Survivability Evaluation Model in Wireless Sensor Network using Software Rejuvenation*

Sazia Parvin** · Thandar Thein** · Dong Seong Kim** · Jong Sou Park**

ABSTRACT

The previous works in sensor networks security have focused on the aspect of confidentiality, authentication and integrity based on cryptographic primitives. There has been no prior work to assess the survivability in systematic way. Accordingly, this paper presents a survivability model of wireless sensor networks using software rejuvenation for dual adaptive cluster head. The survivability model has state transition to reflect status of real wireless sensor networks. In this paper, we only focus on a survivability model which is capable of describing cluster head compromise in the networks and able to switch over the redundant cluster head in order to increase the survivability of that cluster. Second, this paper presents how to enhance the survivability of sensor networks using software rejuvenation methodology for dual cluster head in wireless sensor network. We model and analyze each cluster as a stochastic process based on Semi Markov Process (SMP) and Discrete Time Markov Chain (DTMC). The proof of example scenarios and numerical analysis shows the feasibility of our approach.

Key words : Wireless Sensor Networks, Security, Survivability, Availability

---

* THIS WORK WAS SUPPORTED BY 2006 KOREA AEROSPACE UNIVERSITY FACULTY RESEARCH GRANT

** Dept. of Computer Engineering, Korea Aerospace University

1. Introduction

Wireless Sensor Networks (WSN) consists of a large number of wireless communicating ultra small autonomous devices, called sensor nodes, which are powered with low powered battery and equipped with integrated sensors. In typical application scenarios, sensor nodes are spread randomly to collect sensor data depending on the query. Sensor nodes in sensor networks are usually deployed in antagonistic location, and they should continue to supply its necessary service in a timely manner even though they are under attack or compromised by adversaries. This undefined difficulty is considered as survivability problem in wireless networks. The survivability of conventional networks as well as wireless networks has been considered as a significant issue. Survivability of a system can be defined as the capability to fulfill its mission, in a timely manner, in the presence of intrusions, attacks, accidents and failures[2]. Many researches have been done on sensor network security but the researchers have been focused only security in wireless sensor networks in terms of confidentiality, integrity and authentication. However a small number of studies have been performed on the survivability of wireless sensor networks which is not enough to ensure the survivability in WSNs. Kim et al.[4] proposed a survivability framework of sensor networks in order to enhance the lifetime of sensor nodes but they didn't show any specific methodology. Chiang et al.[12] proposed an approach to increase the availability of sensor networks but they need additional hardware. Recently Kim et al.[11] has proposed adaptation mechanisms to increase the survivability of Sensor networks against Denial of Service attack. They assumed that software rejuvenation is capable to enhance the survivability of sensor nodes in WSN.

As sensor nodes can be attacked by different kinds of threats or compromised by many adversaries in hostile environment. So in this paper, we present a framework of survivability model through software rejuvenation using Semi Markov Process(SMP) and Discrete Time Markov Chain(DTMC) which is capable to enhance the survivability of sensor networks when cluster head is compromised or attacked by adversaries. We employ software rejuvenation which is very cost effective techniques as they don't need any additional hardware. Our model uses a hierarchical cluster based sensor network, which has advantages in terms of cost and energy[1]. We model each single cluster as stochastic process. We analyze Semi Markov Process(SMP) and Discrete Time Markov Chain(DTMC) for our dual cluster head approach.

The rest of this paper is organized as follows. In section 2, related works including brief description of survivability and software rejuvenation are introduced. Our proposed framework for modeling and enhancing survivability based on dual adaptive cluster head of Sensor Networks and model analysis is explained in section 3. In section 4 we discuss our approach in terms of security analysis and future works. At last concluding remarks are presented in section 5.

2. Related Works

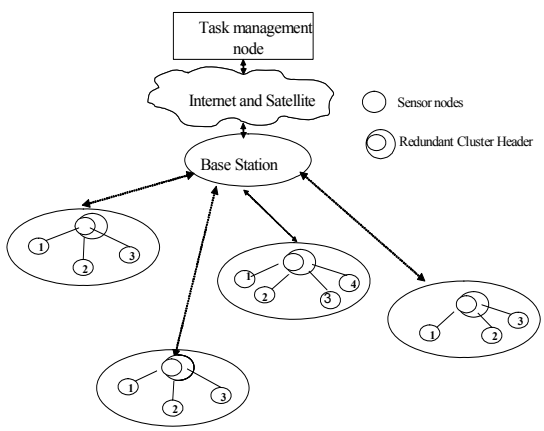
The survivability of conventional networks as

well as wireless networks has been considered as a significant issue. Survivability of a system can be defined as the capability to fulfill its mission, in a timely manner, in the presence of intrusions, attacks, accidents and failures[2]. Kim et al.[4] proposed a survivability framework of sensor networks in order to enhance the lifetime of sensor nodes but they didn't show any specific methodology. Chiang et al.[12] have proposed an approach to increase the availability of sensor networks but they need additional hardware. This redundant hardware requires additional cost. Recently Kim et al.[11] has proposed adaptation mechanisms to increase the survivability of Sensor networks against Denial of Service attack. They assumed that software rejuvenation is capable to enhance the survivability of sensor nodes in WSN. Moon et al.[15] has proposed to the task-role based access control(TBAC) for sensor nodes to enhance the survivability of sensor networks but this approach requires extra information such as membership and the task placed to each sensor node.

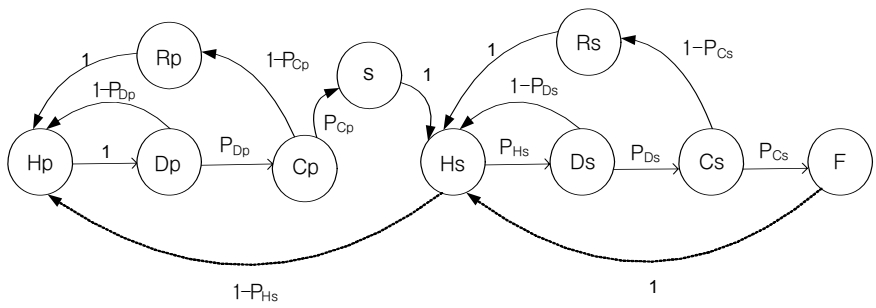
In this paper we want to enhance the survivability of sensor networks by adopting software rejuvenation methodology in dual cluster head in WSNs. Software rejuvenation is a fault management technique which is proactive and aimed at cleaning up the internal system state to prevent the occurrence of more severe future crash failures[8, 9]. Recently Aung et al.[7] have employed software rejuvenation in security field and evaluated its feasibility in terms of availability and survivability. Software rejuvenation is an intervallic preemptive rollback of continuously running application to prevent failures in future[3]. Theinn et al.[16] proposed the survivability model for dual base station but they didn't show survivability evaluation result. So in this paper we show a survivability model of wireless sensor networks using software rejuvenation to dual cluster head.

3. A Framework of Survivability Model

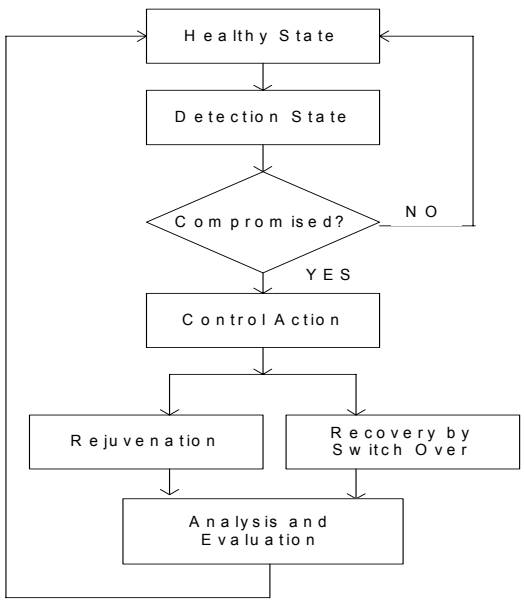
An overall architecture of the framework of survivability model is depicted in(Figure 1). Our framework adopts a hierarchical structural design with dynamic topology. This kind of topology named cluster based sensor network has advantages in terms of cost and energy[1]. One base station manages one or more cluster. Clustering sensors into groups, so that sensors communicate information only to cluster heads and then the cluster heads communicate information to the processing center, may save energy. So in this paper we propose software rejuvenation with dual cluster heads so that in case of failure, an idle cluster head will take



(Figure 1) Wireless Sensor Network with dual cluster head



(Figure 3) State Transition Model



(Figure 2) A framework of survivability model with software rejuvenation

over the duty in a very short time after a serious problem occurred in the primary cluster head. This mutual cluster representation provides a concept to the framework. Each mutual cluster with redundant cluster head can be modeled based on Markov process. Also we can apply software rejuvenation to each cluster head.

A framework of survivability model with rejuvenation for dual adaptive cluster head in wireless sensor network is presented in figure 2. In this framework we considered the system's survivability in different phases and different actions. This model contains six states: Healthy State, Detection State, Compromised State, Rejuvenation State, Redundant State and Failure State.

In rejuvenation state, software rejuvenation methodologies are performed by the policies. In the redundant state, primary cluster head is failed by the active attacks ; a protection switch successfully restores services by switching to the secondary cluster head. If both of the cluster heads are failed, then the system will restore the cluster by selecting the new cluster head.

We construct the state transition model to describe the behavior of the dual cluster head in WSN as shown in (Figure 2).

Let us assume that,

Hp-Healthy state for primary cluster head,

Hs-Healthy state for secondary cluster head

Dp-Detection state for primary cluster head,

Ds-Detection state for secondary cluster head

Cp-Compromised state for primary cluster head, Cs-Compromised state for secondary clus-

ter head.

Rp-Rejuvenation state for primary cluster head, Rp-Rejuvenation state for secondary cluster head, S-Switch Over state, F-Failure State

The various steady state parameters are summarized as follows:

〈Table 1〉 Steady state parameters of SMP

P_{Dp}	Probability of detecting attack for Primary Cluster Head
P_{Ds}	Probability of detecting attack for Secondary Cluster Head
P_{Cp}	Probability that a successful attack has been occurred for primary cluster head
P_{Cs}	Probability that a successful attack has been occurred for secondary cluster head
P_{Hp}	Probability of active primary cluster head
P_{Hs}	Probability of active secondary cluster head
h_{Hp}	Mean time to resist becoming vulnerable to attacks for primary cluster head
h_{Hs}	Mean time to resist becoming vulnerable to attacks for Secondary cluster head
h_{Dp}	Mean time to detect attack when already vulnerable for primary cluster head
h_{Ds}	Mean time to detect attack when already vulnerable for secondary cluster head
h_{Cp}	Mean time to compromise an attack and apply appropriate strategy for recovery for primary cluster head
h_{Cs}	Mean time to compromise an attack and apply appropriate strategy for recovery for secondary cluster head
h_{Rp}	Mean time to perform rejuvenation for primary cluster head
h_{Rs}	Mean time to perform rejuvenation for secondary cluster head
h_S	Mean time to switchover to standby component for undetected attack
h_F	Mean time that the system is in failure state

For computing the availability measure, first we need to compute the steady-state probabilities$\{\pi_i, i \in X_S\}$ of the SMP states.

$$\pi_i = \frac{d_i h_i}{\sum_j d_j h_j},\ i, j \in X_S \tag{1}$$

Where XS = set of States,

$X_S = \{H_P, D_P, C_P, R_P, S, H_S, D_S, C_S, R_S, F\}$

We can assume that

di=embedded DTMC steady state probabilities

hi = mean sojurn time hi's in state $i \in X_S$

The DTMC steady state probabilities di's can be computed as, $\bar{d} = \bar{d}P$ (2)

where, P = DTMC transition probability matrix

$\bar{d} = [d_{H_P}, d_{D_P}, d_{C_P}, d_{R_P}, D_S, d_{H_P}, d_{D_S}, d_{C_S}, d_{R_S}, d_F]$

$$\sum_i d_i = 1, \qquad i \in X_S \tag{3}$$

Rewriting equation (2) into the elementary form, the following DTMC steady state probabilities are made,

$$d_{Hp} = d_{Dp}(1-p_{Dp}) + d_{Rp} + d_{Gs}(1-p_{Hs}) \tag{4}$$
$$d_{Dp} = d_{Hp} \tag{5}$$
$$d_{Cp} = d_{Dp}\, p_{Dp} \tag{6}$$
$$d_{Rp} = d_{Cp}(1-p_{Cp}) \tag{7}$$
$$d_S = d_{Cp}\, p_{Cp} \tag{8}$$
$$d_{Hs} = d_S + D_{Ds}(1-p_{Ds}) + d_{Rs} + d_F \tag{9}$$
$$d_{Ds} = d_{Hs}\, p_{Hp} \tag{10}$$
$$d_{Cs} = d_{Ds}\, p_{Ds} \tag{11}$$
$$d_{Rs} = d_{Cs}(1-p_{Cs}) \tag{12}$$
$$d_F = d_{Cs}\, p_{Cs} \tag{13}$$

Solving the above equations, in conjunction with the total probability relationship given by

(3) gives,

$$d_{H_p} = \frac{(1-p_{H_S})}{2(1+p_{D_p})(1-p_{H_S})+p_{C_p}p_{D_p}[1+p_{H_S}(1+2p_{D_S})]} \quad (14)$$

3.1 Semi-Markov Model

In order to compute the SMP steady-state probabilities(π_i), it can be assumed that the mean sojurn time of states be : { h_{HD}, h_{Dp}, h_{Cp}, h_{Rp}, h_S, h_{Hs}, h_{Ds}, h_{Cs}, h_{Rs}, h_F}

$$\pi_{H_p} = \frac{h_{H_p}}{[h_{H_p}+h_{D_p}+p_{D_p}[h_{C_p}+(1-p_{C_p})h_{R_p}+p_{H_p}h_S]+\frac{p_{C_p}p_{D_p}}{(1-p_{H_S})}]}$$

$$[h_{H_S}+p_{H_S}(h_{D_S}+p_{D_S}h_{C_S})+p_{H_S}p_{D_S}((1-p_{C_S})h_{R_S}+p_{C_S}h_F)] \quad (15)$$

$$\pi_{Dp} = h_{Dp}\frac{\pi_{Hp}}{h_{Hp}} \quad (16)$$

$$\pi_{Cp} = p_{Dp}h_{Cp}\frac{\pi_{Hp}}{h_{Hp}} \quad (17)$$

$$\pi_{Rp} = p_{Dp}(1-p_{Cp})h_{Rp}\frac{\pi_{Hp}}{h_{Hp}} \quad (18)$$

$$\pi_S = p_{Dp}p_{Cp}h_{Cp}\frac{\pi_{Hp}}{h_{Hp}} \quad (19)$$

$$\pi_{Hs} = \frac{P_{Cp}p_{Dp}}{(1-p_{Hs})}h_{Hs}\frac{\pi_{Hp}}{h_{Hp}} \quad (20)$$

$$\pi_{Ds} = \frac{P_{Cp}p_{Dp}}{(1-p_{Hs})}p_{Hs}h_{Ds}\frac{\pi_{Hp}}{h_{Hp}} \quad (21)$$

$$\pi_{Cs} = \frac{P_{Cp}p_{Dp}}{(1-p_{Hs})}p_{Hs}p_{Ds}h_{Cs}\frac{\pi_{Hp}}{h_{Hp}} \quad (22)$$

$$\pi_{Rs} = \frac{P_{Cp}p_{Dp}}{(1-p_{Hs})}p_{Hs}p_{Ds}(1-p_{Cs})h_{Rs}\frac{\pi_{Hp}}{h_{Hp}} \quad (23)$$

$$\pi_F = \frac{P_{Cp}p_{Dp}}{(1-p_{Hs})}p_{Hs}p_{Ds}p_{Cs}h_F\frac{\pi_{Hp}}{h_{Hp}} \quad (24)$$

Now we can derive the equation for availability and survivability.

The system availability in the steady state is defined as

$$A = 1(\pi_S+\pi_F) \quad (25)$$

The system is not survived in all of the rejuvenation process in the normal state, switchover state, and the failure state. The survivability of the system is defined as follows:

$$S = A-[(1-\pi_{Rf})+(1-\pi_{Rs})] \quad (26)$$

3.2 Model Analysis for Software Rejuvenation

In this section, we illustrate the evaluation of model with numerical results. To analyze the SMP model, we need to set parameters for the transition probability and the mean sojurn time in each state. The following Simulation parameters values of SMP are chosen for our analysis.

Mean Sojurn Time:
h_{Hp} = .5, h_{Dp} = 1/3, h_{Cp} = 0.25, h_{Rp} = 0.2,
h_S = 0.5, h_{Hs} = 0.5, h_{Ds} = 1/3, h_{Cs} = 0.25,
h_{Rs} = 0.2 and h_F = 0.5

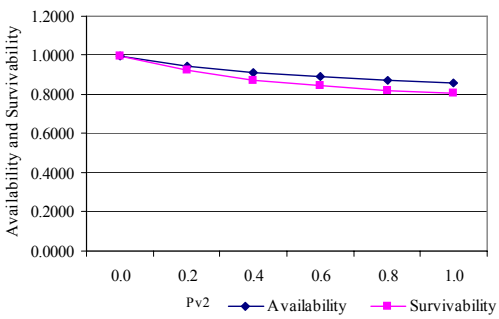
Transition probability :
P_{Dp} = P_{Cp} = P_{Cs} = P_{Hs} = 0.5, 0 < P_{Dp} <1
P_{Ds} = P_{Dp} = P_{Cs} = P_{Hs} = 0.5, 0 < P_{Cp} <1

A good system must be in compromised state as short as possible. Accordingly we assume the mean time of the compromised state is less than that of both states Healthy state (H) and Detection sate (D) in the primary and standby WSN-cluster head. The mean time spent in the Healthy

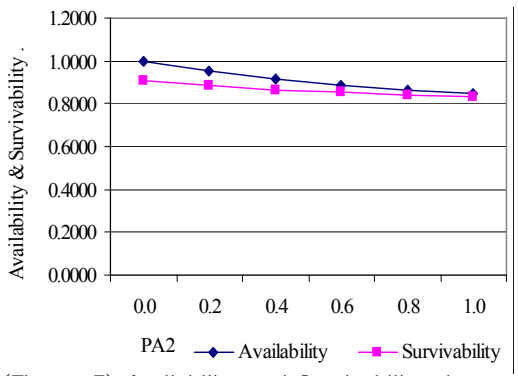
state, $h_{Hp} = h_{Hs} = 1/2$ and the mean time spent in the Detection State, $h_{Dp} = h_{Ds} = 1/3$ time units. The mean time the attacker spends in the state (C), $h_{Cp} = h_{Cs} = 1/4$ time units. On the other hand, rejuvenation must be faster than any other activities. So we assume that the mean time of being in state R is shorter than that of S and F state.

In the rejuvenation state, the mean time spent by the system, $h_{Rp} = h_{Rp} = 0.2$ time units. The mean time spent in the switch over state and failure state: hs and h_F are .5 times respectively. In order to analyze the effects of the transition probability at each states, the probability was set a value between 0.0~1.0.

(Figure 4), (Figure 5) shows the relationships between P_D and P_C. The availability and survivability are increased when the primary cluster head can detect abnormal behaviors of the system in the initial state before they are exposed to the attacks or vulnerable environments. When P_{Dp} is getting bigger (detection capabilities in initial state are degraded), and the availability and survivability of the system are reduced dramatically. When P_{Cp} is getting smaller (the probability of state transition to



(Figure 4) Availability and Survivability changes due to P_{Dp}



(Figure 5) Availability and Survivability changes due to P_{Cp}

rejuvenation state is bigger), the availability and survivability of the system are increased.

4. Security Analysis and Discussion

4.1 Security Analysis

In this section we show some example for explanation how our proposed approach are able to countermeasure several attacks.

DoS Attack-Flooding. Wireless Sensor Networks are especially vulnerable to Denial of Service (DoS) attacks. A DoS attack is any event that diminishes a network's capability to perform its expected function. This type of DoS attack is occurred where connection based communication exists. Adversary node continuously sends a flood of TCP/SYN packet to one node in order to attack a target sensor network as almost nodes of sensor network play a part in routing.

When a cluster head is attacked by the attacker, the whole cluster could be easily compromised. Cluster head is responsible for data aggregation and transferring aggregated data

to base station. If cluster head is attacked, it can bring down the entire cluster. So in this paper we apply dual adaptive cluster head approach using software rejuvenation. If the primary cluster head is compromised then it will switch to secondary cluster head with a very short time and then the whole cluster will be in normal condition.

Buffer Overflow Attack. The cluster head sensor node has a buffer memory and when software is executed in sensor node the variables take place in memory space. Sometimes this buffer memory overflows due to many applications running. So in this situation if we are able to apply software rejuvenation, it will clean up the memory and prevent the cluster head node from buffer overflow attack.

4.2 Discussion and Future work

Software rejuvenation methodology doesn't need any additional hardware so it is cost effective technique for increasing the survivability using the software rejuvenation in dual adaptive cluster head of wireless sensor networks. Our future works include that to apply our approach with real WSN. And we will perform more experiments and verify our methodology in Dynamic programming manners. In the following table we show the comparisons of previously proposed mechanisms and our proposed approach for sensor networks.

〈Table 2〉 The Comparisons of Previous Approach and our Proposed Approach

	Previous Approach	Proposed Approach
Method	Software rejuvenation but there is no specific technique for software rejuvenation.	Software rejuvenation using Markov Model for dual adaptive cluster head.
Flexibility	Not clearly mentioned.	Shows high survivability level in face of attacks by having dual cluster head.

5. Conclusion

Earlier sensor node security mechanisms almost focus on ensuring the confidentiality and integrity and authentication way. So in this paper we proposed a framework of survivability model with software rejuvenation and redundant recovery approach for clustering in wireless sensor networks. The modeling framework for having dual cluster head provides better understanding of the survivability requirements in WSN. This approach can increase the whole network survivability by increasing the clustering survivability having dual adaptive cluster head in the face of attack in the wireless sensor networks.

참 고 문 헌

[1] Y. Guo, J. McNair, "Cost-Efficient Cluster Formation for Wireless Sensor Networks", In Proc. of the 2nd Int.Conf. On Cybernetics and Information Technologies, Systems and Applications, 2005.

[2] R. Ellison, D. Fisher, R. Linger, H. Lipson,

T. Long staff, and N. Mead, "Survivable Network Systems : An Emerging Discipline", CMU/SEI-97-TR-013, 1997.

[3] Y. Huang, C. Kintala, N. Kolettis, and N. Fulton, "Software rejuvenation : analysis, module and application", In Proc. of the Int. Sym. on Fault Tolerant Computing, Pasadena, CA, 1995, pp. 381-390.

[4] D. Kim, K. Shazzad and J. Park, "A Framework of Survivability Model for Wireless Sensor Network", In Proc. of Int. Conf. on Availability, Reliability and Security, 2006, pp. 515-522.

[5] M. Strasser, H. Vogt, "Autonomous and Distributed Node Recovery in Wireless Sensor Networks", SASN'06, Alexandria, Virgina, USA, October 30, 2006.

[6] H. Su and X. Zhang, "Energy Efficient Clustering System Model and reconfiguration Schemes for wireless Sensor Networks", In the Pro. Of Information Sciences and Systems, 2006 40th Annual Conference, 2006, pp. 99-104.

[7] K. Aung, K. Park and J. Park, "A Rejuvenation Methodology of Cluster Recovery", Proceedings of the Fifth IEEE International Symposium on Cluster Computing and the Grid (CCGrid 2005), 2005, Volume 1-Volume 2001, pp. 90-95.

[8] C. Hofmeister, J. Purtilo, "Dynamic Reconfiguration in Distributed Systems : Adapting Software Modules for Replacement", In Proc. Int. Conf. on DCS. 1993, pp. 101-110.

[9] Y. Huang, C. Kintala, N. Kolettis, and N. Fulton, "Software rejuvenation: analysis, module and application", In Proc. of the Int. Sym. on Fault Tolerant Computing, Pasadena, CA, 1995, pp. 381-390.

[10] S. Kogekar, "Constraint-guided dynamic reconfiguration in sensor networks", In Proc. of the third Int. sym. on Information processing in sensor networks, Berkeley, California, USA, 2004.

[11] D. Kim, C. Yang, and J. Park, "Adaptation Mechanisms for Survivable Sensor Networks against Denial of Service Attack", The Second International Conference on Availability, Reliability and Security (ARES 2007) pp. 575-579.

[12] M. Chiang et al, "Architecture of Increased Availability Wireless Sensor Network Nodes", In Proc. Int. Test Conf. 2004, pp. 1232-1241.

[13] S. Bapat, and A. Arora, "Stabilizing Reconfiguration in Wireless Sensor Networks", OSU-Technical Report OSU-CISRC-2/06-TR24.

[14] G. Fuchs, S. Truchat, and F. Dresser, "Distributed Software Management in Sensor Networks using Profiling Technique", In Proc. of 1st Int. Workshop on Software for Sensor Networks, New Delhi, India, 2006.

[15] M. Moon, D. kim and J. Park, "Towards Modeling Sensor Node Security Using Task-Role Based Access Control with Tinysec", Springer-Verlag Heidelberg, lecture Notes in Artificial Intelligence, 2007.

[16] S. Win, T. Thein and J. Park, "To Increase Survivability with Software Rejuvenation by Having Dual Base Station in WSN Environment", In Proc. of Frontiers of High Performance Computing and Networking - ISPA Workshops, Canada, 2007.

Sazia Parvin

2005년 Bachelor of Science, Dept of computer Engineering, Jahangirnagar University

2006년 present. MS in Computer Engineering, Korea Aerospace University

Thandar Thein

1992년 Bachelor, University of Yangon

1996년 MS in Computer Science, University of computer Studies, Yangon

2004년 PhD, University of computer Studies, Yangon

2007년 present. postdoctoral research fellow in Korea Aerospace University

Dong Seong Kim

2001년 Bachelor of Science, Dept of computer Engineering, Kore Aerospace University

2003년 MS in Computer Engineering, Korea Aerospace University

2008년 PhD, in Computer Engineering, Korea Aerospace University

Jong Sou Park

1983년 Bachelor of Science, Dept of Telecommunication Engineering, Korea Aerospace University

1986년 MS in Electronic computer Engineering, North Carolina State University

1994년 PhD, in Computer Engineering, Pennsylvania State University

1994~1996년 Assistant Professor in Computer Engineering, Pennsylvania State University

1996년 Present Professor in Computer Engineering, Korea Aerospace University