Fuzzy Logic based Efficient Route Determination Method for Improving the Energy Efficiency of Sensor Networks in FAP-based WSNs

Won-jin Chung
College of Information and Communication Engineering
Sungkyunkwan University
Republic of Korea

Tae-ho Cho
College of Software
Sungkyunkwan University
Republic of Korea

ABSTRACT

A flooding attack in a wireless sensor network consumes the energy of the sensor node included in the path in the process of sending a persistent false packet to the base station. If a flooding attack is continuously generated, the sensor node with a low residual energy causes energy depletion and the life of the sensor networks is shortened when the number of sensor nodes having depleted energy is large. To prevent such attacks, a flooding prevention scheme was proposed. However, flooding attack prevention does not consider cases where the residual energy of the sensor node is low. In areas where the sensor node is installed a long time ago, the remaining energy of the sensor nodes remains low. For this reason, when the flooding attack prevention method is used to prevent flooding attack, energy depletion occurs in the detection process in the sensor node with low residual energy. In this paper propose a method to improve the energy efficiency of a sensor node by determining an efficient path during routing by adding message authentication code through fuzzy logic or by using flooding attack prevention when setting a path.

Keywords

Wireless Sensor Networks, Network Security, Network Lifetime, Flooding Attack Prevention, Fuzzy Logic

1. INTRODUCTION

Wireless sensor networks (WSNs) consist of a large number of sensors and a base station (BS) that collects information over a wide area. Because the sensor node is low cost, a large number of sensor nodes are installed over a wide area. Sensor nodes are used in various fields including battlefield areas, smart cities, hospitals, and firefighting facilities. When the sensor node detects events, it creates packets and transmits packets to the BS via wireless communications through predetermined paths [1].

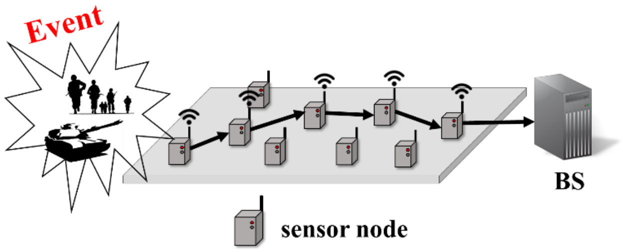


Fig 1: Wireless Sensor Network

However, the computational complexity of sensor nodes is limited. In addition, sensor nodes are constrained as they are unable to recharge their energy by being placed in an external environment. Using these constraints, malicious attackers can easily compromise the sensor nodes [2]. The attacker may attempt a flooding attack using a compromised node. Flooding attacks are an attack on the remaining energy of the sensor nodes and result in a reduction of the sensor network life. In this paper utilized the flooding attack prevention (FAP) scheme proposed by Y. Ping to prevent flooding attacks [3]. FAP is a flooding attack prevention scheme based on the Ad-hoc On-demand distance vector (AODV) routing protocol. Continuous on-going energy consumption of the sensor nodes occurs during the flooding attack detection process through the FAP schemes. If the residual energy of the sensor nodes is low, there is a problem with the depletion of energy in the flooding attack detection process. Such a problem requires an order to exclude the depleted sensor nodes and set up a new route, where it is necessary to perform route research through AODV routing. Furthermore, additional energy consumption occurs in the sensor networks during this process. In this study utilized fuzzy logic to determine the effective route according to whether message authentication code (MAC) is used. The proposed scheme increases the energy efficiency of the sensor node by selecting the most efficient path between that using the existing FAP scheme and that using MAC. Section 2 of this paper describes the AODV routing protocols, flooding attacks, FAP, and MAC protocols used in FAP. Section 3 describes the proposed scheme using fuzzy logic. Section 4 describes the results of the experiments and Section 5 presents the conclusions and future plans.

2. RELATED WORKS

2.1 AODV Routing Protocol

The AODV routing protocol uses routing tables to minimize route navigation costs when sending packets to destinations [4]. To establish a path, the presence of the corresponding path in the routing table is first determined. The packet is sent to the configured route without the route research process if the path exists in the routing table. If the path does not exist in the routing table or if an error occurs when using the corresponding path, the path is route researched using the extended ring search (ERS) algorithm. ERS is a scheme that uses time to live (TTL) in the process of finding a destination node. It has been proposed to reduce the unnecessary route request (RREQ) packet to be transmitted to the whole network by gradually expanding the search range. The source node sets the timeout to RING_TRAVERSAL-TIME.

RING_TRAVERSAL_TIME =

2 * NODE_TRAVERSAL_TIME * (TTL_VALUE + TIMEOUT_BUFFER) (1)

For the source node, set NODE_TRAVERSAL_TIME to 40 ms and set the TTL_VALUE to 1. The source node waits for the route request (RREP) packet for

RING_TRAVERSAL_TIME. If the RREP packet is not received during RING_TRAVERSAL-TIME, it is increased by TTL_INCREMENT (= 2). Repeat this process and if the TTL_VALUE exceeds TTL_THRESHOLD (= 7), set the timeout to NET_TRAVERSAL_TIME and retransmit the RREQ packet.

NET_TRAVESAL_TIME =

2 * NODE_TRAVERSAL_TIME * NET_DIAMETER (2)

NET_DIAMETER is set to 35. Therefore, NET_TRAVESAL_TIME is set to 2,800 ms. If the RREP packet is not received for the NET_TRAVESAL_TIME time, it is determined that the destination node does not exist in the network and the route search is stopped. This process improves the energy efficiency of the network by reducing unnecessary RREQ transmissions. Fig 2 shows the entire diagram of the ERS [5].

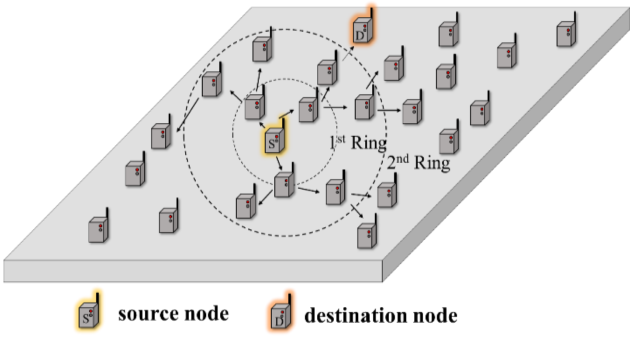


Fig 2: Extended Ring Search

However, AODV is a proposed protocol based on the ad-hoc network. In order to use AODV in WSNs, it is necessary to consider the sensor node energy problem consumed in the route research process because a transmission error occurs due to the limited energy of the sensor node and link quality [6].

2.2 Flooding Attack

The flooding attack in the WSNs generates false packets from the compromised node and continues to forward false packets to the BS. Therefore, the sensor nodes included in the packet forwarding path consume energy continuously in the process of transmitting and receiving the packets. If a flooding attack occurs continuously and if a node detects an event due to a network overload sending a packet, the event packet detected due to a continuous false packet may be blocked. In addition, if the energy of sensor nodes in the path is depleted as flooding attacks occur, the new route must be set aside except for that sensor node. If this happens repeatedly, the sensor node that is depleted of energy generates a shadowing area, which shortens the life of the sensor networks [7].

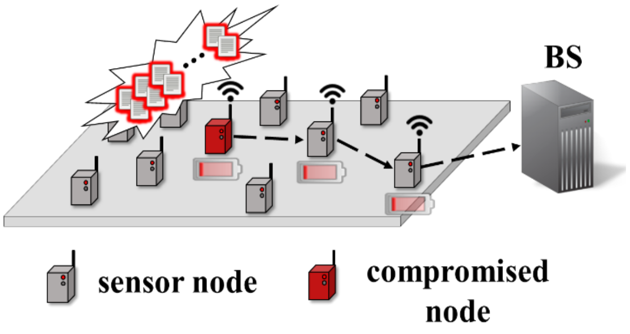


Fig 3: Flooding Attack

2.3 FAP

FAP is a security technique that uses the AODV routing protocol to prevent flooding attacks in the ad-hoc network. FAP compares the ID of the sensor node with the packet creation time at the BS when the attacker attempts the flooding attack. If the number of packets having the same node ID and packet generation time in the packet arrived at the BS is greater than a predetermined threshold value, it is judged to be a flooding attack. The BS then registers the suspected sensor node ID in the blacklist and updates the blacklist of all the sensor nodes through the broadcast. Thus, the downstream node judges that the sensor node sending the continuous packet is a flooding attack and the forwarded packet is blocked and not transmitted to the next sensor node. In this process, the FAP detects and prevents flooding attacks.

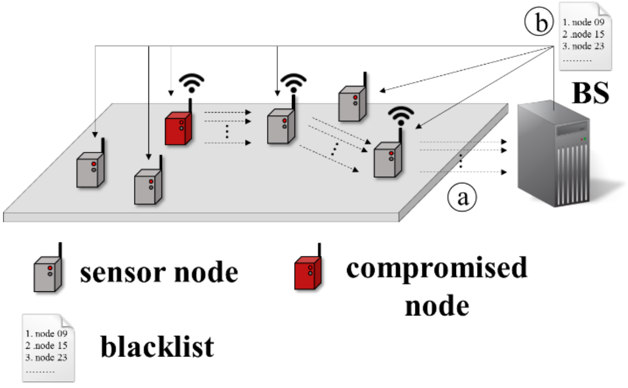


Fig 4: Flooding Attack Prevention - 1

Fig 4 and 5 show the process of detecting flooding attack through FAP when flooding attack occurs. Fig 4(a) shows the process of transferring false packets to the BS when flooding attack occurs. In this case, the BS collects the source node ID and the packet generation time. The BS estimates that a flooding attack occurs at the source node through the FAP technique. The BS then registers and updates the source node ID in the blacklist. Fig 4(b) shows the process of transferring the updated blacklist to all of the sensor nodes.

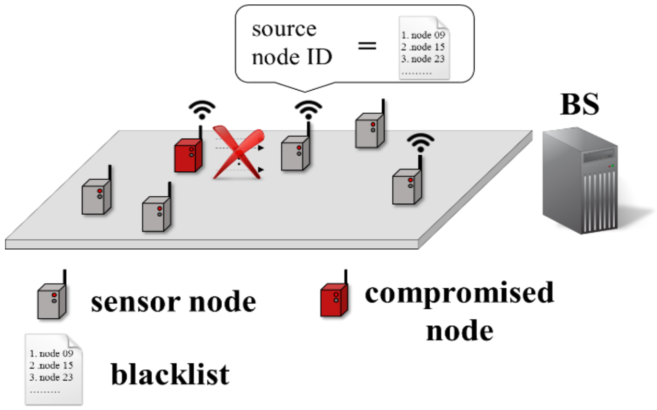


Fig 5: Flooding Attack Prevention - 2

The downstream node that receives the packet is compared to the node ID of the source node using the updated blacklist. As shown in Fig 5, if there is a node ID of the source node in the blacklist, it is judged to be a flooding attack and all packets transmitted from the source node are blocked.

2.4 MAC

MAC is a small amount of information used to authenticate messages. The message authentication generates MAC by receiving a private key through a MAC algorithm. The sender then communicates the MAC with the message. The receiver uses the transmitted message to generate MAC in the same way that the sender created the MAC. The private key used to generate the MAC is the same private key as the sender. Then, when the MAC is identical to the MAC transmitted to the sender, the message is determined to be a normal message. This is a way to protect authentication and integrity through MAC [8].

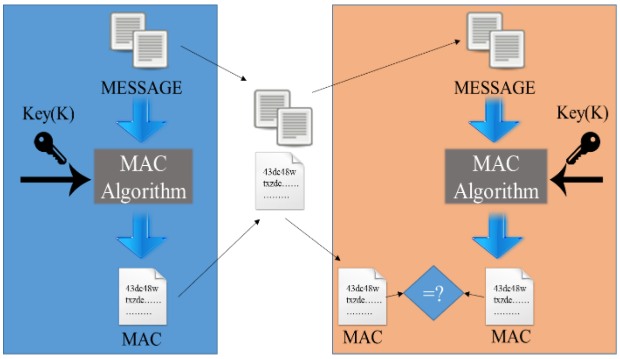


Fig 6: Message Authentication Code

3. PROPOSED SCHEME

3.1 Assumptions

The sensor nodes are randomly placed and flooding attacks occur through the compromised node. The route of the AODV routing table must be updated after a route research process. The BS can locate the position of each sensor node. Further, the BS can estimate the residual energy and state of the sensor nodes from the sensor node to the BS.

3.2 Fuzzy System

The proposed method increases the energy efficiency of each sensor node by adding MAC to the packet according to fuzzy logic, thereby extending the lifetime of the sensor networks. When using MAC to validate packets, the private key used in the MAC algorithm is distributed to the upstream node and the downstream node defined in the routing function. Then, the MAC is generated and the packet is verified by mutual authentication. However, there is a large amount of energy consumption in the downstream node to generate the MAC to validate the packet. Therefore, when setting the route through the fuzzy logic in the route research process, the most efficient route among the route setting method using the MAC and FAP scheme is determined for the packet.

3.2.1 Input and Output Parameters

The input parameters are the distance (D) between the event detection node and the BS, the residual energy (RE) of the sensor node, and the frequency of occurrence of the event (FE). The output parameter is whether or not the MAC is applied (MA).

3.2.1.1 Input Parameter

D = {S (Short), M (Medium), F (Far)}

RE = {L (Large), M (Medium), S (Small)}

FE = {VL (Very Low), L (Low),

M (Medium), H (High), VH (Very High)}

3.2.1.2 Output Parameter

MA = {Y (Yes), N (No)}

The first parameter is the distance between the event detection node and the BS, which is an important factor determining whether to add MAC to a packet through fuzzy logic. If a flooding attack occurs from a compromised node, a large number of false packets are delivered to the BS through the established route. When a flooding attack occurs, if the distance between the compromised node and the BS is long, the verification through MAC continues. During the verification process, energy consumption of the downstream node occurs and if the residual energy is low, energy is exhausted. Due to these problems, authentication via MAC is required only if the distance between the compromised node and the BS is short. The second input parameter is the residual energy of the sensor node. When a sensor node with a low residual energy verifies a flooding attack through MAC, the energy of the sensor node is exhausted due to excessive energy consumption. Therefore, if the path contains sensor nodes with low residual energy, flooding attack verification through MAC cannot be applied. The last parameter is the frequency of events. In the event that there is a large number of events, if MAC is used for verification, the event should be verified through the downstream node even if there is no flooding attack. When an event occurs frequently, the downstream nodes consume a lot of energy through continuous verification. Therefore, in areas where frequent events occur, the FAP scheme should be applied. When the FAP technique is used, the energy consumption of each sensor node is comparatively low because it judges whether a flooding attack is made by comparing the sensor node IDs in the black list.

3.2.2 Fuzzy Role

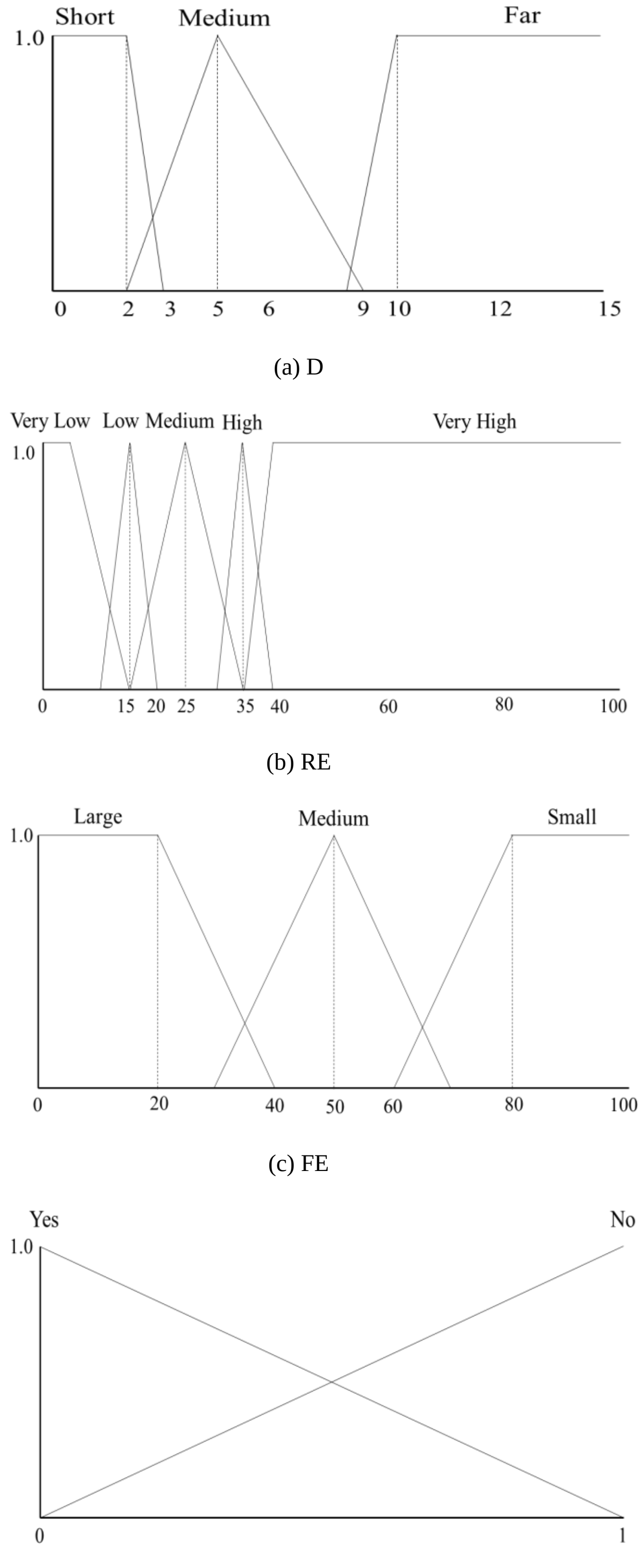
Some of the fuzzy rules used in the proposed scheme are shown in Table 1.

Table 1. Fuzzy Rule

Rule	Input			Output (MA)
	D	RE	FE	
2	S	L	L	Y
7	S	M	L	Y
14	S	S	H	N
18	M	L	M	Y
24	M	M	H	N
28	M	S	M	N
32	F	L	L	Y
36	F	M	VL	Y
40	F	M	VH	N
44	F	S	H	N

Rule 2 should apply the proposed scheme when the distance between the event detection node and the BS is short, the residual energy of the sensor node is large, and the event occurrence frequency is low. Rule 28 does not apply the proposed scheme when the distance between the event detection node and the BS is medium, the residual energy of the sensor node is small, and the event occurrence frequency is medium.

3.2.3 Fuzzy Membership Function



(a) D

(b) RE

(c) FE

(d) MA

Fig 7: Membership Function

Fig 7(a), Fig 7(b), and Fig 7(c) show the membership functions for the input parameters, and Fig 7(d) shows the membership function for the output parameters.

4. EXPERIMENTAL RESULTS

The size of the sensor field used in the experiment is 1,000 × 1,000 m^2 and the number of sensor nodes used is 500. The false packet size used in the flooding attacks is 29 bytes in TinyOS and the size of the MAC used for verification is 4 bytes [9]. The energy consumed when transmitting 1 byte of the sensor node is 16.25 µJ and the energy consumed when receiving 1 byte is 12.25 µJ [10]. Fig 8 shows the energy efficiency of the sensor networks according to the number of flooding attacks. When the energy of each sensor node is compared and the flooding attack occurs 50 times, the proposed method shows that the energy efficiency of the sensor networks was improved by about 20% compared to the FAP technique. Fig 9 shows the energy consumption of three nodes among a large number of sensor nodes.

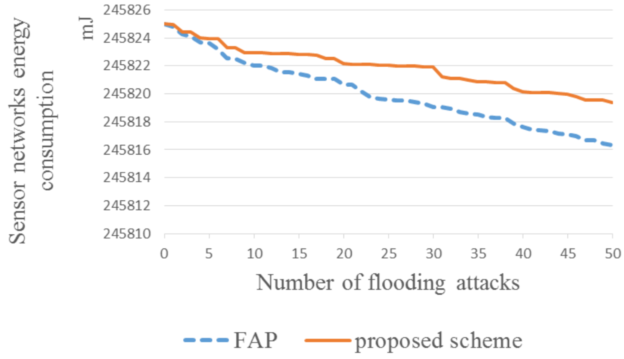


Fig 8: Sensor network energy efficiency

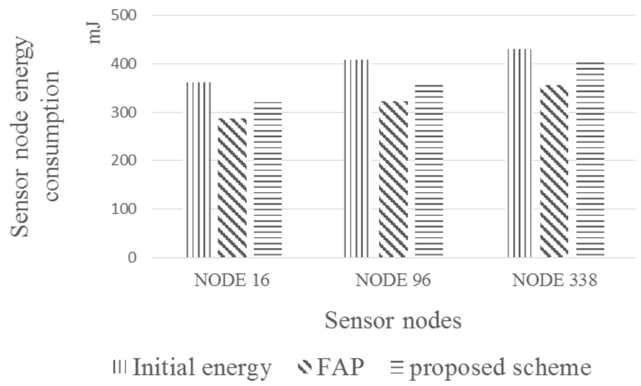


Fig 9: Sensors nodes energy efficiency

Also, when 50 flooding attacks occur, the residual energy of three downstream nodes is exhausted in the FAP scheme. However, in cases where flooding attacks occur, the FAP scheme prevents flooding attack using the sensor node ID and the blacklist comparison process. Therefore, when blacklist data of the FAP scheme is sufficient, the consumed energy efficiency can be similar or even better compared to the proposed scheme.

5. CONCLUSIONS

The FAP scheme is used as a security technique to cope with flooding attacks. However, the FAP scheme does not consider the residual energy of the sensor node. Therefore, when the residual energy of the sensor node is low, the sensor node is depleted of energy due to flooding attack. If a sensor node suffers from depletion of energy, a route reset is required, resulting in additional energy consumption of the sensor networks. To address these problems present an efficient path determination scheme through fuzzy logic. The energy efficiency of the sensor networks is improved by determining the efficient path between the FAP technique and the verification of flooding through the MAC technique. The experimental results show that the energy efficiency of BS peripheral sensor nodes improved by about 20% compared to FAP. This reduces the amount of energy depletion of the sensor nodes around the BS. However, when a large number of flooding attacks occur, the energy efficiency of the FAP scheme is improved because the blacklist data is sufficient when the FAP scheme is used. Future research will use both the blacklist technique used in the FAP scheme and the MAC verification when a flooding attack occurs. Therefore, the future study will evaluate the path determination method that improves the energy efficiency through the fuzzy logic by using the blacklist method and the MAC verification method at the same time.

6. ACKNOWLEDGMENTS

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. NRF-2015R1D1A1A01059484)

7. REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "A survey on sensor networks," Communications Magazine, IEEE, vol. 40, pp. 102-114, 2002.

[2] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," Ad Hoc Networks, Vol. 1, No. 2, pp. 293-315, 2003

[3] Y. Ping, H. Yafei, Z. Yiping, Z. Shiyong and D. Zhoulin, “Flooding attack and defence in ad hoc networks,” Journal of Systems Engineering and Electronics, Vol. 17, No.2, pp. 410-416, 2006

[4] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc on-demand distance vector (AODV) routing," IETF RFC 3561, 2003

[5] N. D. Pham and H. Choo, "Energy efficient expanding ring search for route discovery in MANETs," Communications, 2008

[6] V. C. Gungor, C. Sastry, Z. Song, and R. Integlia, "Resource-aware and link quality based routing metric for wireless sensor and actor networks," Communications, 2007

[7] D. R. Raymond and S. F. Midkiff, “Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses,” IEEE Pervasive Computing, vol. 7, pp. 74-81, 2008

[8] Y. Wang, G. Attebury, and B. Ramamurthy, “A survey of security issues in wireless sensor networks,” IEEE Communications Surveys & Tutorials, vol. 8, pp. 2-23, 2007

[9] J. Deng, R. Han, and S. Mishra, "Defending against path-based DoS attacks in wireless sensor networks," In Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks pp. 89-96, 2005

[10] F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical en-route filtering of injected false data in sensor networks," IEEE Journal on Selected Areas in Communications, Vol. 23, No. 4, pp. 839-850, 2005