Sensors and Materials, Vol. 30, No. 8 (2018) 1681–1690
MYU Tokyo

S & M 1625

Reliable Node Management Architecture for Disaster Surveillance and Response Systems

Soo-Mi Yang[1] and Hee-Jung Byun[2*]

[1]Department of Information Engineering, The University of Suwon,
Wauan-gil 17, Hwasungsi, Gyeonggido 18323, Korea
[2]Department of Information and Telecommunication Engineering, The University of Suwon,
Wauan-gil 17, Hwasungsi, Gyeonggido 18323, Korea

(Received May 16, 2017; accepted February 16, 2018)

Keywords: disaster surveillance, multisensor network, reliable node management, energy saving, disaster response

In this study, a system supporting disaster surveillance and response decisions is investigated. In a multisensor surveillance system, distributed sensor nodes such as cameras can sense, monitor, and collect data continuously. To recognize an urgent situation and make a decision in response, distributed reasoning agents should be able to analyze and process various surveillance data in real time. However, the loss of resources such as sensor nodes and communication paths may occur during the overall process. Therefore, a safer data delivery system with shorter delays is needed. In this paper, a more reliable node management architecture based on energy-efficient algorithms is proposed to fulfill this need. This architecture determines the path of a packet from either the events generating the packet, the local environmental conditions, or the states of the adjacent nodes to improve the stability, energy efficiency, and delay guarantee of the system. To find the path for the required data, an ant colony optimization algorithm is adopted. This algorithm reduces the decision time and cache processing time resulting in low energy consumption. The performance analysis of the proposed method shows that the scheme improves the system reliability by controlling the parameters of each node.

1. Introduction

Wide-area surveillance should provide necessary responses when disaster occurs. Various sensors are used to detect and predict disastrous events. For disaster surveillance and response, a wide-area network consisting of agents with sensors is built. Each network node is equipped with a reasoning agent, multitype sensors, and communication interfaces. These components enable a node to recognize the environment, exchange sensory data with other nodes, process context data, and make decisions.

To avoid bottlenecks and overcome the loss of resources, a surveillance network is dispersed and replicated. Owing to the lack of central control, the distribution of information is inevitable and thus distributed control techniques that can provide scalability are required. Under these

[*]Corresponding author: e-mail: heejungbyun@suwon.ac.kr

http://dx.doi.org/10.18494/SAM.2018.1869

circumstances, dynamically changing nodes can emerge and disappear without any regulations.

For wide-area surveillance, as indicated in Refs. 1 and 2, electronic vehicles and helicopters are utilized with a central control node. The surveillance areas are assigned with the necessary monitoring equipment like electronic vehicles and helicopters while the response decision is made only in the center node. In Ref. 3, a smart communication platform system (SCPS) is reported to be built between disaster surveillance systems (DSSs). The overall system does not contain the distributed inference agents. As shown in Refs. 4 and 5, an unmanned aerial vehicle (UAV) is used for disaster surveillance. Here, a UAV provides image data transfer to the incident control center while response inference is conducted in the control center. However, the efficiency of the data exchange strategy is not considered.

As the importance of disaster response grows, guidelines for it need to be established. Related ISO standards mainly focus on the role of the government in a disaster, specifically about what government officials should do to maintain control of the situation. Among these standards, ISO/TR 22351(6) describes the message structure required for facilitating interoperability between existing and newly generated information systems. However, the data format is defined without a data management scheme.

Many publications about fault tolerance for unreliable networks have appeared. Recently, a fault-tolerant structural health monitoring system in wireless sensor environments specifically supporting loose coupling between sensors and application components has been developed.(7) However, this work is nonscalable and incompatible with other existing schemes.

Our technique solves the problems identified and is adaptable to existing schemes in a seamless way. It uses decision agents for event detection and utilizes an efficient data exchange method for aggregating the results detected by individual sensor nodes. It can thus select the best decision among different candidates through higher-order inference in shorter time. Although the proposed surveillance network is based on information centric networking (ICN),(8) its direct, unrefined application is not recommended because overhead on management costs may occur. It discourages higher-order reasoning for better decisions, because it is considered too complex to administrate and process. The proposed mechanism for managing surveillance information supports constant creation and helps manage dynamic context definitions and event data over the ICN. The response of the surveillance system is decided dynamically on the basis of the recognized features of the data and the real-time event data from the other nodes. The information is structured in a dispersed way because it is not possible for agents to keep all the required information for context reasoning. To improve the confidence level of unreliable networks in a data exchange, a network reliability model for unreliable nodes and edges is established and a communication method is applied to improve the reliability. Furthermore, we developed a communication algorithm that requires a smaller bandwidth. The proposed architecture not only results in reduced network traffic but also enhances the system performance.

The rest of this paper is organized as follows. In the next section, a reliable disaster management architecture and the analysis model are described. In Sect. 3, experiments to evaluate the performance of our method and its implementation are discussed. Section 4 presents conclusions.

2. Reliable Disaster Management Architecture

Sensor nodes comprising a surveillance network have limited computational capability. To fulfill their needs under challenges such as the dynamic nature of target areas and the instability of communication, a robust and light-weight inference technique is required for event detection and context inference. Furthermore, the network needs to detect disastrous events rapidly enough to create awareness and generate timely alarms. For disaster management, every individual agent performs event detection using its own reasoning algorithm based on the features and events collected from neighboring nodes. To incorporate these tasks, a cooperative inference technique using knowledge bases and decision trees is required. When a decision in a disaster is generated, administrative hierarchy is taken into account.

A standardized message structure by the ISO(6) can contribute to situational awareness among various parties involved in an emergency situation. The standardization of the message structure deals with the message elements and the codes for semantics. Its goal is to make messages unambiguous and it is used to transfer messages between human users and to send parameters for software programs. Such a structured message is called emergency management shared information (EMSI), and it follows an extensible markup language (XML) structure. Figure 1 shows an object model and data elements of EMSI.

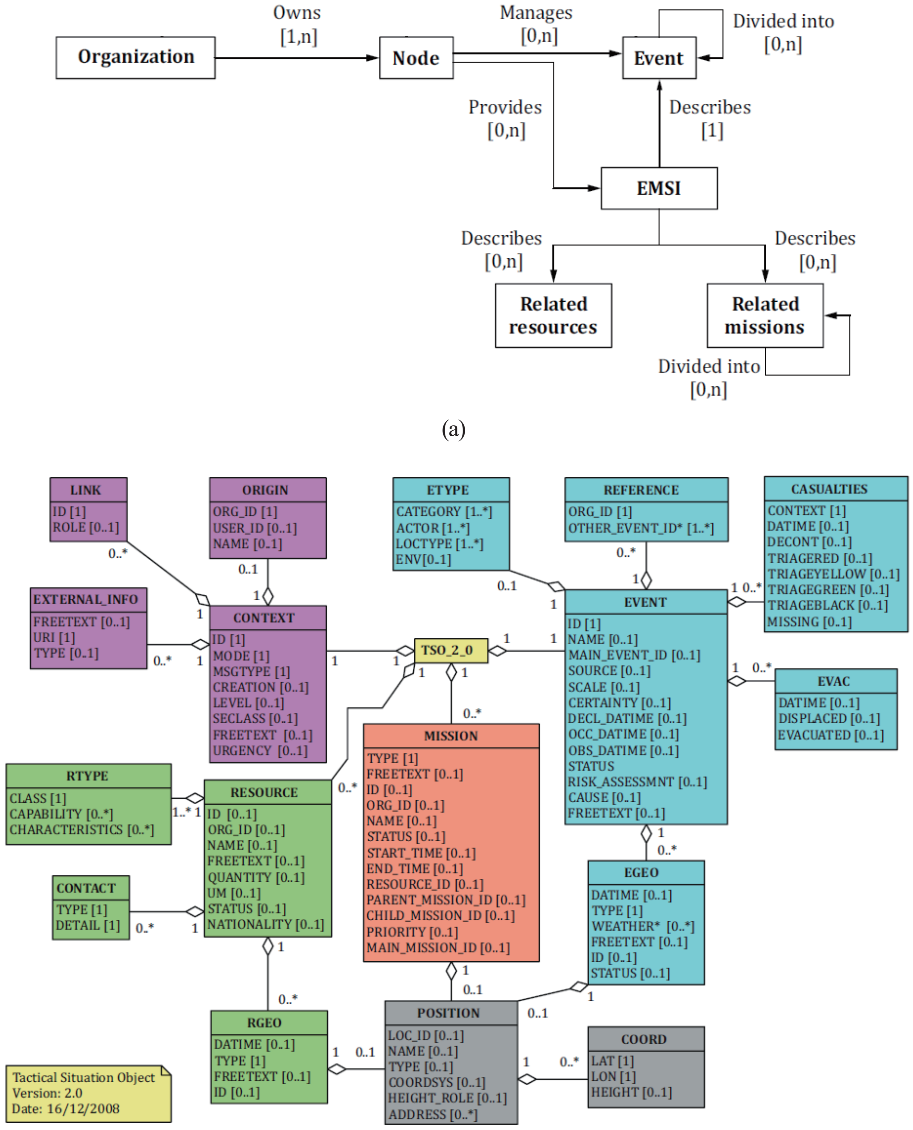
For cooperative and efficient disaster detection and recognition, the EMSI data packet model can be applied when establishing the surveillance policy. To improve the cost incurred by data exchange between nodes, an efficient node management strategy is additionally required.

For cooperation between agents, data packets should be multicasted to achieve fast and scalable transmission. Our network reliability model using this structure for disaster management is composed of two aspects—node dynamics and edge dynamics. Because nodes and edges can emerge and disappear freely in our surveillance environment without any regulations, the following subsections show how to achieve higher reliability with lower cost.

2.1 Node dynamics management

An agent suspects that its neighbor is faulty when it fails to receive requested information. The analysis regarding the distribution of nodes is based on the statistical population of the surveillance information. Because a piece of information is assumed to be randomly uniform, this population can be captured by a binomial distribution.

Packet transmission analysis and management techniques assume that nodes join according to a Poisson process with the rate λ and leave according to an exponential distribution with the rate μ. A fail-stop failure model is assumed so that all nodes leave without informing other nodes. New nodes arrive and leave according to a Poisson process at the same rate to keep the number of nodes in the system roughly constant. The term P_n, the probability of forwarding a message to a faulty node from each node, is shown as



(a)

(b)

Fig. 1. (Color online) (a) Modified object model and (b) data elements of EMSI.

$$
\begin{aligned}
&f(t)=\mu e^{-\mu t},\\
&F(t)=\int_0^t f(x)dx=1-e^{-\mu t},\\
&P_n=1-F(T)\cdot\frac{1}{\mu T}=1-(1-e^{-\mu T})\cdot\frac{1}{\mu T},
\end{aligned}
\tag{1}
$$

where *f*(*t*) represents the probability of error during time *t* and *f*(*t*) represents the cumulative distribution function. In the surveillance network, messages are sent using user datagram protocol (UDP) by default. This is fast and simple, but messages forwarded to a faulty node can be lost. The term T is the maximum time that takes to detect the error. The message loss rate L_n is shown as

$$L_n = 1 - (1 - P_n)^h = 1 - \left(\frac{1 - e^{-\mu T}}{\mu T} \right)^h, \tag{2}$$

where h is the distance corresponding to the number of hops required to access the information. Node availability can be improved by applications if necessary. Applications can use the transmission control protocol (TCP), retransmission, and/or acknowledgement flags. This guarantees a high reliability because nodes can choose an alternate node if a previously chosen one is detected to be faulty. However, waiting for timeouts to detect a faulty node can lead to bad performance. Therefore, the probability of being able to route efficiently without waiting for timeouts using the message loss rate is calculated.

To derive an equation for the cost of maintaining the surveillance network structure, we need to know the control traffic required. Each node generates control traffic dominated by two operations. One is the update operation following node creation and the other is the maintenance operation in forwarding interest base (FIB) and pending interest table (PIT). Thus, the maintenance cost C_n is defined as

$$C_n = \frac{2 \cdot (\lambda_c + \lambda_m) \cdot (\mu \cdot T)^h}{(1 - e^{-\mu \cdot T})^h}, \tag{3}$$

where λ_c is the rate of table entry creation and λ_m is the rate of table entry modification. The two messages for request and reply are considered.

2.2 Edge dynamics management

In a disaster, an unreliable network environment can suffer not only faulty nodes, but also weaknesses of faulty transmission links either wired or wireless. There always exists some degree of packet loss during transmission. However, we should prepare for unreliable packet transmissions especially in disastrous situations.

For reliable delivery of the packets, the surveillance message s_i needs to be delivered to the R_i receivers. Let F_s be the frequency required for the successful transmission of the message s_i to all R_i receivers. The probability of an R_i receiver, r, not receiving the updated information is equal to the probability of packet loss, p, when a single transmission occurs. Let F_r be the frequency of message transmission necessary for receiver r to successfully receive the message packet. Because all the packet loss events for receiver r are mutually independent, F_r is geometrically distributed as(9,10)

$$P_e[F_r = f] = p^{f-1} \cdot (1 - p), \tag{4}$$

and we can deduce the average expected number of packet transmissions as

$$E(F_r) = \sum_{f=1}^{\infty} f \cdot P[F_r = f] = 1/(1-p). \tag{5}$$

Because the packet loss events at different receivers are independent, the probability $P[F_r \leq f]$ expresses that all R_i receivers will receive the packet within f transmissions. The average expected frequency of packet transmissions can be computed as

$$E[F_r] = \sum_{f=1}^{\infty} (1-(1-p^{f-1})^{R_i}). \tag{6}$$

$E[F_r]$ can be numerically computed by truncating the summation when the f-th value falls below the threshold.

2.3 Application of ant colony optimization

A security monitoring network system that utilizes ICN efficiently uses network bandwidth by reducing the amount of transferred data through caching. We can selectively transmit interest packets by ant colony optimization (ACO).(11–13) ACO is a metaheuristic technique for solving combinatorial optimization problems that can be reduced to finding good paths through graphs. An ACO algorithm chooses a route by using pheromone traces of previous ants among multiple paths.

According to the description in Ref. 13, the probability of the k-th transition from the x state to the y state takes the amount of pheromone, τ, and the reciprocal distance η into account. Each influence is controlled by α and β.

$$p_{xy}^{k} = \frac{(\tau_{xy}^{\alpha})(\eta_{xy}^{\beta})}{\sum_{z \in allowed_y} (\tau_{xz}^{\alpha})(\eta_{xz}^{\beta})} \tag{7}$$

Time-consuming complex computational algorithms may not operate properly in a disaster even in a light-weight device. Therefore, we suggest a new algorithm in which the time interval for interest packet arrival is set as the pheromone quantity, as shown in Eq. (8), to achieve faster operation.

$$\begin{aligned} \tau_0 &= C_{time\_threshold} \\ \tau_n &= \frac{\tau_{n-1} + (t_n - t_{n-1})}{k} \end{aligned} \tag{8}$$

The term $C_{time\_threshold}$ is set as the anticipated time interval in the disaster. The term k represents the strength of pheromones. As pheromones spread by ants accumulate, frequent visits of previous interest packets have priority. Interest packets are forwarded to nodes through the path with more pheromones. The level of p_{xy}^{k} also limits the number of packet transmissions. To this purpose, the FIB must record the recent timestamp on each face of the face list. The distance reciprocal η can be calculated as the number of network hops, or the actual distance if the sensor node knows the location through a global positioning system (GPS).

Including the ACO metaheuristic, the main method is shown in Algorithms 1 and 2. In Algorithm 1, constructed EMSI packets are exchanged for the response inference carried out by agents. In Algorithm 2, after initialization, the metaheuristic iterates over three phases. Node and edge dynamics management is applied during packet transmissions.

```
Algorithm 1: The disaster surveillance framework
    while (disaster event occurs) do
        Request information exchange following EMSI
        Route packets utilizing ACO
        Perform response inference
        Route packets utilizing ACO if needed
    end while
```

```
Algorithm 2: The ACO framework
    while (termination condition not met) do
        Construct ant solutions applying Eq. (7)
        Apply local search with neighbors if applicable
        Update pheromones applying Eq. (8)
    end while
```

The faults of nodes and edges in unreliable networks affect the management of the surveillance network. The cost increases proportionally to the packet loss p and the number of recipients, R_i. If we let C_d be the cost for surveillance network management in a disaster, Eqs. (1) through (8) induce C_d, reflecting both node dynamics and edge dynamics.

$$C_d = \sum_{f=1}^{\infty} (1-(1-p^{f-1})^N), \tag{9}$$

where $N \propto C_n \times R_i \times p_{xy}^k$. The performance evaluation and analysis based on Eq. (9) are given in Sect. 3.

3. Performance Evaluation and Experiments

The reliable node management model proposed in this paper provides mechanisms by which node fault and packet loss are dynamically compensated and energy consumption is decreased within the response constraints. To demonstrate the performance enhancement of the proposed model, we measured the expected packet transmissions and compared them with the transmissions generated by an existing model. The plots of expected packet transmissions $E_P[C_d]$ measured according to Eq. (9) are shown in Fig. 2. The probability of packet loss is p and the ratio of faulty nodes to reliable nodes is μ. Higher packet loss represents unreliable network transmission edges. When μ and p are high, the estimated $E_P[C_d]$ is also high. This means that, when the network is unreliable and faulty in a disaster, more packet transmissions occur to overcome the harsh environment. When ACO is applied, P_{xy} represents the level of

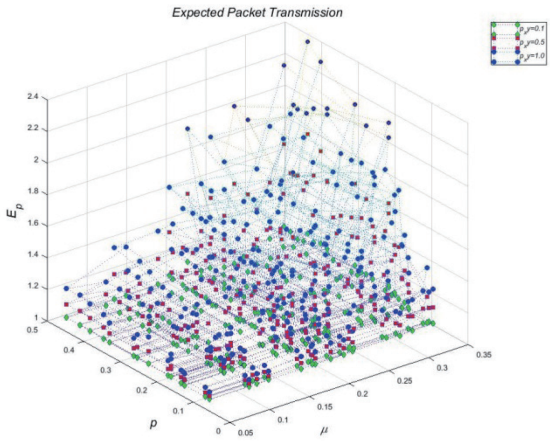


Fig. 2. (Color online) Expected packet transmission comparison by network dynamics.

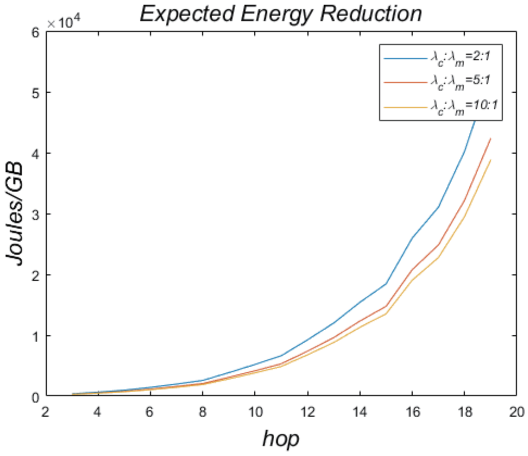


Fig. 3. (Color online) Expected energy reduction by network scaling.

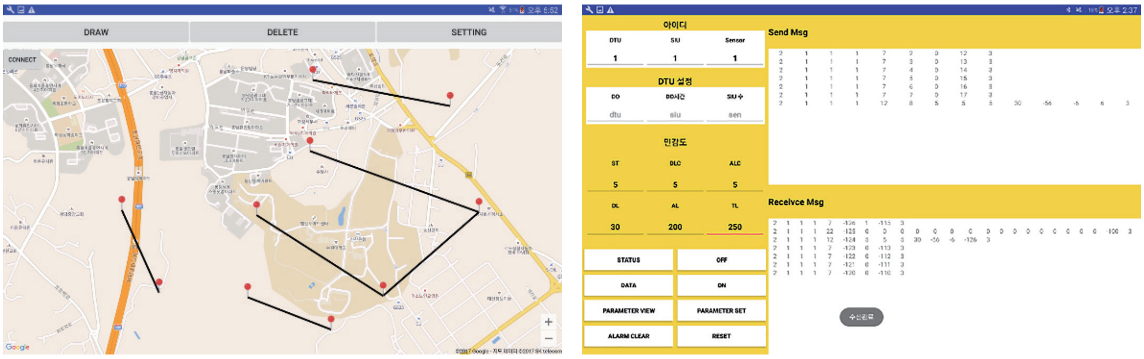
algorithm application. In Fig. 2, the experimental results obtained at P_{xy} values of 1.0, 0.5, and 0.1 are plotted; each P_{xy} represents the absence of algorithm application to normal surveillance and disaster surveillance. However, P_{xy} can vary according to the situation. As P_{xy} decreases, the number of expected packet transmissions gradually decreases. This saves bandwidth and results in energy reduction. The main finding from these evaluations is that, in a disaster surveillance and response system, the application of ACO is helpful for unreliable and faulty network environments.

Figure 3 shows the energy reduced by power comparison. To measure the energy consumption in ICN, we followed the analysis given in Ref. 14. When Eq. (10) is satisfied, energy is reduced.

$$\frac{K*(N-M)*E_{link}}{T_{in-cache}} > P_{storage} \tag{10}$$

In Eq. (10), K is the number of requests, N is the distance from the source, and M is the distance from the cache. In Fig. 3, energy reduction is investigated using the λ_c:λ_m ratio. The terms λ_c and λ_m are the PIT and FIB entry creation and modification rate, respectively. Energy is relatively more reduced in dynamic environments with lower λ_c:λ_m ratios. The analyzed effects indicate that PIT and FIB dynamics are responsible for more energy consumption. Therefore, reducing dynamics by ACO improves the efficiency of disaster surveillance.

The implementation of the proposed architecture will be further developed in the future. Figure 4 shows our current progress. Figure 4(a) shows the dynamics of nodes and edges for understanding the situation. The status of nodes and edges can be inspected and confirmed through the display. Figure 4(b) shows the sensor node interface display. It shows real-time monitoring information to help security officials. Necessary human control interfaces are also provided.



DTU 1 SIU 1 Sensor 1

DO dtu BD시간 siu SIU수 sen

ST 5 DLC 5 ALC 5

DL 30 AL 200 TL 250

Send Msg

```
2  1  1  1  7   2  0  12  3
2  1  1  1  7   3  0  13  3
2  1  1  1  7   4  0  14  3
2  1  1  1  7   5  0  15  3
2  1  1  1  7   6  0  16  3
2  1  1  1  7   7  0  17  3
2  1  1  1  12  8  5  5   5  30  -56  -6  6  3
```

Receivce Msg

```
2 1 1 1 7  -126 1 -115 3
2 1 1 1 22 -125 0 0    0 0  0   0  0    0 0 0 0 0 0 0 0 0 -100 3
2 1 1 1 12 -124 5 5    5 30 -56 -6 -126 3
2 1 1 1 7  -123 0 -113 3
2 1 1 1 7  -122 0 -112 3
2 1 1 1 7  -121 0 -111 3
2 1 1 1 7  -120 0 -110 3
```

(a) (b)

Fig. 4. (Color online) (a) Node and edge status display and (b) sensor monitor of the experiments.

4. Conclusions

The primary goal of our architecture is to provide a reliable, scalable, and efficient monitoring network node management during disasters. To detect disastrous events and to make a decision in a fast and accurate manner, we proposed a distributed disaster surveillance technique. The proposed approach is based on detecting events using an ACO running on sensor nodes and applying a reasoning algorithm for disaster response. For efficient sensor node management, we also considered the characteristics of distributed computing environments. Because these environments are generally heterogeneous, decentralized, and large-scale, they demand a flexible data management technique to distribute messages generated by the disaster.

For reliable distribution of packets, we built a network reliability model based on EMSI and ICN. Then, we investigated the reliability by considering both node dynamics and edge dynamics. The proposed model compensates for the absence of a node caused by node failure or communication failure by utilizing multicast packets to achieve scalability. Equations regarding the loss of messages caused by faulty nodes and the cost of managing the loss are derived. Our model provides an affordable scheme to manage unreliable nodes and communication networks. It can also reduce the management cost and overhead generated by the creation and change of FIB and PIT entries.

The proposed model was simulated and we obtained encouraging performance results. Performance enhancements were quantified by considering faulty nodes and packet loss. Furthermore, with ACO applied to path selection, packets can be sent faster, consuming only a small amount of energy.

Acknowledgments

This research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT & Future Planning (2017R1A2B1007779).

References

1 K. Mase: 2013 IEEE 24th Annual Int. Symp. Personal Indoor and Mobile Radio Communications (PIMRC) (IEEE, London, 2013) 3466.

2 K. Mase: Sens. Transducers **185** (2015) 84.

3 Z. N. K. Wafi, A. H. Alnajjar, and R. B. Ahmad: Proc. Technology Management and Emerging Technologies (ISTMET) (IEEE, New York, 2015) 369.

4 C. Luo, E. Asemota, and C. Grecos: Proc. Vehicular Technology Conference (VTC Spring) (IEEE, 2015) 1.

5 A. Wada, T. Yamashita, M. Marutama, T. Arai, H. Adachi, and H. Tsuji: NEC Technical Journal **8** (NEC Corporation, Tokyo, 2015) 68.

6 ISO/TR 22351:2015 Societal security-Emergency management-Message structure for exchange of information https://www.iso.org/standard/57384.html (accessed July 2017).

7 M. Z. A. Bhuiyan, G. Wang, J. Cao, and J. Wu: IEEE Trans. Comp. **64** (IEEE, New York, 2015) 382.

8 IRTF Information-Centric Networking Research Group https://irtf.org/icnrg (accessed July 2017).

9 S. Rafaeli and D. Hutchison: ACM Comput. Surv. **35** (ACM, New York, 2003) 309.

10 S. Setia, S, Zhu, and S, Jajodi: Perform. Eval. **49** (2002) 21.

11 M. Dorigo, M. Birattari, and T. Stutzle: IEEE Comp. Intell. Mag. **1** (2006) 28.

12 M. Dorigo and T. Stützle: Handbook of Metaheuristics (Springer US, New Mexico, 2010) p. 227.

13 Ant Colony Optimization Algorithms https://en.wikipedia.org/wiki/Ant_colony_optimization_algorithms (accessed July 2017).

14 T. Braun and T. A. Trinh: European Conf. Energy Efficiency in Large Scale Distributed Systems EE-LSDS 2013, LNCS **8046** (Springer, Heidelberg, 2013) 271.

About the Authors

Soo-Mi Yang received her B.S., M.S., and Ph.D. degrees in computer engineering from Seoul National University of Seoul, Korea, in 1985, 1987, and 1997, respectively. From 1988 to 2000, she was a researcher at the Korea Telecom Research Center where she worked on telecommunication networks, internet, and information security. From 2000 to 2001, she was a visiting scholar at UCLA, USA. From 2002 to 2004, she was a faculty of the Suwon Science College, Korea. She is currently an associate professor in the Department of Information Engineering at The University of Suwon, Korea. Her research interests include access control, network security, and secure system software.

Hee-Jung Byun received her B.S. degree from Soongsil University, Korea, in 1999, an M.S. degree from Korea Advanced Institute of Science and Technology (KAIST), Korea, in 2001, and a Ph.D. degree from KAIST in 2005. She was a senior researcher at the Samsung Advanced Institute of Technology and Samsung Electronics from 2007 to 2010. She is currently an associate professor in the Department of Information and Telecommunications Engineering, The University of Suwon, Korea. Her research interests include network protocol design, network modeling, controller design, and theoretical analysis.