NUMBER OF NEIGHBOUR NODES BASED NEXT FORWARDING NODES DETERMINATION SCHEME FOR ENERGY ENHANCEMENT OF WSNS USING A FUZZY SYSTEM

Jae Kwon Lee and Tae Ho Cho

School of Information Communication Engineering, Sungkyunkwan University
Suwon 400-746, Republic of Korea
jklee@ece.skku.ac.kr, taecho@ece.skku.ac.kr

ABSTRACT

Wireless Sensor Networks (Wsn) Are Used In Various Areas. These Networks Are Deployed In An Open Environment. So, They Are Very Weak Against An Attack, And Easily Damaged.The Wsn Has Limited Resources In Terms Of Battery Life, Computing Power, Communication Bandwidth And So On. Many Attacks Aim At That Point.The False Report Injection Attack Is One Of Them. Yu Et Al. Proposed A Dynamic En-Route Filtering Scheme (Def),To Prevent A False Report Injection Attack.In This Paper, We Propose An Energy Enhancement Scheme For Def Using A Fuzzy System. The Def Is Divided Into Three Phases (Key Pre-Distribution Phase, Key Dissemination Phase, Report Forwarding Phase). We Applied Our Scheme At The Next Forwarding Node Determination. So We Used Three Input Factors Of A Fuzzy System To Make A Determination. These Are The Availability Of Energy, Distance To The Base Station, And Usage Count.Through The Experiments, Our Proposed Method Shows Up To 8.2% Energy Efficiency, Compared With The Def. If The Networks Consume More Energy, Our Proposed Method Shows More Efficiency For The Energy.

KEYWORDS

Wireless Sensor Networks, Fuzzy Rule-based System, Dynamic Filtering Scheme, False Report Injection Attacks

1. INTRODUCTION

Wireless Sensor Networks (WSN) have been applied in many areas to enrich people's lives [1-2]. Sensor configuring of sensor networks is made forvarious functions with lowpower and lowcost. These sensorsare distributed in an open environment [1]. A sensor node would be deployed in a dangerous place, or a place that people cannot go.The WSN would consist of one or more base stations, and many sensor nodes [2]. Each sensor hasthe function of sensing, computing and wireless communication. The base station collects necessary information from each sensor, and manages it. If some event occurs, the sensor detects that event, and delivers that information to the base station[1].Figure 1 shows briefly the operation of the WSN.

A WSN would be easily attacked by an adversary, because it was configured in an open environment [3].The adversary can easily damage sensor nodes, using a compromised node. A false report injection attack of those attacks would cause a false alarm at the base

DOI : 10.5121/ijcsity.2013.1305

station.Therefore, this attack can needlessly consume the energy of the forwarding nodes on the forwarding path[4-5].

To protect against these attacks, many schemes of various forms have been proposed. One of them is the Dynamic En-route Filtering scheme (DEF) that Yu and Guan proposes[4]. The DEF is divided into three main phases. Those three phases are the key pre-distribution phase, the key dissemination phase and the report forwarding phase. These are explained in the following section.In this paper, we proposed a method for enhancement of the energy efficiency with sustaining the detection power, using fuzzy logic in the DEF. The forwarding nodes to send a report are determined by the fuzzy logic. We use three input factor for the fuzzy logic. These are the number of neighbour nodes, the available energy and the usage count.

This paper is organized as follows. In chapter 2, we explain the DEF in detail, and refer to the motivation of the proposed method. In chapter 3, we explain the proposed method in detail. In chapter 4, we show the experimental results, which compare the basic DEF and the proposed method. In chapter 5, we refer to the experimental results, and future work.

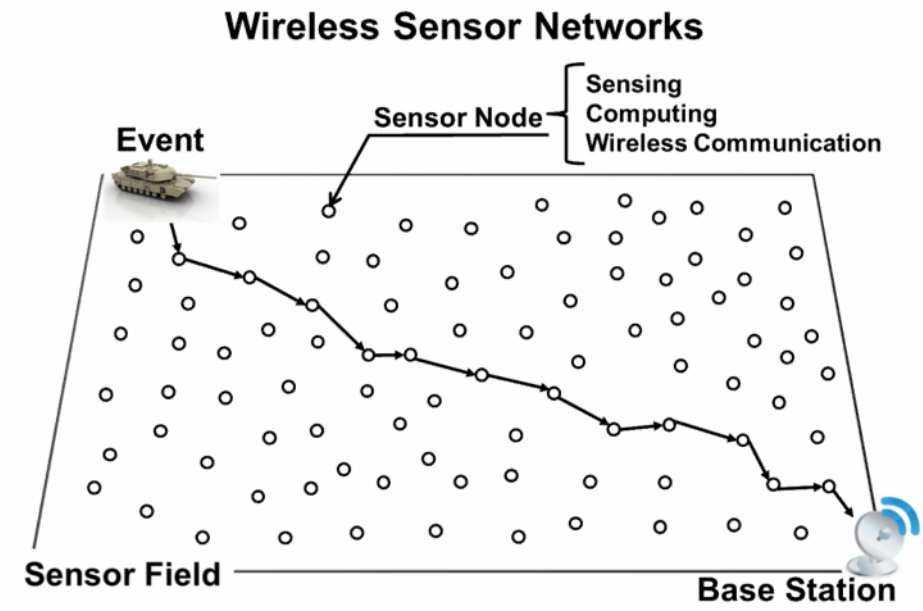

Figure1. Wireless Sensor Networks

2. BACKGROUND

2.1. False Report Injection Attack

Figure 2 shows briefly aFalse Report Injection Attack (FRIA).The adversary injects a false report to the compromised node. The false report has a non-existing event. That report wastefully consumes the energy of the forwarding nodes on the path. If the Base Station receives the report, it operates following the report. In the case of a false report, it causes confusion of the users, and uselessly consumes the energy of nodes.Sensor networks have limited resourcesof computational power, communication bandwidth, energy, and so on.If the energy is depleted, the node does not operate. That means the WSN is dead. The energy of the node is strongly related to the network

lifetime. To consume energy is to shorten the network lifetime.Yu et al. proposed a Dynamic En-route Filtering Scheme. DEF is a scheme that protectsfrom false report injection attack or service denial attack in WSNs.

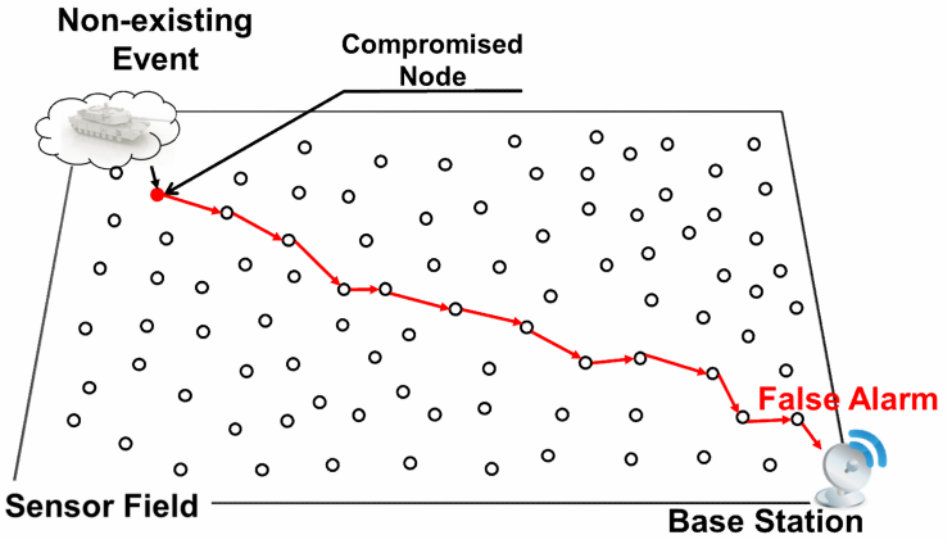

Figure2. False Report Injection Attack

2.2. Dynamic En-route Filtering Scheme

Yu et al. proposed a Dynamic En-route Filtering Scheme (DEF). DEF is scheme that protectsagainst a false report injection attack or service denial attack in WSNs.

DEF has been proposed by considering the changes of a dynamic sensor network, compared with other filtering schemes.Thus, it copes actively with the changing topology of a sensor network.In DEF, each node is composed as a unit of a cluster.Cluster based sensor networks do not duplicate data transmission [6]. So they prevent unnecessary energy consumption.

DEF verifies the fitness possibility of a report using a Message Authentication Code (MAC).This MAC is made up by an authentication key of each sensor node.The DEF is divided into three main phases,as inFigure 3.

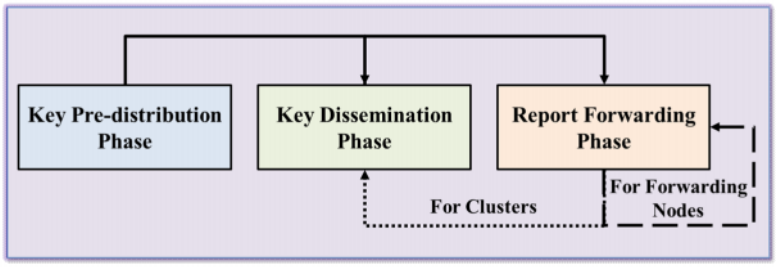

Figure3. Three phases of the DEF

First, it is composed of the key pre-distribution phase, and then periodically, the key dissemination phase and report forwarding phase.The Key pre-distribution phase is executed once, when the sensor is distributed in a network. This phase is divided into two phases in detail.First, each node is pre-loaded with each other's different seed key.They generate an authentication key-chain using a common hash function *h* from each seed key.M as the hash chain length, seed key for a given node v_i is to be $k_m^{v_i}$, and that authentication key is represented as inFigure 4.

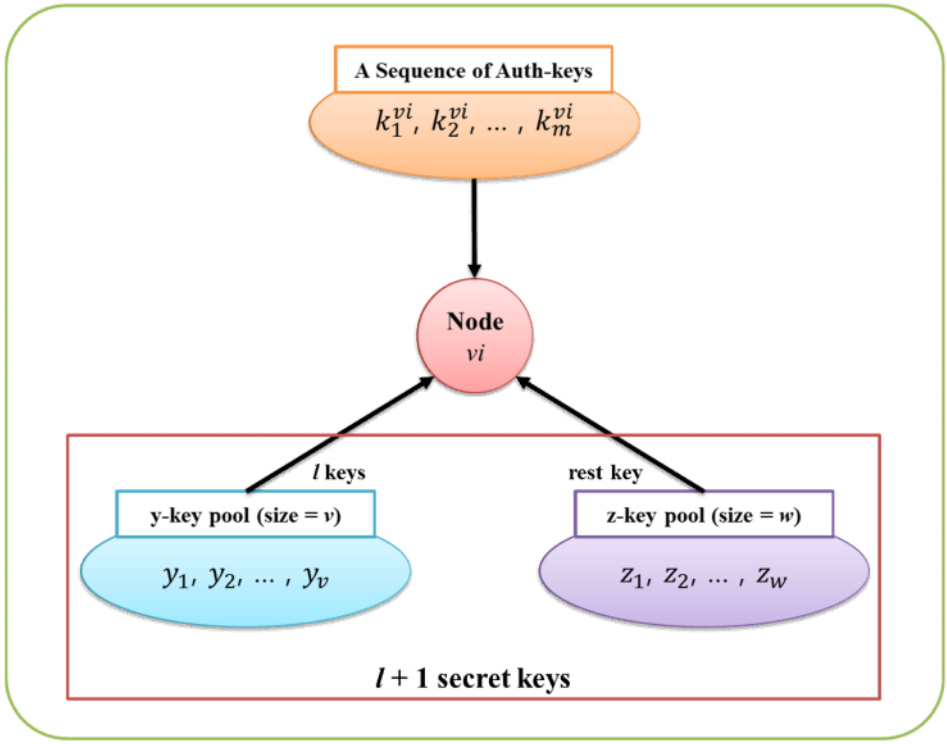

Figure4. Authentication Keys in a cluster

In the next key dissemination phase, the cluster-head discloses the authentication key of a node belonging to the cluster, after the report forwarding of each round.However, it would be vulnerable to an attack of report injection using a false authentication key or a fake cluster, through a compromised node.DEF forcibly disseminates the key for preparing for these attacks.That is,the cluster-head sends to a forwarding node, before the first authentication key of all the nodes' hash chain sends the report in the first round.The forwarding nodes verify that the report is authentic, compared with an authentication key that the cluster-head discloses using the disseminated key.The key dissemination is in case the forwarding node recognizes that the dissemination key has failed, especially when the network topology is very dynamic according to this, periodically executed disseminates.

In the case of the re-dissemination, the first unused authentication key in the key chain is disseminated.First,the unused authentication key is called a current authentication key of the node.The cluster-head selects q of the forwarding nodes of its neighbours'. These q nodes could be selected based on various formulas.For example, they could be selected based on the distance to the base station, quality of communication, available of energy, speed of energy consumption,

or a combination of all.A suitable formula could be selected according to the application layer.For this reason, a selection method is not specified in the existing DEF.

Finally, in the report forwarding phase, each node generates a report that contains the sensing information per round.The number of the report that is generated per round is fixed beforehand, when the node is distributed.All sensor nodes select a new authentication key in each round.The cluster-head forwards a collecting report per round to q of the selected node.The report is forwarded to the base station as hop-by-hop. The report is verified for its integrity using a disclosed key hop-by-hop in the forwarding node.Then, it informs the verified information to the next hop node. When the report is delivered or dropped, it performs the same procedure at every forwarding node.

2.3. Motivation

In DEF, the key dissemination phase is divided into four detailed phases.These are the process of generating an authentication message as nodes in a cluster, the process of aggregating an authentication message that the cluster-head receives from all the nodes in a cluster, and then the process of selecting the forwarding node for aggregating the authentication messages of surrounding neighbours, and finally the process of verifying that authentication message.

Here, the process of selecting the forwarding node for sending the aggregated authentication message is a part for determining the forwarding node as a fixed number of q.These processes selecting for the report can easily switch to other nodes, when a forwarding node of downstream is compromised.This key dissemination phase is re-executed whenever the topology of networks changes, and sends the new authentication key every time.In basic DEF, the cluster-head used is selected by the distance to the base station, quality of link, available energy, speed of energy consumption, or all of these toward the next hop forwarding nodes.However, we used a fuzzy rule-based system for more energy efficiency of next hop node selection [7]. Through this system, we will show that we could be both energy efficient and maintain the verification performance.

3. PROPOSED METHOD

3.1. Assumptions

In this paper, we assume that following factor.In this paper, we will assume that following factor. The entire routing path uses the shortest path routing. The first key is pre-distribution and the base station would be known the base station to hops, the transmission amount, and other information. Whenever the topology changes,the key dissemination phase is executed. Each node has a neighbour’s each node.

3.2. Overview

DEF determines the next hop forwarding nodes as a pre-defined factor. When this next hop forwarding node is determined, we select the next q forwarding nodes using an announced four factor at upper motivation.In the proposed method, we select the next q forwarding nodes by the distance from the target node to base station, current energy of the target node, and usage count for message transmission, using a fuzzy system.When selecting q forwarding nodes, it is more effective to ask “how many q?” We conclude by experimental means.By these means, we maintain a security of network and enhance more effective energy consumption.

3.3. Proposed Method

To determine the next-hop node is an important part for the balanced energy consumption of networks and early detectionof false reports. If a false report attack is infiltrated into the network, not only does a false alarm occur at the base station, but also it consumes the useless energy of nodes on the forwarding path. Due to this, the lifetime of an entire network can be shortened, and a malfunction can occur.

Our proposed methoduses three factors fordeterminingthe next forwarding nodes.Those are the number of neighbouring nodes, currentlyavailable energy, and usage count to the transmission message. This uses a fuzzy function for next forwarding nodes, which is more effective.A fuzzy function is applied at the node of a forwarding path from the cluster-head.The advantage of the fuzzy rule-based system can be used to approximate deduction.As an input factor of the fuzzy function, it represents that the number of neighbour node is “NN”, the currentlyavailable energy is “CE”, and finally the usage count of message transmission is “UC”.

NN is the number of neighbours of the candidate node. The many neighbours mean many candidate nodes. So we determine the NN to have many candidate nodes. CE would gradually decrease the energy, whenever a message transmission occurs, according to the formal formula. When the sensor node is first distributed, itscriterionis 100%.Finally, UC would gradually be increased one by one, when the first distribution is count 0.For these three factors, the result would be represented by an alphabet R.The fuzzy rule-based system would be represented as inFigure5,for the three input factors.

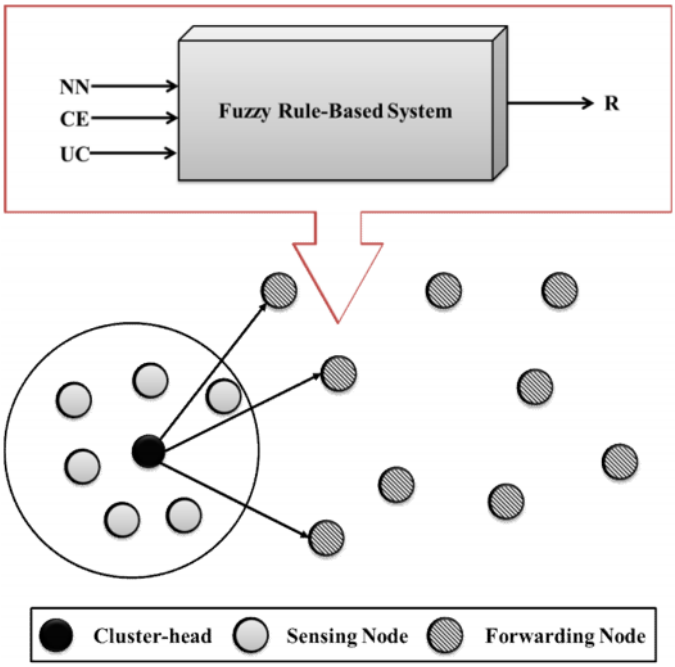

Figure5. Fuzzy Rule-based System

The fuzzy membership function would be represented as in the following Figure6for each factor.Three factors would be input as each divided in-to three parts.NN is Few, Adequate, Many

as you see, and CE is Low, Medium, High; finally UC is divided into Few, Sometimes, Many.The rules according to the fuzzy function would be the number of 27(=3x3x3x).

$$NN = \{F(Few), A(Adequate), M(Many)\}$$
$$CE = \{L(Low), M(Medium), H(High)\}$$
$$UC = \{F(Few), S(Sometimes), M(Many)\}$$
$$R = \{B(Bad), N(Normal), G(Good)\}$$

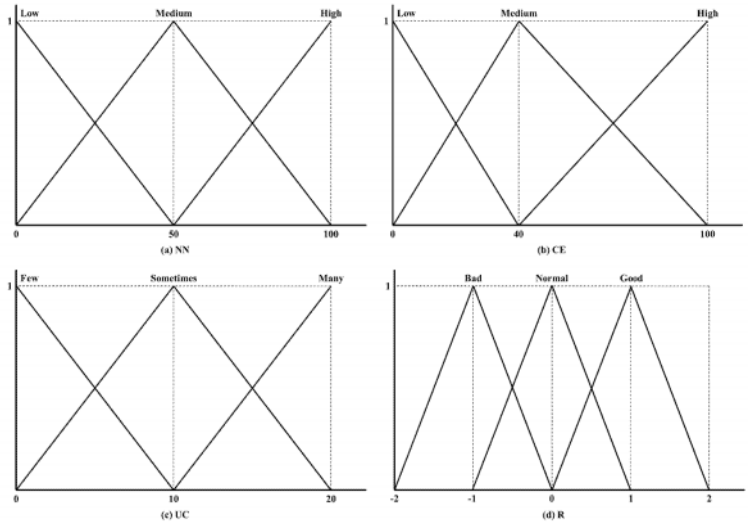

Figure6. Fuzzy membership function\

Table 1 is part of the rules of making the fuzzy rules.

Table 1. A part of the fuzzy rules

Rule No.	Input Factor			Result
	NN	CE	UC	
2	Few	Low	Few	Bad
7	Few	High	Sometimes	Normal
14	Adequate	Medium	Few	Normal
17	Adequate	High	Few	Good
20	Many	Low	Few	Normal
26	Many	High	Few	Good

For example, if NN is Adequate, CE is High and UC is Few, the result is Good. The forwarding nodes within a one hop from the cluster-header could be candidate nodes for the message transmission node.These candidate nodes would be selected as fixed q by the proposed fuzzy rule-based system in the upper column.

A generated message in each sensor node per each round would be forwarded to the base station as aggregating to the cluster-head through the fixed forwarding node of q.When the forwarding

node selects the next forwarding node, it could select the next forwarding node with the same method.The number of q could be fixed beforehand.However, if the number of transmission message is increased according to this q, then the energy consumption of the entire network is increasing. So, it's a very important part to select an appropriate q. We evaluate an appropriate number of q through an experiment.

4. EXPERIMENTAL RESULTS

In this paper, we will show the energy efficiency of the proposed method compared with the existing DEF, through experiment.The experiment would be processed based on the assumption of the proposed method, and assumes that all the sensor nodes had sent one of the messages.We fixed the sensor field size as 1000 x 1000(m^2) and the number of the distributed nodes are 500 sensors in the sensor field [8].

In this experiment, we assume that the attack generates a false report, and gradually increase the ratio of the false report among the whole reports.The result of the experiment is as in the following Figure7.

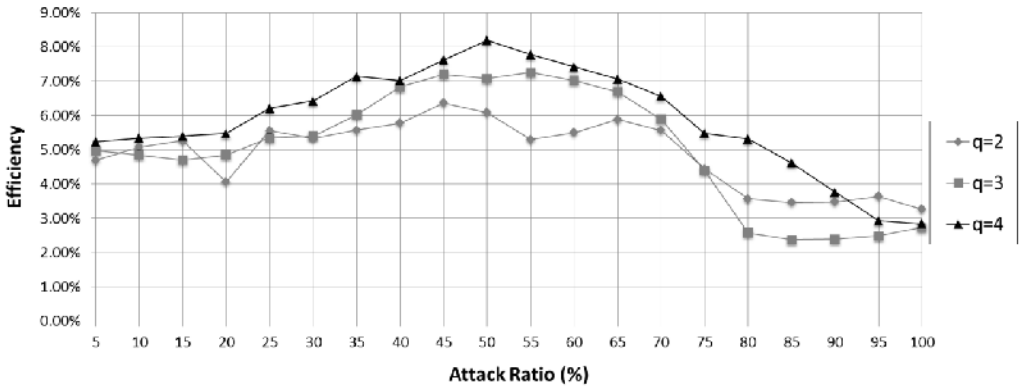

Figure7. Energy efficiency for each attack ratio

In Figure 7, we can see the difference of the energy efficiency according to the number of q. We can see the difference of energy efficiency according to gradually increasing the ratio of a false report in each number of q.If q=2, we show a lower 3.3% to upper 6.5% efficiency, and if q=2, a lower 2.4% to upper 7.3% efficiency.Then if q=4, this shows the minimum efficiency 2.8% to the maximum 8.2% efficiency.

The following Figure8 is a graph that represents the whole energy efficiency.It showsan increaseof energy efficiency, according to the increasing number of q.This represents that the proposed method would show more efficiency, according to an entire network use being more efficient.

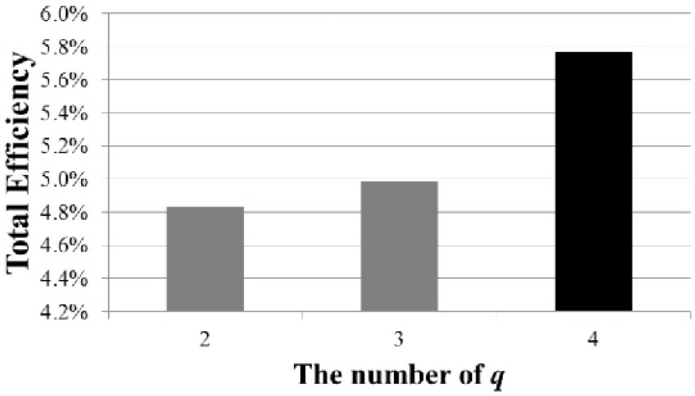

Figure8. Total efficiency against the number of q

If almost all reports are a false report(over 80%), the proposed method is hardly distinguished from the existing DEF.However, if the ratio of a false report is over 80%, granted that the problem of that the sensor field is impossible to use, we weigh up the real existing case that is 30% to 60% cases.Thus, the proposed method shows an efficiency of 5% to 8% compared with the existing DEF.

According to increasing the number of q, the energy efficiency is increased.Thus, that means that the more energy we consume, the more the proposed method shows energy efficiency.

5.CONCLUSIONS

In this paper, we used a fuzzy system for energy efficiency in the proposed DEF, to protect against a false report injection attack of WSNs.As a result, the energy efficiency is different according to q, but it generally shows the efficiency of a minimum 4.8% to maximum 5.8% and it shows a minimum 5.3% to maximum 8.2% efficiency to really using section of 30% to 60%.Thus, the proposed method means to show the more energy consumption, the more energy efficiency, compared with the existing DEF in this paper. In the future, we will expand that experiment, find an optimum number of q, and then show the energy efficiency according to that.

ACKNOWLEDGEMENTS

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (No. 2013R1A2A2A01013971)

REFERENCES

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “A Survey on Sensor Networks”, IEEE Communication Magazine, Vol. 40, Issue : 8, pp. 102-114, Aug. 2002.

[2] J. N. Al-Karaki and A. E. Kamal, “Routing techniques in wireless sensor networks: a survey”, IEEE Wireless Communication Magazine, Vol. 11, pp.6-28, 2004

[3] C. Karlof et al., “Secure Routing in Wireless Sensor Networks:Attacks and Countermeasures”, Elsevier’s Ad Hoc Networks Journal, Special Issue on Sensor Network Protocols and Applications, Vol. 1, No. 2-3, pp. 293-315, 2003.

[4] Z. Yu, Y. Guan, "A Dynamic En-route Filtering Scheme for Data Reporting in Wireless Sensor Networks", IEEE/ACM Transactions on Networking, Vol. 18, Issue:1, pp.150-163, 2009.
[5] Z. Yu and Y. Guan, "A Dynamic En-Route Scheme for Filtering False Data Injection in Wireless Sensor Networks", IEEE INFOCOM, PP. 1-12, Apr. 2006
[6] B. Karp and H.T. Kung, "GPSR: Greedy Perimeter Stateless Routing for Wireless Networks", in Proc. ACM MobiCom, pp. 243-254., 2000
[7] N. Serrano, H. Seraji, "Landing Site Selection using Fuzzy Rule-Based Reasoning", IEEE International Conference on Robotics and Automation 2007, pp. 4899-4904, Apr. 2007.
[8] F. Ye, H. Luo, S. Lu and L. Zhang, "Statical En-Route Filtering of Injected False Data in Sensor Networks", IEEE Journal on Selected Areas in Communications, Vol. 23, Issue:4, pp. 839-850, Apr. 2005

Authors

JaeKwonLeereceived hisB.S. degree in Computer Software Engineering from the Kumoh National Institute of Technology, Republic of Korea, in 2012. He is currently a Master student in the School of Information and Communication Engineering, Sungkyunkwan University, Republic of Korea. His research interests are in the areas of wireless sensor network, intelligent systems, modelling & simulation, and enterprise resource planning.

Tae Ho Cho received his Ph. D. degree in Electrical and Computer Engineering from the University of Arizona, USA, in 1993, and his B.S. and M.S. degrees in Electrical Engineering from Sungkyunkwan University, Republic of Korea, and the University of Alabaman, USA, respectively. He is currently a Professor in the School of Information and Communication Engineering, Sungkyunkwan University, Republic of Korea. His research interests are in the areas of wireless sensor network, intelligent systems, modelling & simulation, and enterprise resource planning.