CONTROL SCHEME OF THE NEIGHBOUR INFORMATION OF FEEDBACK MESSAGE BASED ON NEIGHBOURHOOD DENSITY IN INSENS

Ji Won Kim and Tae Ho Cho

College of Information and Communication Engineering, Sungkyunkwan University,
Suwon 440-774, Korea
jwonkim@ece.skku.ac.kr tacho@ece.skku.ac.kr

ABSTRACT

An INSENS protocol is proposed to construct secure Wireless Sensor Networks (WSNs) that prevent attacks aimed at the network layer of WSNs. To achieve these objectives, all nodes which compose the network, send the feedback message to the base station. The feedback message contains the information of all neighbourhood nodes of a sender node. Therefore, if it owns many neighbour nodes within its communication range, then this node sends many feedback messages. This case arouses excessive energy consumption of each node in the sensor network. To solve this problem, we propose a control scheme of the neighbour Information of the feedback message based on the neighbourhood density. To compute the neighbourhood density, we add a new phase that exchanges the count of the neighbouring nodes of each node among the adjacent nodes. We insert this phase between the route request phase and the route feedback phase for improving INSENS. Consequently, all the sensor nodes send a different type of feedback messages by computing neighbourhood density. Through simulation, the proposed method show more efficient energy consumption compared to the original INSENS.

KEYWORDS

WSN, INSENS, Feedback message, neighbourhood density

1. INTRODUCTION

Small sensor nodes enable various functions due to the advancement in the technology of micro-electro-mechanical-system (MEMS). For example, there are wireless communications, data processing, and so on. Wireless sensor networks (WSNs) have appeared with the transmission of data between the two senor nodes based on the wireless network. WSN has numerous sensor nodes and a base station (BS) in a sensor field [1-2]. A sensor node owns limited resources namely energy, a computation module, and data storage. The sensor nodes are deployed in a hostile and dangerous environment such as a battlefield. Due to these elements, an intruder easily compromises the sensor nodes in the network, even though they have many advantages.

Numerous attacks are generated on whole layers of the WSN. In these attacks, the objective of the network layer attack is the forgery of the routing information or blocking the data communication. Wormhole, Sybil, selective forwarding, sinkhole, hello-flood attacks are the typical examples. These are performed by the compromised original node or the newly injected node [3].

Intrusion-tolerant routing protocol for wireless Sensor NetworkS (INSENS) is proposed for the prevention of these network layer attacks in the sensor network [4]. INSENS blocks the network

DOI : 10.5121/ijasuc.2012.3202

layer attacks from Sybil or wormhole. Moreover, if the malicious node existed then, it guarantees a secure data communication through a routing path. In the process of an INSENS protocol, each node transmits a feedback message to a BS in order to notify the information of entire network topology. BS computes the routing table of each node based on this topology information. Therefore the feedback message includes the information of all the neighbour nodes. If the feedback message increases by neighbour nodes then, it should separate to send pieces of packet as the size of the packet is limited. In this result, when INSENS constructs the routing paths in the sensor network, the excessive energy consumption is caused due to the communication overhead between the nodes.

In this paper, we propose a control scheme of the neighbour Information of a feedback message based on the neighbourhood density. In the proposed method, we use different feedback message according to the neighbourhood density of each node. For this scheme, a new process is inserted that exchanges the neighbour nodes count with each other adjacent nodes between the rout request and the route feedback phase of INSENS. Each node computes its own degree of neighbourhood density by using these neighbour node counts. Further, they send different feedback messages as a degree of the neighbourhood density to the BS.

The remainder of this paper is organized as follows: Section 2 briefly describes the INSENS as the general background. Section 3 introduces our proposed method, and Section 4 presents the simulation results. Finally, we discuss the conclusion in Section 5.

2. Background: INSENS

2.1. Objective

In INSENS, first objective is to block the network layer attacks like Sybil or wormhole. Second objective is to guarantee a secure data communication under circumstance of malicious nodes' existence. In order to achieve these objectives, it applies OHC (One-way Hash Chain number), nested MAC [5], and fallback path.

2.2. Operation process

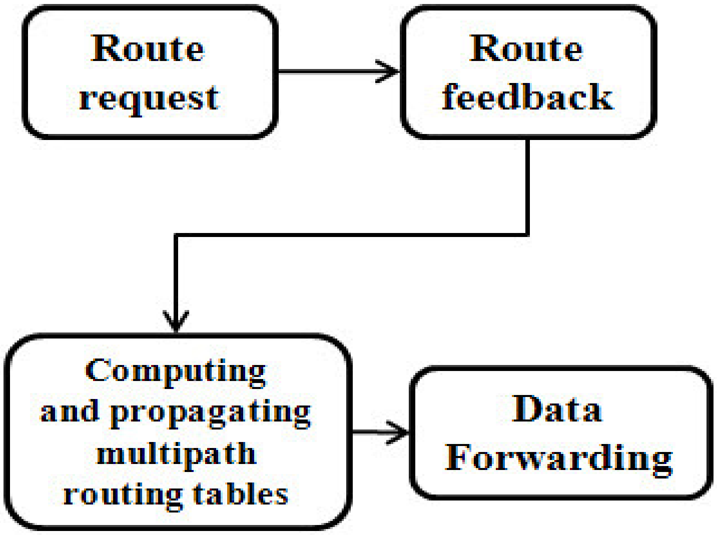


Figure 1. One cycle of operation process of INSENS

Figure 1. shows that INSENS consists of Route request, Route feedback, Computing and propagating multipath routing tables, and Data forwarding phase. In the route request phase, a rout request message is initially forwarded from the BS. The format of this message is

REQ || BS || OHC || MAC (K_{bs}, REQ || BS || OHC)

Where REQ is the message type, BS means the ID of the BS, OHC is a one-way hash chain sequence number. OHC prevents the reuse of the REQ messages. After receiving the route request message for the first, each node re-broadcasts the modified route request message to its neighbors within a possible range of its transmission. The format of the modified request message is

REQ || ID_x || OHC || MAC (K_x, ID_x || OHC || MAC_{parent})

Each node establishes its neighbours set based on the received route request message, and then it selects the parent node as the first message arrived. Parent node is the first received REQ message sending node. In this message, MAC is generated through the MAC of a parent as the REQ message is modified. This is called as a nested MAC. That is, Sybil and wormhole attacks are prevented through OHC and nested MAC as the intruder cannot freely insert a new node.

In the route feedback phase, the sensor nodes start this after waiting for the phase of the route request for a while. The format of a feedback message is

FDBK || ID_x || E (K_{xe}, NBR_x) || MAC (K_{xm}, OHC || FDBK || ID_x || E (K_{xe}, NBR_x))

Each node x forwards a feedback message which includes all the information of its neighbours, from NBR_x to BS. An NBR_x contains IDs of its neighbours and MAC.

In computing and propagating multipath routing tables phase, the BS constructs a topology of the network after verification of the information of the NBR_x. It guarantees the full topology completion of the network as every node transmits all the information of its neighbours. The BS constructs the shortest path using Dijkstra's algorithm based on the completed topology, and it establishes a primary path. The fallback path is computed as follows.

Table 1. set of exception nodes

N_1	the set of nodes belonging to the primary path
N_2	the set of nodes belonging to N1 and any neighbour nodes of the nodes in N1
N_3	the set of nodes belonging to N2 and any neighbour nodes of the nodes in N2

In order to establish a fallback path, every node computes the shortest path from its source node to the BS without a set N3. If the fallback path is undiscovered then, the former process is repeated by using a set N2 and N1.

In the data forwarding phase, the BS delivers the information to each node after the computation of its forwarding table. Each node maintains the forwarding table that has several entries. Each entry is a 3-tuple.

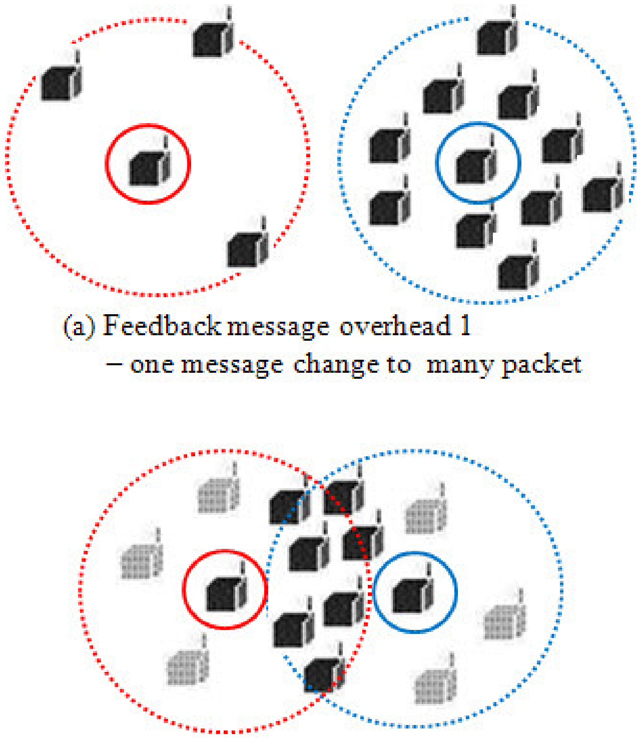
< Destination, Source, Immediate sender >

For example, a route from node S to D: S→N1→N2→N3→D, the forwarding table of N1 will contain an entry <D, S, S>, the forwarding table of N2 will contain an entry <D, S, N1>, and the forwarding table of N3 will contain an entry <D, S, N2>. A node searches for a matching entry in its forwarding table. If it finds a match then, it forwards the data packet.

3. PROPOSED METHOD

3.1. Motivation

In the INSENS protocol, as all of the feedback messages are not guaranteed to arrive at the BS, feedback messages include all of the neighbourhood information of each node. But the size of a feedback message is limited. So, if a node has many neighbours within a communication region then, many packets occurs for the transmission of a single feedback message. In this case, communications of the node increases between the node and another node. The node conserves excessive energy. In addition, duplicate information of the neighbouring nodes is forwarded to the BS in a region where the nodes are densely gathered.



(a) Feedback message overhead 1
– one message change to many packet

(b) Feedback message overhead 2
– messages included duplicate information

Figure 2. Example of feedback message overhead

3.2. Overall process

The proposed method is composed of five phases: a route request, Exchange of the neighbour node count, route feedback, computing and propagating multipath routing tables phase, and data forwarding phase. Newly added or modified phases compared with INSENS are the exchange of the neighbour node count phase and route feedback phase. In exchange of the neighbour node count phase, all nodes exchange the neighbour node count with other adjacent nodes to compute the neighbourhood density. This phase is newly added to INSENS. In the route feedback phase, all nodes send the different type of the feedback message according to the computed density. This phase is modified when compared with INSENS. Figure 3. shows the overall process of the proposed method.

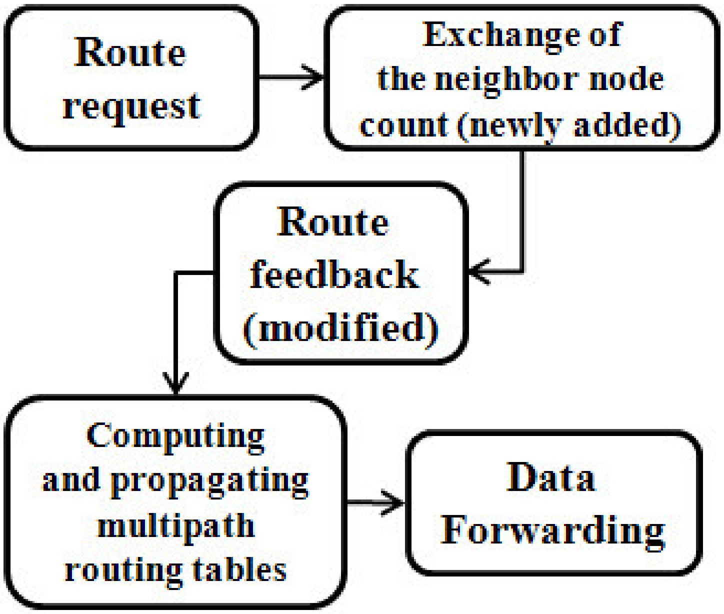

Route request
Exchange of the neighbor node count (newly added)
Route feedback (modified)
Computing and propagating multipath routing tables
Data Forwarding

Figure 3. Overall process of proposed method

3.3. Exchange of the neighbour node count phase

In the original INSENS, each node know that a number of neighbour nodes that exist around itself when the route request phase is finished. That is, the number of its neighbours is accurately unrecognized before each node completely finishes the route request phases. Therefore, the network needs a phase of our proposed method that exchanges the number of its neighbours to recognize the number of the neighbours. They broadcast the number of its neighbours. As a result, a node forwards the number to its surrounding nodes, and they receive the number of its neighbours.

3.4. Neighbourhood density computation and limited feedback message transmission

The neighbourhood density of each node is computed by the following Eq.1.

$$D = (s - m_1) + (s - m_2) + \dots + (s - m_n) \qquad (1)$$

D is the neighbourhood density. *S* is the neighbour node count of itself that compute the neighbourhood density. m_n is the neighbour node count of the nth adjacency node. If the computed result *D* is smaller than specific criteria value then, this node becomes the complete feedback node (CF node). CF node sends a feedback message that includes all information of the neighbour nodes. Otherwise, if the computed result *D* is bigger than the specific criteria value then, this node becomes the incomplete feedback node (IF node). IF node sends feedback messages that include only the information of the parent node. Many nodes are selected as IF node in region that node is densely gathered. Otherwise, CF node is selected in region that node is sparsely gathered. As a result, data amount of feedback messages is can be controlled by using the proposed method. Moreover, it is also possible to achieve efficient energy consumption.

4. SIMULATION RESULT

Simulation environment is established like following condition to compare with INSENS and proposed method. Sensor filed is a virtual environment area about 1km2. The number of deployed sensor nodes is 500, 750, 1000. Maximum transmission distance is 100m [6]. Energy consumption for message sending, receiving, and creation is about 16.25 μJ, 12.5 μJ, and 7.5 μJ respectively [7]. Criteria value of the IF and CF nodes' selection is 0. One round implies that the overall process of INSENS and proposed method performs one time.

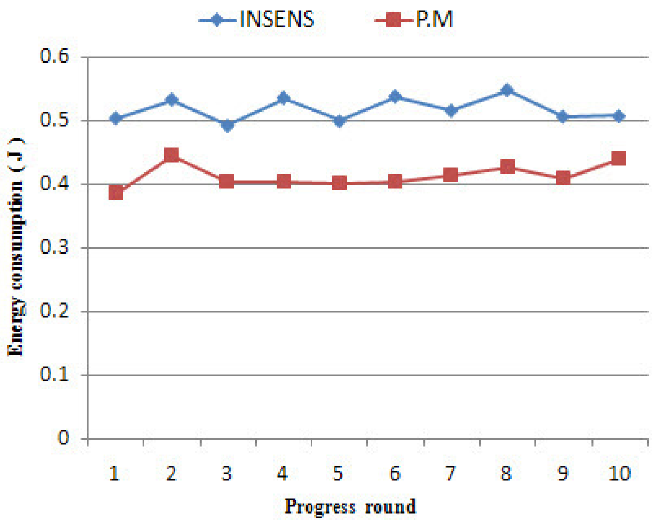


Figure 4. Comparison of energy consumption (500 nodes)

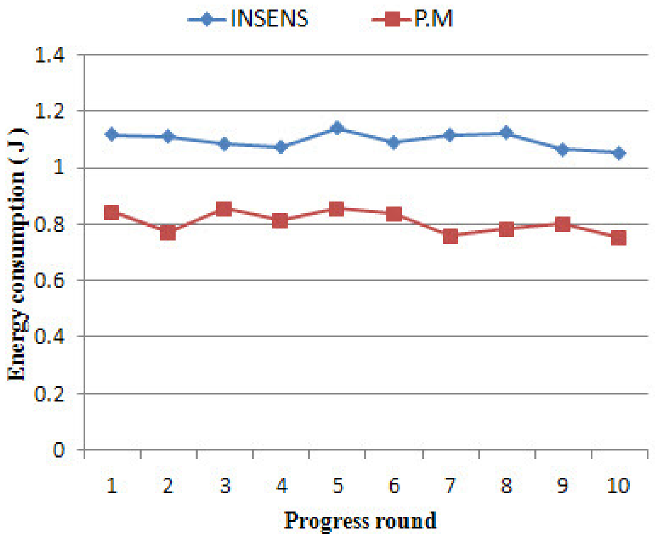


Figure 5. Comparison of energy consumption (750 nodes)

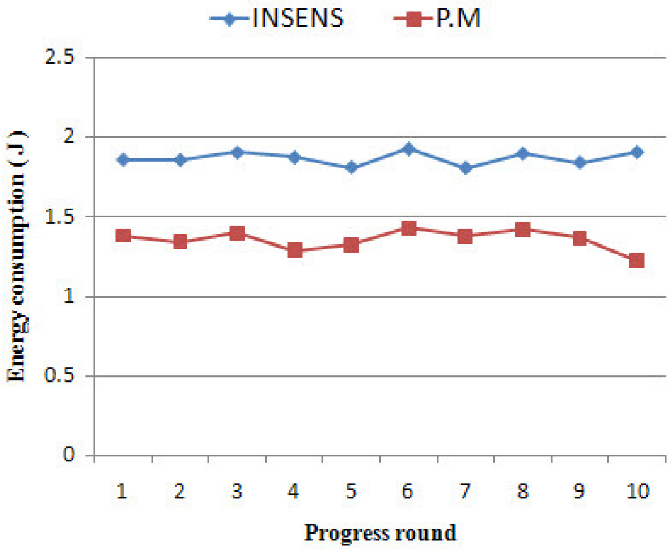


Figure 6. Comparison of energy consumption (1000 nodes)

Figure 4, 5, 6 shows energy consumption of INSENS and proposed method in situation that deployed 500, 750, 1000 sensor nodes.

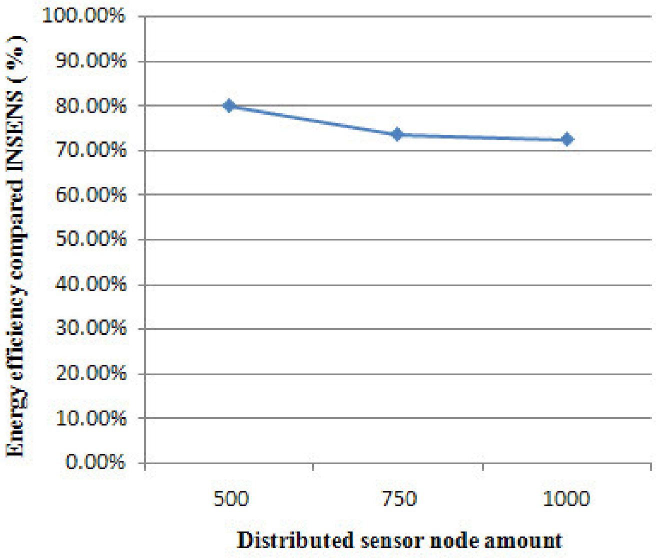


Figure 7. Average energy efficiency compared INSENS

Figure 7 shows the average energy efficiency compared to INSENS. In all situations, energy consumption of the proposed method is more decreased about 20%~30%. In the proposed method, the size of a feedback message is controlled by the neighbourhood density. Therefore, the communication usage among the nodes decreases when compared to the original INSENS. In this result, the total energy consumption is decreased.

5. CONCLUSION

In this paper, we propose the control scheme of the neighbour information of the feedback message based on neighbourhood density. In the proposed method, the exchange of the neighbour node count phase is added for the computation of the neighbourhood density. The amount of neighbour node in the feedback message is controlled by the computed neighbourhood density. Simulation result shows that the energy consumption is decreased against original INSENS.

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. 2011-0004955).

REFERENCES

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensor networks: a survey”, Computer Networks, Volume 38, Issue 4, March 2002, 393-422

[2] J.N. Al-Karaki, A.E. Kamal, "Routing techniques in wireless sensor networks: a survey", Wireless Communications, IEEE , vol.11, no.6, Dec. 2004, 6-28

[3] Chris Karlof, and David Wagner, Secure routing in wireless sensor networks: attacks and countermeasures, Ad Hoc Networks, Volume 1, Issues 2-3, September 2003, 293-315

[4] Jing Deng, Richard Han, and Shivakant Mishra, INSENS: Intrusion-tolerant routing for wireless sensor networks, Computer Communications, Volume 29, Issue 2, January 2006, 216-230,

[5] Mihir Bellare, Ran Canetti, Hugo Krawczyk, “Keying Hash Functions for Message Authentication”, Advances in Cryptology — CRYPTO ’96, Lecture Notes in Computer Science, LNCS 1109, 1996, 1-15

[6] Xbow sensor networks, http://www.xbow.com

[7] Heinzelman, W.R.; Chandrakasan, A.; Balakrishnan, H., "Energy-efficient communication protocol for wireless microsensor networks," System Sciences, 2000. Proceedings of the 33rd Annual Hawaii International Conference on , vol., no., pp. 10 pp. vol.2, 4-7 Jan. 2000

Authors

Ji Won Kim received his B.S. degree in Computer Engineering from Sungkyunkwan University in 2010. He is now a master’s student in the School of Information and Communication Engineering at Sungkyunkwan University. His research interests include wireless sensor networks, modelling and simulation and artificial intelligence.

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