International Journal of Electrical, Electronic and Communication Sciences
ISSN: 2517-9438
Vol:2, No:6, 2008

Low Energy Method for Data Delivery in Ubiquitous Network

Tae Kyung Kim, and Hee Suk Seo

***Abstract*—**Recent advances in wireless sensor networks have led to many routing methods designed for energy-efficiency in wireless sensor networks. Despite that many routing methods have been proposed in USN, a single routing method cannot be energy-efficient if the environment of the ubiquitous sensor network varies. We present the controlling network access to various hosts and the services they offer, rather than on securing them one by one with a network security model. When ubiquitous sensor networks are deployed in hostile environments, an adversary may compromise some sensor nodes and use them to inject false sensing reports. False reports can lead to not only false alarms but also the depletion of limited energy resource in battery powered networks. The interleaved hop-by-hop authentication scheme detects such false reports through interleaved authentication. This paper presents a LMDD (Low energy method for data delivery) algorithm that provides energy-efficiency by dynamically changing protocols installed at the sensor nodes. The algorithm changes protocols based on the output of the fuzzy logic which is the fitness level of the protocols for the environment.

***Keywords*—**Data delivery, routing, simulation.

I. Introduction

WSN (Wireless sensor network) is composed of the small-scale sensor nodes which have abilities of perception, calculation, and wireless communication. And each sensor node is composed of sensor, processor, memory, transceiver, location measurement system, and battery. Sensor node not only collects data through the perception and transmit it but also performs routing function which transmits received data to another node. These sensor nodes scattered in the center field where they are generally arranged. Each sensor node transmits the perceived data to BS (Base Station) outside. BS helps to approach the data which collected by user, connecting the sensor network with existing communication infra like the Internet. Recent advances in micro-electro-mechanical systems technology, wireless communications and digital electronics have enabled the development of low-cost, low-power, and multi-functional sensor nodes [1]. These nodes, which consist of sensing, data processing, and communicating components, further leverage the concept of sensor networks [2], in which a large number of sensor nodes collaborate to monitor certain environment [3]. Sensor networks are expected to interact with the physical world at an unprecedented level to enable various new applications [4]. In many applications sensor nodes are deployed in open environments, and hence are vulnerable to physical attacks, potentially compromising the node's cryptographic keys [5]. False sensing reports can be injected through compromised nodes, which can lead to not only false alarms but also the depletion of limited energy resource in battery powered networks [6].

H. S. Seo is with the Korea University of Technology and Education, Byungcheon, Chungnam 330-708 Korea (corresponding author to provide phone: +82-41-1495; fax: +82-41-1462; e-mail: histone@kut.ac.kr).

T. K. Kim is with the Seoul Theological University, Bucheon-City, Kyonggi 422-742 Korea (e-mail: tkkim@ stu.ac.kr).

II. Background

A. Direct Diffusion

Policy Directed Diffusion [7] is the data-centric routing protocol, based on query of BS. Inquiry in Directed Diffusion is displayed as interest composed of a pair of property and value [8]. Such interest is regularly flooding into all over sensor network from BS; a gradient will be set up for sensor nodes to transfer data to BS. After the setting of gradient, a multi-path routing is created between BS and sensor node, data sensed by sensor node is transferred to BS through it. And plus one or a number of paths among the multi-path routing will be enhanced by BS and data will be transferred through the enhanced paths, and this decreases the consumption of the energy of sensor network preventing unnecessary flooding. Design of Directed Diffusion can be altered or modified to needs, is adaptive for query-driven sensor network but also adaptable for even-driven sensor network [9,10].

B. DEVS and SES

The DEVS formalism is a theoretically well-grounded means of expressing modular discrete event simulation models developed by Zeigler [11,12]. A DEVS is a structure:

$$M = < X , S , Y , \delta \text{ int} , \delta \text{ ext} , \lambda , ta >$$

Where X : the set of input event types,

S : the sequential state set,

Y : the set of external event types generated as output,

δ int : $S \rightarrow S$, the internal transition function,

δ ext : $Q \times X \rightarrow S$, the external transition function,

$$Q = \{(s,e) \mid s \in S, 0 \leq e \leq ta(s)\}$$

λ : $S \rightarrow Y$, the output function,

ta : $S \rightarrow R+0, \infty$, the time advanced function,

$R+0, \infty$ is a real number set except a negative number.

X means the set of events that occur outside the system. Y means the set of output variables. S means the cross product of definition areas of state variables and s ($s \in S$) means the sequential snap shot of system according to time progress. ta(s) is defined as the time allowed to be at the state s unless system doesn't get external events. δ int is defined as the function that explains the change of the state of model according to time progress when there are no external events. δ ext is defined as the function that represents the change of the state of model by the events occurred in the outside of the system. λ is defined as the output of the system in the state s. The DEVS environment supports building models in a hierarchical and modular manner, in which the term "modular" means the description of a model in such a way that is has recognized input and output ports through which all interaction with the external world is mediated. This property enables hierarchical construction of models so that the complex network security models can be easily developed.

The SES (System Entity Structure) [13] directs the synthesis of models from components in the model base. The SES is a knowledge representation scheme that combines the decomposition, taxonomic, and coupling relationships.

The entities of the SES refer to conceptual components of reality for which models may reside in the model base. Also associated with entities are slots for attribute knowledge representation. An entity may have several aspects, each denoting a representation. An entity may also have several specializations, each representing a classification of the possible variants of the entity.

C. Fuzzy Logic

Fuzzy if-then rules have been applied to many disciplines such as control systems decision making, pattern recognition, and system modeling. Fuzzy if-then rules also play a critical role in industrial applications ranging from consumer products, robotics, manufacturing, process control, medical imaging to financial trading. Fuzzy rule-based inference can be understood from several viewpoints. Conceptually it can be understood using the metaphor of drawing a conclusion using a panel of experts. Mathematically, it can be viewed as an interpolation scheme. Formally, it is a generalization of a logic inference called modus ponens [14].

The important feature of a fuzzy variable is its membership. Zadeh extended the notion of binary membership to accommodate various "degree of membership" on the real continuous interval. The endpoints of 0 and 1 conform to no membership and full membership, respectively, This is analogous to the indicator function for precise variables. Linguistic variables are variables whose values are not numbers but words, clauses or symbols in a natural or artificial language. For example, price is a linguistic variable in the second instance of the above. Its value may be cheap, reasonable, expensive or some other phrase which is composed of fundamental atomic terms and linguistic hedges. For instance, very cheap, slightly expensive, and so on, illustrate linguistic hedges.

The values of a linguistic variable are fuzzy values. Any linguistic variable has a finite or infinite set of terms (values) in which some are fundamental atomic terms and others are compound terms. Generally, the meaning of a compound can be expressed by combining atomic terms with some hedges.

III. LMDD Model

Various compositions are possible for wireless sensor network according to application. Assumption about wireless sensor network for LMDD algorithm is as follows.

- All node uses Radio model same as LEACH, TEEN

In this algorithm, BS uses Amplifier when it sends broad casting messages to sensor node. Using the Radio Model, BS could distribute protocol code to sensor node or transmit it directly to a long way at one time. Consequently sensor node will not be routed and it is also possible to reduce the energy consuming a lot. This study sets the range of electric wave of BS and Sensor node to be 300m.

- BS can continuously receive the power supply

BS collects information from the sensor node, and sends it to task manage node through the Internet in wireless sensor network [1,3]. BS needs continuous power supply to accomplish a fuzzy operation, and broadcasting protocol code and switch messages into the sensor node.

- All nodes know the general location of oneself

In order to reduce an expense, It can be used either low power GPS (Global Positioning System) or Triangulation [15] which is able to grasp general locations of nodes, affixing GPS to only a few node.

- All nodes will be able to load any routing protocol with dynamic

For this algorithm, all sensor nodes should load routing protocol with dynamic. One of the ways is to use Active networking technologies [16]. This technologies have not only routing function also calculation function. If referenced Active networking technologies, it would be possible to embody the sensor node loading routing protocol as sensor node has also these functions.

LMDD algorithm basically consists of four steps, Initialization, Protocol selection, direct code distribution, and Direct protocol switching. In an exceptional situation, Request-response code distribution, and Local protocol switching are added.

The task administration node which the user manages transmits several suitable routing protocol codes, hash codes, Parameters, fuzzy membership function, fuzzy rules, etc to BS through Internet. BS initiates the work with data received from the task administration node. Hash code about each routing protocol can be created by hash algorithm-MD5,

RIPEMD-160. This study uses a hash code as a protocol switching message, since hash code is only thing to be identified about each routing protocol. If there is environmental change in network, such as additional arrangement or arrangement scope of node, while accomplishing the task, the task administration node transmits new parameters in this step. The transmission of routing protocol code such as TEEN and Directed Diffusion, hash code, parameters, fuzzy membership function, and fuzzy rules to BS. Parameters.

When BS receives parameters from the task administration node, FBPS that is inside of BS selects the suitable degree to each protocol. And the biggest suitable degree is selected among the suitable degrees. If there are more than two, all are selected. Fig. 1 shows the example that FBPS received the parameters (Number of nodes = 300, Deployed Area = 10000 ㎡) and select TEEN as the most efficient routing protocol.

BS confirms the existence of hash code in record of cache routing protocol selected by FBPS and exams whether BS has distributed the selected routing protocol to the sensor node or not. If the routing protocol was already distributed, go to the next step, direct protocol switching, otherwise BS broadcasts it to the all sensor node which is in the radio and then stores the hash code of corresponding protocol in protocol distribution record. The sensor node received the routing protocol code from BS initiates routing, loading additional protocol routing.

BS compares the hash code of protocol routing by FBPS with those stored in cache. If it accords each other, using protocol and selected routing protocol are in accord, BS does not accomplish a protocol switching. Otherwise BS broadcasts hash code and stores it to the cache. The sensor node received hash code from BS replaces currently using routing protocol with a corresponding protocol and accomplishes the routing. BS broadcasts hash code of TEEN which is selected in protocol selection step to sensor node. In this step, it reduces the energy consumption, using hash code which is small size instead of protocol code as a protocol switching message. On the other side, the sensor node which is rearranged or out of radio scope of BS (300m) cannot receive either routing protocol or switching messages. To solve this problem, additional steps are necessary.

The sensor node perceived events or received data from neighbor node investigates whether routing protocol is inside of cache or not. If there is no routing protocol in the node, it sends broadcast requesting message to the neighbor node. And the neighbor node which received request massage transmits to currently using requested node.

FBPS selects the routing protocol for the most efficient energy as a decision-making system based on fuzzy inference system under the current network situation. FBPS has "Number of nodes" and "Deployed Area" as input variables, and "Fitness" as output variable. Input variables are the fuzzy set which expresses the components of the network environment; "Number of nodes" means the number of the sensor node arranged in sensor field, and "Deployed Area" is the area of the square territory sensor network is arranged. "Fitness", the output variable, shows how much routing protocol is suitable to current situation.

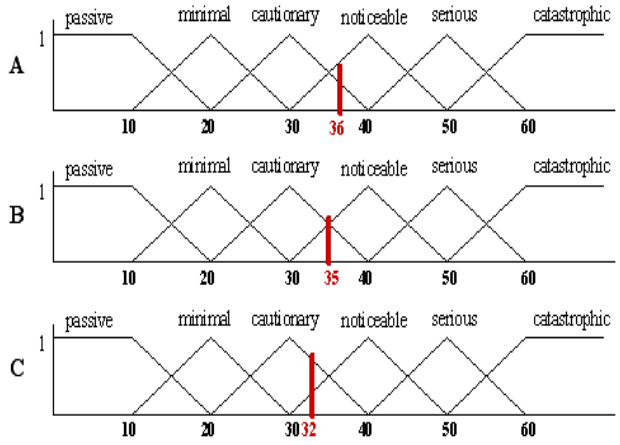

Fig. 1 Membership function of each agent

Directed Diffusion and TEEN are selected as the switching candidacy protocol in this study. Although the number of sensor node increases, the energy consumption in entire network does not increase a lot, because TEEN is a single hop routing protocol. The other side, as Directed Diffusion is a process of flooding interest, the more sensor node number increases, the more entire energy consumes in entire network.

BS could stay farer than radio scope of cluster head, when sensor node arranged in a broad area, since cluster head in TEEN is selected randomly. Therefore, when BS could not receive all data from cluster head, it means the waste of energy. Consequently the energy efficiency falls down, when TEEN is arranged in a board area. The other side, Directed Diffusion which is a hop routing way can transmit data to BS without above problem if arranged in a board area.

IV. Simulation

To evaluate the efficiency of proposed algorithm, our research team organized a simulation environment, using simulator, DEVS Object C, developed by ourselves. The first energy of sensor node was set as 1J, and the scope of radio was from 40m for Directed Diffusion to 0-300m for TEEN. BS was set (0, 0), and sensor node was distributed inside of square arrangement area randomly. Events occurred every 20 seconds in the area where sensor nodes are. The simulation was accomplished for 1000 seconds. In the beginning, 100 nodes were arranged in 10000㎡ (100m x 100m), after that for 300 seconds, 200 more sensor nodes were added, and for the last 600 seconds, arrangement area was extended to 90000㎡ (300m x 300m) and 200 nodes were additionally arranged.

In this study, in order to evaluate energy efficiency when using a single routing protocol only and when using LMDD algorithm, the average energy consumption was established as performance index. The average energy consumption is a value

calculated by dividing energy consumed by each sensor node comprising a sensor network with an unduplicated event number received by BS. In other words, the average energy consumption means the average energy value consumed by each node for transferring one event to BS. Therefore, as this value becomes smaller, an event can be delivered to BS with smaller energy.

V. Conclusion

In this study, LMDD algorithm was proposed as a way of ensuring energy efficiency of a sensor node in a dynamic network environment, and it was proven that when algorithm proposed as a result of performing simulation is used is more energy efficient rather than when a single routing protocol was used. Also, according to an environment where a sensor node is placed, the proposed algorithm also includes technique of dynamically positioning a routing protocol on a sensor node so that the algorithm may select and use other appropriate routing protocols. Moreover, in this study, only "number of node" and "area of a domain where a sensor node was positioned" were considered as fuzzy input variables, however, in order to more enhance energy efficiency, a node failure rate and a packet size may be also added as input variables according to situations.

Whenever a network environment changes, in LMDD algorithm, FBPS reduces overhead because of an exchange message transfer by selecting energy efficient protocol and controlling the transfer of protocol code / switch message. However, energy efficiency may be lowered due to transfer of an exchange message in an environment where there should be frequent protocol exchanges, then an operator needs to determine whether to use this algorithm after considering energy efficiency in a situation concerned. In addition, a sensor node needs to load diverse protocols in LMDD algorithm. A sensor node may have various performances according to the purpose of use. Then, for the proposed algorithm, a sensor node needs to have a better performance than general sensor nodes. Accordingly, in order to apply LMDD algorithm to an actual situation, it needs to determine the appropriateness of the use of the algorithm given the number of candidate routing protocols applicable and the price of a sensor node with sufficient memory as to contain the protocols.

References

[1] Akyildiz, I.F., Weilian Su, Sankarasubramaniam, Y., Cayirci, E., "A survey on sensor networks," IEEE Communications Magazine, Vol. 40, pp.102-114, Aug. 2002.
[2] Qiangfeng Jiang, Manivannan, D., "Routing protocols for sensor networks," Consumer Communications and Networking Conference, 2004, First IEEE, pp.93-98, Jan. 2004.
[3] Al-Karaki, J.N., Kamal, A.E., "Routing techniques in wireless sensor networks: a survey, " Wireless Communications, IEEE, Vol. 11, Issue: 6, pp.6-28, Dec. 2004.
[4] K. Akkaya, M. Younis., "A Survey on Routing Protocols for Wireless Sensor Networks," Ad Hoc Networks, Elsevier Science, To appear.
[5] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless sensor networks," in the Proceeding of the Hawaii International Conference System Sciences, Hawaii, Jan. 2000.
[6] Tennenhouse, D.L., Smith, J.M., Sincoskie, W.D., Wetherall, D.J., Minden, G.J., "A survey of active network research," Communications Magazine, IEEE, Vol. 35 , Issue: 1, pp.80-86, Jan. 1997.
[7] James P.G. Sterbenz, Bernhard Plattner, "Introduction to Active Networks Tutorial," May, 2003.
[8] K. Psounis, "Active networks: Applications, security, safety, and architectures," IEEE Commun. Surveys, vol. 2, no. 1, 1999.
[9] A. Manjeshwar, D. Agrawal, "TEEN: a Routing Protocol for Enhanced Efficiency in Wireless Sensor Networks," in International Proc. of the 15th Parallel and Distributed Processing Symposium, pp.2009-2015, 2001.
[10] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A Survey on Sensor Networks", IEEE Commun. Mag., vol.40, no.8, pp.102-114, Aug. 2002.
[11] K. Akkaya and M. Younis, "A Survey on Routing Protocols for Wireless Sensor Networks", Ad hoc Netw., vol.3, no.3, pp.325-349, May 2005.
[12] S.H. Chi and T.H. Cho, "Fuzzy Logic based Propagation Limiting Method for Message Routing in Wireless Sensor Networks", Lect. Notes Comput. Sc., vol.3983, pp.58-64, May 2006.
[13] F. Ye, H. Luo, and S. Lu, "Statistical En-Route Filtering of Injected False Data in Sensor Networks", IEEE J. Sel. Area Comm., vol.23, no.4, pp.839-850, Apr. 2005.
[14] B. Przydatek, D. Song, and A. Perrig, "SIA: Secure Information Aggregation in Sensor Networks", Proc. of SenSys, pp.255-265, Nov. 2003.
[15] H. Yang ans S. Lu, "Commutative Cipher Based En-Route Filtering in Wireless Sensor Networks", Proc. of VTC, pp.1223-1227, Oct. 2003.
[16] W. Zhang and G. Cao, "Group Rekeying for Filtering False Data in Sensor Networks: A Predistribution and Local Collaboration-based Approach", Proc. of INFOCOM, pp.503-514, Mar. 2005.