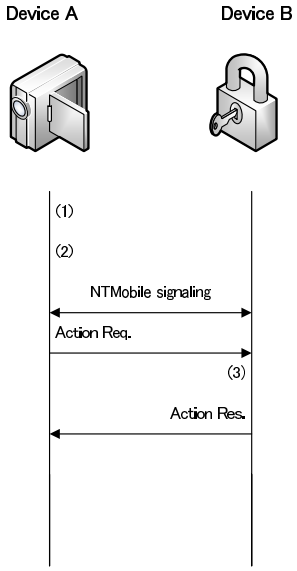

Fig. 7. Cooperative operation process of recipes

C. Recipes registration process

Fig. 6 shows the recipe registration process for the cooperative operation between the M2M device A and B in the proposed framework. Additionally, we explain each procedure in the following.

1) The user can define a recipe that binds APIs of the M2M devices A and B on the application.
2) In this example, we assume that M2M device A causes an action on M2M device B. Therefore, the cooperation operation between M2M devices A and B is required. Thus, the recipe server transfers the defined recipe to each device.
3) The recipe server starts the tunnel construction process using a function of NTMobile for M2M devices A and B because it may not access to each device due to NAT traversal.
4) The recipe server sends the recipe to M2M devices A and B after the confirmation of the tunnel construction.
5) The M2M devices A and B receive the recipe and confirm the operation between the devices to verify the recipe. In this case, M2M devices also start the tunnel construction by using the function of NTMobile before the operation verification.
6) Both devices report the verification result to the recipe server.
7) The recipe server notifies that the recipe has been successfully registered in the application on the M2M devices.

D. Cooperative operation of recipes

Fig. 7 shows the process for realizing cooperative operation based on the recipe by using the proposed framework. Additionally, we explain each procedure in the following.

1) M2M device A, which is a trigger device, builds a tunnel to M2M device B to notify the trigger.

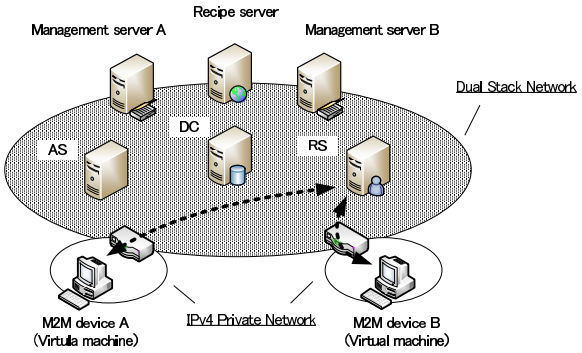

Fig. 8. Experimentation environment

TABLE I
SPECIFICATION OF DC, RS AND M2M DEVICES

	DC, RS	M2M devices
OS	Linux	Linux
Distribution	CentOS 6.6	Ubuntu 12.04
Kernel version	2.6	3.2
CPU	AMD Opteron 4180	Intel Core i7
Clock	2.6 GHz	1.8 GHz
Memory	512 MB	1 GB

2) The proposed framework on the M2M devices A and B exchange information after the tunnel building between M2M devices was completed. Thus, M2M device B identifies the actions based on the trigger.
3) M2M device B realizes the device cooperation by doing the predefined action based on the recipe. Then, M2M device B notifies that the action has been completed on the M2M device A.

IV. EVALUATION EXPERIMENT

A. Experimentation environment

We have measured the signaling time of the proposed cooperative operation mechanism with two virtual machines as the M2M devices. The virtual machines implement the NTMobile and the application of the cooperative operation mechanism. Fig. 8 and Tab. I show the evaluation environment and specification of each equipment respectively. Additionally, in order to clarify the characteristic of the measurement environment, Round-Trip time (RTT) between each equipment was measured. Tab. II shows the measured RTT.

B. Experiment result and Considerration

Tab. III shows the cooperative operation time. From the results, we could find that the communication delay was more dominant than the processing delay. Although the experimental network has short delay, practical wired networks typically are under a substantial delay. Therefore, the processing time of the proposed mechanisms is not a big overhead comparing to the communication delay in networks.

V. CONCLUSION

This paper has proposed the new framework for a privacy oriented M2M cooperative system. The propose framework realizes a cooperative operation between M2M devices with end-to-end communication by NTMobile that is a secure IP mobility and accessibility network protocol for IPv4 and IPv6 networks. Additionally, it also supports various kinds of M2M devices manufactured by different vendors and flexible cooperative operations between different vendors' M2M devices.

TABLE II
RTT OF END-TO-END

	RTT [ms]		
pair	min	avg	max
M2M device A - DC	10.05	10.97	13.274
M2M device A - RS	9.67	10.70	12.20
M2M device B - DC	9.08	9.87	11.34
M2M device B - RS	9.48	10.08	11.35
DC - RS	0.23	0.28	0.34

TABLE III
EXPERIMENTAL RESULT

	Signaling time [ms]		
process	min	avg	max
Name resolution and Tunnel construction	69.42	79.79	95.91
Cooperative operation	19.71	20.71	22.00

ACKNOWLEDGMENT

This work is supported in part by Grant-in-Aid for Scientific Research (B)(15H02697) and Grant-in-Aid for Scientific Research (C)(26330103), Japan Society for the Promotion of Science (JSPS) and the Integration research for agriculture and interdisciplinary fields, Ministry of Agriculture, Forestry and Fisheries, Japan.

REFERENCES

[1] G. Wu, S. Talwqr, K. Johnsson, N. Himayat and K. D. Johnson, "M2M: From Mobile to Embedded Internet," IEEE Communications Magazine, Vol.49, No.4, pp.36-43, Apr. 2011.
[2] oneM2M, "oneM2M Use Cases Collection," oneM2M TR 0001 0.0.5, Nov. 2013.
[3] Z. Shelby, K. Hartke, C. Bormann and B. Frank, "Constrained application protocol (CoAP)," draft-ietf-core-coap-12, Oct. 2012.
[4] I. Fette and A. Melnikov, "The websocket protocol," draft-ietf-hybithewebsocketprotocol-17, Sept. 2011.
[5] G. Montenegro, N. Kushalnagar, J. Hui and D. Culler, "Transmission of IPv6 packets over IEEE 802.15.4 networks," IETF RFC-4944, Sept. 2007.
[6] ETSI, "Machine to Machine communications (M2M); M2M service requirements," ETSI TR 102 689 V1.1.2, May 2011.
[7] ETSI, "Machine to Machine communications (M2M); Functional architecture," ETSI TR 102 690, Dec. 2011.
[8] ETSI, "Machine to Machine communications (M2M); Use Case of M2M applications for Connected Consumer," ETSI TR 102 857 V1.1.1, Aug. 2013.
[9] H. Solima, "Mobile IPv6 Support for Dual Stack Hosts and Routers," RFC 5555, IFTF, 2009.
[10] M. bonola and S. Salsano, "S-UPMT: a secure Vertical Handover solution based on IP in UDP tunneling and IPsec," GTTI Riunione Annuale 2010, (online), http://www.gtti.it/GTTI10/papers/gtti10_submission_29.pdf, 2010.
[11] H. Suzuki, K. Kamienoo, T. Mizutani, T. Nishio, K. Naito and A. Watanabe, "Design and Implementation of Establishment Method of Connectivity on NTMobile," IPSJ Journal, Vol. 54, No. 1, pp. 367–379, Jan. 2013.
[12] K. Naito, K. Kamienoo, T. Nishio, T. Mizutani, H. Suzuki, A. Watanabe, K. Mori and H. Kobayashi, "Realization and Implementation of IP Mobility in NTMobile," IPSJ Journal, Vol. 54, No. 1, pp. 380–393, Jan. 2013.