3-12 Autonomous Access Control among Nodes in Sensor Networks with Security Policies

IWAO Tadashige and AMAMIYA Makoto

This paper describes a new framework of policy control sensor networks. Sensor networks are shared by various applications, and have many nodes. Hence, sensor networks need to have ability to accept various applications, and to deploy application modules to nodes easily. Sensor nodes should have appropriate application modules. A framework that is based on VPC on KODAMA enables sensor nodes to have appropriate modules by assignment rules in a policy. When users only put application policies to sensor networks, sensor nodes propagate the policies and perform appropriate roles in the applications. This paper also shows that sensor networks with policies change behavior corresponding to detected active RFID tags as an example.

Keywords
Sensor Network, Ad-hoc network, Policy, Access control, RFID, Multi-agents systems

1 Introduction

Sensor networks[1][2] are expected to form an important component in future ubiquitous environments. Simply put, sensor networks connect the physical world and the logical world: they sense physical phenomena, convert the phenomena to logical objects, and feed back physical phenomena as a result of interactions among the objects in the logical world. Sensor networks detect a variety of quantities, including temperature, acceleration, GPS locations, and infrared light. Sensor networks handle not only physical phenomena but also artifacts such as RFID data. RFID tags are among the objects observed by sensor networks, and are used to manage people and commerce.

Many applications are expected to begin using sensor networks in the near term, for individual access to a variety of services. Users will be able to share a single sensor network holding numerous applications. Sensor networks will thus need to be adaptable to a variety of purposes. Applications will have to be installed dynamically and easily, with the appropriate modules added at the appropriate nodes. However, as sensor networks involve an extremely large number of nodes, it will be difficult to install modules manually within each node, thus a method will be required to enable installation of the right modules in the corresponding nodes automatically. Security is also an important issue; personal data handled in sensor networks must be protected. It is not enough for sensor networks to apply a single security method, uniform technique to the handling of data. For example, some applications may need to pass data through nodes that require different types of authentication according to detected data type. In such cases, a secure method for the handling of application-specific data is needed. Thus, sensor networks will require a framework for the appro-

priate deployment of application modules in the nodes, data must also be handled securely, and a variety of applications must be dynamically implemented.

We have now proposed such a framework for sensor networks. The framework is based on VPC on KODAMA [3]-[6], which enables policy-based control of multi-agent systems. The agents construct so-called "communities" based on the policies. The policies define the conditions for entry of agents into a community and the roles of the agents within the community, and also include rules for the allocation of these roles. Allocation is made according to the attributes of the agents and the defined allocation rules. The agents behave according to the allocated roles and provide services in collaboration with other agents. The agents of VPC on KODAMA function to authenticate other agents and to allocate roles securely. In sensor networks, the agents are the sensor nodes, and the roles entail the detection of data and processing of the detected data. Applying VPC on KODAMA to sensor networks enables the sensor network to adopt application policies, to allocate appropriate modules to the respective nodes, and thus to process data securely.

Section **2** discusses policy-based multi-purpose sensor network control. Section **3** describes VPC on KODAMA within a sensor network. Section **4** presents an example of this framework in use. For example, a sensor network will alter its behavior according to the detected RFID and to the underlying policies. Section **5** discusses related studies.

2 Policies in multi-purpose sensor networks

2.1 Requirements for multi-purpose sensor networks

Characteristics of sensor networks include detection of physical phenomena by multiple sensor nodes, processing of detected data, and internodal exchange of data. In multi-purpose sensor networks, various applications use the sensor nodes.

Each node must have a framework that will support a variety of applications. To execute services within a multi-purpose sensor network, each node should be able to adopt a range of applications. However, it is impractical to install all application modules in the sensor nodes in advance. Thus, the nodes should be able to adopt applications dynamically. On the other hand, the number of nodes in a given sensor network is expected to be enormous, and it will be difficult to install applications in each node manually.

In the use of personal data handled by the sensor network, security will also be essential. Personal data must be protected within these networks. Depending on the type of data detected, methods of protection will vary. Accordingly, multi-purpose networks need to feature a framework that enables deployment of different security mechanisms for different applications. In short, the essential factors in multi-purpose sensor networks will include diversity in applications, application deployment, and security.

• Diversity of applications

Applications in sensor networks provide services involving many coordinated sensor nodes. Each sensor node has its own role. A given application will rely on cooperation among the nodes as these nodes perform their various assigned roles. Some nodes may have different roles from other nodes in the sensor networks and some roles may involve tasks that can only be executed on authenticated nodes. Consequently, appropriate roles will have to be assigned to appropriate nodes.

• Deployment of applications

When deploying applications in a sensor network, two problems must be taken into consideration. The first involves the number of sensor nodes, an important factor when installing applications in the sensor network. The second problem lies in the difference between the installation module and the remaining modules. To solve both of these problems, a mechanism is required to enable automatic placement of the appropriate modules at the correct nodes among the many

nodes within the sensor network.

• Security

Sensor networks face two critical security issues: protection of the detected data and protection of the sensor network. The protection of the detected data is assessed in terms of how securely the sensor network handles the detected data. The protection of the sensor network concerns the means by which the sensor network protects itself against unauthorized data intrusion and access. A sensor network detects, processes, and transfers data, therefore security needs to be taken into consideration separately for each of these operations in light of both of these issues.

In the first step, the nodes detect data. If a sensor node can be designed to determine whether the detected data is genuine, the sensor node should indeed feature such a mechanism. However, it is generally difficult to determine the authenticity of physical phenomena such as humidity and temperature. In these and similar cases, data from two or more sensors are compared. If the data is artificial, such as bar codes and RFIDs, verifying mechanisms can be implemented, such as digital signatures. As the mechanism depends on the application, the ability to acquire modules dynamically is also important in this step.

In the next step, the nodes process the detected data. As discussed above, the process modules are best introduced externally. This requires authentication of the process modules. The process modules should able to execute a "smart" response if the processed data is unauthorized. For example, if an unauthorized RFID tag is detected, it should be destroyed. Whether or not the RFID tag is authorized will depend on the system, and the responses to unauthorized events will differ among the process modules of the various applications.

In the last step, the nodes transmit the processed data to other nodes. In this step, a node should determine whether the node to which it is sending data or from which it is receiving data is trustworthy. Applications do not use all nodes in the sensor network. Only the nodes involved in the given application should be able to exchange data. Thus we can assume that logical networks will vary between applications. Assuming that a logical network exists for each application, the nodes used by an application will be able to send and receive data if the nodes are linked within the application's logical network. Here it is important to consider how the nodes involved in an application will construct a logical network for application security. There are no central nodes in sensor networks. Thus, the nodes involved in an application will have to establish a specific logical network autonomously.

2.2 Policy control in multi-purpose sensor networks

To control an extremely large number of nodes, policy-based control is also effective, functioning similarly to laws in society. When a large number of nodes are involved, direct manual control of each node is difficult to perform. The nodes should be able to regulate themselves autonomously according to specified rules, just as individuals in society comply with laws. We refer to the descriptions that the nodes must follow as policies.

In terms of policies in multi-purpose sensor networks, the discussion thus far has highlighted the following issues.

(1) Allocation of the appropriate role to the appropriate node

(2) The roles in a sensor network are classified into schema for the sensors and schema for the ad-hoc network. The sensor schema involves how the sensor nodes detect and process data. The ad-hoc network schema addresses how the nodes construct a logical network for each application and how they transfer or receive data.

(3) How each node determines whether a given policy is genuine

A framework for multi-purpose sensor networks should feature mechanisms to support the above three items in policy control.

3 Policy-based routing and access control in ad-hoc networks

3.1 VPC on KODAMA

VPC on KODAMA[3]-[6] provides a mechanism to control a multi-agent system through policies. The agents detect genuine policies and determine their own roles according to their attributes and allocation rules.

The structure of VPC on KODAMA includes a hierarchical structure of communities. The agents belong to communities and also have their own community. An agent features attributes and two policies: a public policy that defines the conditions for the agent to enter a community and its role in the community, and a private policy that defines the conditions for the agent to access its own private data (its attributes, for example).

When an agent satisfies the conditions specified by the community policy, the agent can join the community and play a role in the community according to that policy. Figure 1 shows the structure of the public policy. For an agent to have a given role it must feature the corresponding attribute. The public policy includes a digital signature for the agent, and the other agents verify the signature to confirm that the policy is genuine.

Tamper-resistant devices are used to determine roles. These devices resist unauthorized acquisition of information, block tampering, and store agent attributes. Thus without authorization even users are unable to modify an agent's various attributes, such as PKI certification. A module that determines roles (according to attributes and specified policy conditions) is stored in a tamper-resistant device. The agent checks the signature of the policy, sends conditions to the decision module located in a tamper-resistant device, and then acquires its assigned community role. This role is implemented as a program module. The agent reads and executes the program module in accordance with its role.

```
<policy package>  ::=  <rules> <roles> <contents>
        <rules>   ::=  <rule> | <rule> <rules>
         <rule>   ::=  <condition> <role names>
   <role names>   ::=  <role name>
                  |    <role name> <role names>
    <condition>   ::=  "TRUE"
                  |    "and" <condition> <condition>
                  |    "not" <condition>
                  |    "eq" <attribute>
    <attribute>   ::=  <variable name> <value>
    <attribute>   |    <db name> <key ID> <serial number>
        <roles>   ::=  <role> | <role> <roles>
         <role>   ::=  <role name> <modules>   <init description>
     <contents>   ::=  <content> | <content> <contents>
      <content>   ::=  <content name> <content path>
```

Fig.1 Public policy structure

3.2 Construction of dynamic networks

Ad-hoc networks[7][8] enable continued communication when nodes are added or eliminated dynamically. To send information to a destination node, the nodes in an ad-hoc network select appropriate adjacent nodes and repeat transfer of the reception data. As a result, one of the main characteristics of ad-hoc networks is that data is transferred through several nodes. The nodes act as the agents that establish a route to the destination and that transfer the data. These networks provide easy user deployment of sensor nodes.

In ad-hoc networks, the following functions are important.

(1) Route determination

(2) Data transfer

(3) Link maintenance

Route determination involves the identification of an appropriate communication route between two nodes. Data transfer involves the method by which a node transfers data to another node. Link maintenance entails verifying whether a node can communicate with an adjacent node in the routing pathway. If the node cannot communicate with the adjacent node, another route must be determined. Fig-

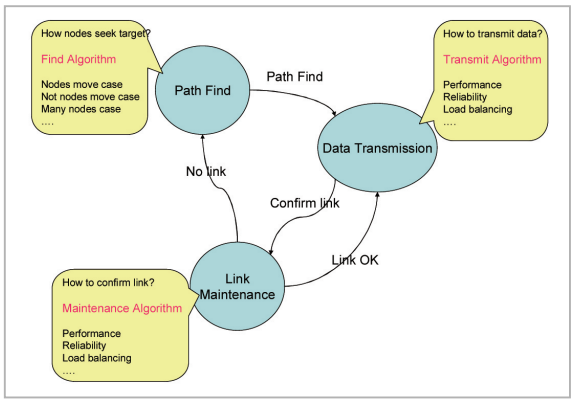

Fig.2 Relationship between the functions of ad-hoc networks

ure 2 shows the relationship between these functions.

First, the communication node needs to find a routing pathway to the destination node. By determining the routing pathway, the node can then identify an adjacent node for delivery of the information to the destination node. When the adjacent node is accessible, the communication node sends data to the adjacent node for subsequent delivery to the destination node. Given that the adjacent node may have moved or may fail to function, the communication node needs to determine whether the adjacent node is accessible. If the node detects that the adjacent node is not accessible, it then determines another route and repeats the routine described above.

These functions are implemented in different ways according to the characteristics of the application and the node. If the node handles important data, the node should adopt a secure method for data transfer. When the application emphasizes transfer performance, the node should adopt a method that emphasizes transfer performance over security. The data transfer method will also differ between data corresponding to physical phenomena and personal data. Personal data should be transferred via a secure method.

The algorithm to implement these functions should be selected according to the application. As it is difficult to devise algorithms corresponding to all applications in advance, nodes should be able to adopt external modules that themselves implement the appropriate algorithms.

The algorithm should also be considered as a type of network behavior. On a macroscopic network level, overall network behavior is an important issue. Even if each node may seem to operate normally, these operations are worthless if the entire system does not function as a network. Even if network traffic exceeds the network capacity, the ad-hoc network must remain stable. In this context, status control and the functions of each node determine the behavior of the entire system as a network. For example, with two or more nodes sharing the same medium, communication easily fails when many nodes search for a path at a given moment. Thus these algorithms should feature a mechanism to prevent network breakdown.

3.3 Access control and routing using VPC on KODAMA

Applying VPC on KODAMA to sensor networks allows these networks to control access and routing. VPC on KODAMA can also provide a mechanism by which nodes acquire the appropriate modules dynamically according to the application. Figure 3 shows a sensor network based on VPC on KODAMA and the corresponding node structure.

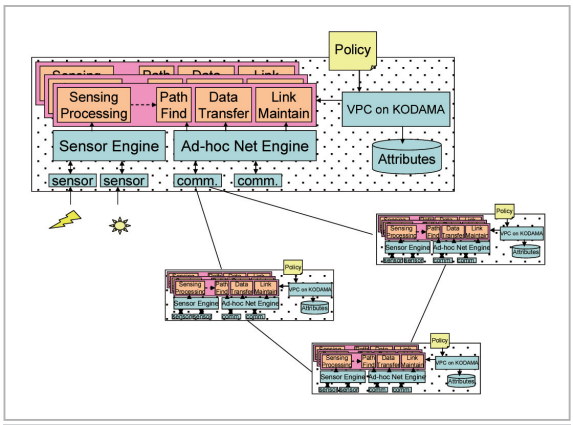

Fig.3 *Architecture of sensor network based on VPC on KODAMA*

Each sensor node has a sensor engine, an ad-hoc network engine, and a VPC on KODAMA engine. The VPC on KODAMA engine manages the attributes of the sensor node and adopts the policies. A policy includes ad-hoc network modules such as the sensor processing module and the route determination module.

The VPC on KODAMA engine evaluates policies based on the engine's attributes and identifies the sensor information processing module, the route determination module, the data transfer module, and the link maintenance module.

The ad-hoc network engine executes the modules selected by the VPC on KODAMA engine. The ad-hoc network engine forms an

ad-hoc network according to the behavior of the route determination module, transfers data through the data transfer module, and maintains the link using the link maintenance module.

The sensor engine manages the sensor in the sensor node. The sensor engine's treatment of the sensors depends on the processing of the module selected by the VPC on KODAMA engine. The sensor information processing module determines how the node receives data from the sensor, how the node processes the data, and destination to which the node transfers the data.

This architecture allows each node to acquire the necessary data from the appropriate sensor, to process the data, and to transfer the data to the appropriate node according to the application policy. Even when processes differ from node to node, this architecture installs the appropriate processes at the corresponding nodes. This architecture also allows the user to install applications easily. The policy propagates in the nodes until its TTL (Time To Live) expires. The user does not need to consider which module should be on which node.

4 Application

This section discusses an RFID sensor network as an applied example of access control and routing based on VPC on KODAMA.

This application is designed to detect the position of a user within a given region. The behavior of the application's sensor network changes according to the automatically detected ID. Each user has an active RFID tag that regularly sends out ID data. The RFID receiver placed within the given region receives the ID and sends the information to the specified server, and the server then calculates the position of the user bearing the ID. Different servers will be selected depending on the ID. The ID qualifies as personal information and should be processed by the appropriate server.

Figure 4 shows an overview of the system. This system consists of two servers, two types of sensors, and two types of RFID tags. One server, sensor, and tag are for VIP users and the other set is for general users. The servers are in charge of managing user information: the VIP server specifically manages VIP user information, and the other server manages information for the remaining users. Each sensor node features a VPC on KODAMA framework, a sensor for the active RFID tag, and an ad-hoc network engine. The only difference between the sensors for VIP users and those for the other sensors involves certification: the sensors for the VIP users feature certification issued and authenticated by the VIP server. The sensor engines and the ad-hoc network engines for VIP users and general users are the same. The tags regularly transmit their IDs; for VIP tags these IDs are coded, while IDs for general users are not.

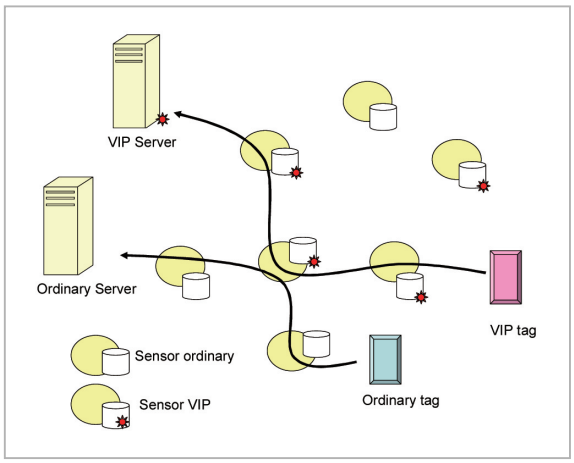

Fig.4 *System overview*

Figure 5 presents an outline of system policy. If a sensor node has the certification of the VIP server, the sensor node can function as a VIP RFID sensor. All sensors can also operate as normal RFID sensors. The policy is described in XML and is authenticated by an S/MIME signature. Each sensor checks the signature to determine whether the policy is genuine.

The role of a VIP RFID sensor is executed by a VIP tag detection module, a signature base route determination module, a data transfer module for communication to reliable nodes (i.e., a "reliable transfer module"), and a

```
<rule>
   <condition> eq VIP certificate </condition>
   <role> VIP RFID sensor </role>
</rule>
<rule>
   <condition> TRUE </condition>
   <role> normal RFID sensor </role>
</rule>
                              …
<role>
   <role name> VIP RFID sensor </role name>
   <module> VIP tag detection </module>
   <module> finding path with signature </module>
   <module> reliable forwarding </module>
   <module> polling link check </module>
</role>
                              …
<role>
   <role name> normal RFID sensor </role name>
   <module> RFID detection </module>
   <module> path finding </module>
   <module> sending </module>
   <module> polling link check </module>
</role>
                              …
```

Fig.5 *Allocation rules and definition of roles*

link check module. The VIP tag detection module can only detect coded VIP tags. The signature base route determination module identifies the route to the VIP server. The algorithm for this module involves three processes. First, the module broadcasts the request message to the destination node, along with the signature of the node. Second, each of the remaining nodes (i.e., other than the destination node) attaches its ID to the message as a signature and transfers the message to the adjacent node. Third, the destination node (the VIP server node) checks the signature list for the request message. If all signatures are genuine, the destination node returns a response message along with the signature list along the reverse route to arrive at the node that transmitted the request message. Each of the nodes in the route registers adjacent nodes authorized by the VIP server and the source node. The VIP server node destroys the message if the list contains nodes lacking VIP server certification. Thus, the VIP sensor nodes can construct a secure route consisting only of VIP RFID sensors. The reliable transfer module sends the coded tag ID detected with the node signature to the adjacent node authorized by the VIP server without modification. Here the node receives an ACK signal from the adjacent node to which it has sent the tag ID. Only the VIP server can decode the coded ID. In this manner, the data can be sent to the server securely without fail. The link check module regularly sends a “Hello” message to adjacent nodes to ensure that the adjacent nodes are accessible.

The role of a normal RFID sensor is executed by an RFID detection module, a route determination module, a transfer module, and a link check module. The RFID detection module detects the normal RFID tags but not the VIP RFID tags. The route determination module finds the route of the broadcasted request (without node signatures). The transfer module sends the detected ID to the general server without authentication.

The user provides this policy to one of the nodes in the sensor network. The sensor nodes copy and distribute the policy among themselves. If the (certified) VIP sensors have the policy, they can function both as VIP RFID sensors and as normal RFID sensors. They send the data with the detected VIP tag securely to the VIP server through the sensor nodes. The VIP sensor can also detect normal tags and transfer the data to the normal server. Other (uncertified) sensors function as normal RFID sensors. They detect general RFID tags and send the data to the general server.

In this manner, the role of the sensor changes according to the policy. The user does not need to deliver the policy to all sensor nodes. The appropriate modules are also installed in the corresponding nodes.

5 Related studies

MOTE[1] is a sensor network module. MAP[2] is a protocol that delivers program codes to sensor nodes. INSENSE[9] is an intrusion-resistant routing protocol for wireless sensor networks. SIA[10] features a mechanism to detect unauthorized nodes through questions (not through an initial assessment of authenticity).

MOTE provides hardware and software

platforms for sensor networks. The MOTE software platform can adopt program codes dynamically. However, the user is required to send the code directly to each node. VPC on KODAMA for sensor networks provides a mechanism that frees the user from having to deliver the program code directly.

MOAP implements multi-hop network programming. One of the challenges of multi-hop network programming is to transmit the program code to two or more sensor nodes without saturating the network. To disseminate the program code packet to the selected number of nodes without saturating the network, MOAP uses an algorithm known as the "ripple dissemination protocol". The purpose of MOAP is to deliver the same program code to all nodes. Thus, it can be difficult to change the program code according to node. VPC on KODAMA for sensor networks, however, provides a mechanism to deliver the program code according to node.

The INSENSE sensor nodes send the detected data to target nodes along several routes. If the destination node verifies data that has passed through several routes, the sensor network can detect unauthorized nodes. As the nodes send the same data two or more times, the communication cost with INSENSE is high. The VPC on KODAMA protection mechanism, on the other hand, provides secure communication without sending the same data more than once. The VPC on KODAMA sensor nodes can verify unauthorized policies using signatures. The matching process is performed within a tamper-resistant device. In this manner, the mechanism can prevent physical and program attacks.

SIA regularly provides nodes with a mechanism to detect unauthorized nodes through questions. This mechanism places a significant load on network resources. This is because the SIA model is aimed at major server control; when the sensor network features a single server, this model functions well. However, with two or more servers, or when the nodes are in mutual communication, the communication cost of the question-based approach is too high. VPC on KODAMA for sensor networks provides signatures in the framework for reliable nodes.

6 Summary

This article discusses a new framework for policy control sensor networks, based on VPC on KOMADA, enabling sensor nodes to feature the appropriate modules as policies. The user need only submit the application policy to the sensor network via a secure method; the sensor nodes then execute their respective roles within the application. VPC on KODAMA represents the fruit of a 15-year research project initiated in 2001 by the former TAO (Telecommunications Advancement Organization of Japan), entitled "Research and development in network security policy control techniques".

Diversity and security of applications are essential in sensor networks. To maximize application diversity, sensor nodes must be able to adopt application modules dynamically and to feature the appropriate modules. How the sensor nodes detect, process, and transfer data will depend on the application. Appropriate detection modules and network modules should be installed. Sensor networks should also be protected against unauthorized access; at the same time, detected data should also be protected.

VPC on KODAMA for sensor networks enables the sensor nodes to determine the appropriate detection module and network module according to the application policy and node attributes. Each policy has a signature, and each node can verify this signature to assess its authenticity. As roles are determined in secure devices, unauthorized devices cannot assume roles.

This article presented an example sensor network that changes its behavior in response to detected RFIDs. The sensor nodes alter their roles according to the applicable attributes and policies, functioning as a secure sensor network. Only nodes that can handle VIP tags can detect these tags securely and transfer data

through authenticated nodes, and only the VIP server can identify the IDs of the VIP tags.

In this manner, VPC on KODAMA for sensor networks provides a suitable framework for these networks. In the future, we intend to discuss lightweight implementation of this system and to develop the framework using actual devices.

References

1 J. Jong and D. Culler, "Incremental Network Programming for Wireless Sensors", IEEE SECON 2004.

2 Thanos Stathopoulos, John Heidemann, and Deborah Estrin, "A Remote Code Update Mechanism for Wireless Sensor Networks", CENS Technical Report #30, http,//lecs.cs.ucla.edu~/ thanos/moap- TR.pdf

3 T.Iwao, S.Amamiya, K.Takahashi, G.Zhong, T.Kainuma, L.Ji, and M.Amamiya, "An Information Notification Model with VPC on KODAMA in an Ubiquitous Computing Environment, and Its Experiment", CIA 2003, pp.30-45, 2003.

4 K.Takahashi, S.Amamiya, T.Iwao, G.Zhong, and M.Amamiya, "Testing of Multi-agent-based System in Ubiquitous Computing Environment", KES 2004, pp.124-130, 2004.

5 T.Iwao, S.Amamiya, G.Zhong, and M.Amamiya, "Ubiquitous Computing with Service Adaptation Using Peer-to-Peer Communication Framework", FTDCS 2003, pp.240-248, 2003.

6 G.Zhong, S.Amamiya, K.Takahashi, T.Iwao, K.Kawashima, T.Ishiguro, T.Kainuma, and M.Amamiya, "You've Got Mail From Your Agent : A Location and Context Sensitive Agent System", ESAW 2003, pp.392-409.

7 A.Bruce McDonald and Taieb Znati "A Mobility-Based Framework for Adaptive Clustering in Wireless Ad-Hoc Networks", IEEE Journal on Selected Areas in Communication, Vol.17, No.8, Aug. 1999.

8 Sung-Ju Lee,William Su and Mario Gerla, "Ad hoc Wireless Multicast with Mobility Prediction", To appear in Proceedings of IEEE ICCCN'99, Boston, MA, Oct. 1999.

9 Deng, J., Han, R., and Mishra, S., "A performance evaluation of intrusion-tolerant routing in wireless sensor networks", In proceedings of the 2nd IEEE International Workshop on Information Processing in Sensor Networks (IPSN 2003), pp.249-364, 2003.

10 Przdatek, B., Song, D., and Perrig, A., "SIA, Secure information aggregation in sensor networks", In proceedings of the 1st ACM International Conference on Embedded Networkd Sensor Systems, ACM Press, pp.255-265, 2003.

***IWAO Tadashige**, Ph.D.*

Ubiquitous Business Development Department, Business Promotion Division, Ubiquitous Systems Group, Fujitsu Limited

Multi-agent Systems, Sensor Network, Ad-hoc Network

***AMAMIYA Makoto**, Dr. Eng.*

Professor, Department of Intelligent Systems, Faculty of Information Science and Electrical Engineering, Kyushu University

Super Parallel Distributed Processing Architecture, Parallel Distributed Artificial Intelligent Systems, Multi-agent Systems