# Intrusion Detection Scheme against Sinkhole Attacks in Directed Diffusion Based Sensor Networks

**Soo Young Moon and Tae Ho Cho**

Sungkyunkwan University, Suwon 440-746, Republic of Korea

**Summary**
Wireless Sensor Networks (WSNs) detect and report interesting events when they occur in the target region. These networks are vulnerable to security breach due to wireless communication and lack of infrastructure. In sinkhole attacks, an attacker attracts network traffic by forging or replaying routing messages through compromised nodes. Thus attracted traffic is used for selective forwarding, denial of service (DoS) and false report attacks. In this paper, we show the vulnerability of the directed diffusion routing protocol to sinkhole attacks. And we also propose the intrusion detection scheme using fuzzy logic for detecting and defending sinkhole attacks in directed diffusion based sensor networks.

***Key words:***
*Wireless sensor networks, sinkhole attack, intrusion detection system, fuzzy logic.*

## 1. Introduction

Wireless Sensor Networks (WSNs) are emerging technologies that enable immediate interaction between human and environment. The role of WSNs is to detect and report interesting events in the target region to a user when they occur. There are many application areas of WSNs such as disaster prevention, object tracking, monitoring of human facilities. Many sensor nodes equipped with event sensing, computation and message transmission capabilities organize a WSN, and a sink node collects event data from them for providing it to a user. Each sensor node is powered by a battery, so it always suffers from limited energy resource [1-3]. Fig. 1 shows the organization of WSN.

In WSNs, sensor nodes use multi hop, wireless links to transmit messages. Also, usually there is no infrastructure to manage and support the operation of WSN. Due to the features, WSNs are prone to many security attacks. In sinkhole attacks, an attacker attracts network traffic by forging or replaying routing messages through compromised nodes. The compromised nodes can try selective forwarding, denial of service (DoS) and false report attacks for attracted traffic [4-6].

In this paper, we show the vulnerability of the directed diffusion routing protocol to sinkhole attacks, and propose the intrusion detection scheme for detecting and defending sinkhole attacks in directed diffusion based sensor networks. In the proposed scheme, a few master nodes (MNs) monitor the communication between sensor nodes. Each MN periodically sends the number of routing messages heard in its monitoring area divided by the number of event-sensing nodes in the area to the sink node. The sink node derives a detection value from it and the number of average hop counts between any two nodes in that area. Fuzzy logic [7] is used for derivation of the detection value.

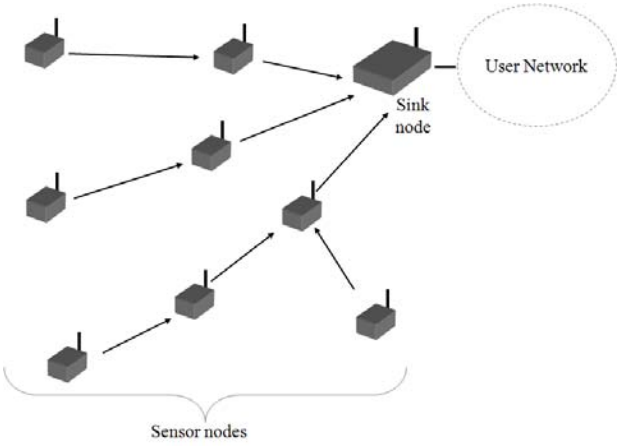



Fig. 1 Organization of WSN

The remaining sections are as follows. In section 2 we briefly review the operation of directed diffusion and vulnerability to sinkhole attacks. In section 3 we present the proposed scheme to detect and defend the sinkhole attacks in directed diffusion based sensor networks. In section 4 we show the simulation result. In section 5 we conclude the paper and state future work.

## 2. Background

### 2.1 Directed Diffusion

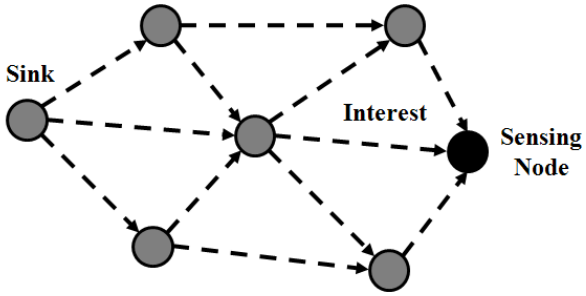
Directed diffusion [8, 9] is a data-centric routing protocol for a WSN. In directed diffusion, sensor nodes route

Manuscript received July 5, 2009
Manuscript revised July 20, 2009

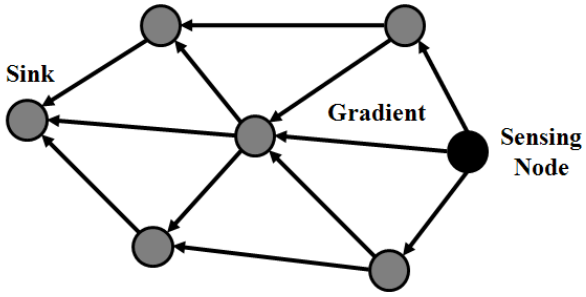
messages based on the data contained in it, not nodes' addresses. The operation of directed diffusion can be divided into three steps; 1) interest dissemination, 2) gradient setup, 3) path reinforcement and event data forwarding. In interest dissemination, a sink node broadcasts an interest message that is a sensing task to each of its neighbors. Again, the neighbor nodes of the sink node broadcast the interest message to their neighbors. The interest message is disseminated through the whole network in this way. An interest message contains event type, target region, interval, duration, and some other fields.

Once a node receives the interest message from its neighbor, it establishes a gradient toward the neighbor. Each gradient contains 1) the neighbor node's ID to which a node will forward corresponding event messages, 2) a required event data rate, and 3) duration.

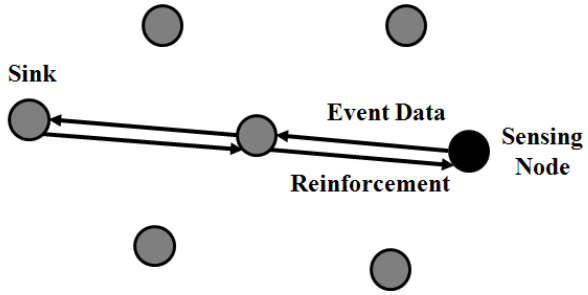
When an event occurs and it matches the event type in previous interest messages, the sensing nodes generate and forward event messages based on their gradients. Intermediate nodes also forward the messages to the sink node based on their gradients. After the sink node receives the event messages, it chooses the neighbor node that first sent an event message to it. Then the sink node sends a path reinforcement message to the node. The path reinforcement message is forwarded through the best path between the sink node and the event sensing nodes. After that, event messages are forwarded through the reinforced path [8, 9]. Fig. 2 illustrates the operation of the directed diffusion.




(a) Interest dissemination




(b) Gradient setup




(c) Data forwarding through reinforced path

Fig. 2 Overview of directed diffusion

## 2.2 Sinkhole Attacks in Directed Diffusion

In sinkhole attacks, the objective of an attacker is to lure as much as traffic from a target area through a compromised node. For this, the compromised node advertises high quality routes to the sink node. Then its neighbor nodes forward event messages destined for the sink node to it. Using lured traffic, the compromised node is able to try various attacks including selective forwarding, denial of service (DoS), false report attacks.

In directed diffusion, the attacker forges routing messages used in the directed diffusion protocol. Specifically, he fabricates path reinforcement messages used for setting a routing path from a sensing node to the sink node. The compromised node sends the forged path reinforcement messages to the other nodes. The receiving nodes send event messages to the compromised node when they sense events or receive event messages from other nodes. Consequently, the compromised node can lure much traffic from target area and try various attacks including selective forwarding, denial of service (DoS) and false report attacks. Fig. 3 shows the sinkhole attacks in directed diffusion.

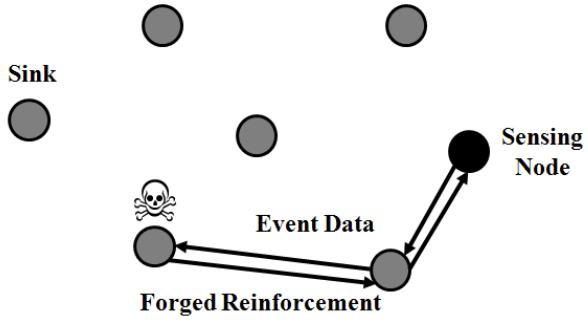



Fig. 3 Sinkhole attacks in directed diffusion

## 3. Proposed Scheme

### 3.1 Assumptions

The assumptions in the proposed scheme are as follows. Sensor nodes equipped with limited resources such as energy, computation capacity and transmission range [10, 11] are deployed in the field randomly. The target region is divided into several areas and the sink node can estimate the average number of hop counts between any two nodes in each area. The master nodes used in the proposed scheme possess more energy and computation power, and can communicate with the sink node directly. In directed diffusion each node sends a path reinforcement message to the first node which sent required event reports to it. The path through which a path reinforcement message is forwarded is the shortest path between the sink node and an event sensing node.
In sinkhole attacks, an attacker forges path reinforcement messages and sends them to the event sensing nodes. The nodes that receive the forged messages send event messages to the compromised node. Then he can try selective forwarding, denial of service (DoS), false report attacks.

### 3.2 Motivation & Goal

The objective of the proposed scheme is to detect and defend sinkhole attacks possible in directed diffusion based sensor networks. In directed diffusion, the number of reinforcement messages transmitted in each area is proportional to the number of event-sensing nodes in that area, and can be represented as the following equation.

$$N_R \approx Avg_{Hop} \cdot N_{SN} \quad (1)$$

In the above equation, $N_R$ is the number of reinforcement messages transmitted in an area, and $N_{SN}$ is the number of event-sensing nodes in that area. $Avg_{Hop}$ is the average number of hop counts between any two nodes in that area. In sinkhole attacks, an attacker forges path reinforcement messages used in the directed diffusion. Hence there will be more path reinforcement messages transmitted in the field than those in normal condition. If we measure the number of path reinforcements messages sent between sensor nodes, we can detect the sinkhole attack. For this, the proposed scheme uses a few master nodes (MNs) that collect data for intrusion detection. Each Master node counts the number of event-sing nodes and path reinforcement messages transmitted in its area. The sink node receives the data from the MNs and judges whether sinkhole attack has occurred or not in each area. The concept of master nodes that monitors sensor network and send data to the sink nodes was borrowed from [12], a previous work on intrusion detection system in sensor networks.

### 3.3 Overview

Some definitions to describe our scheme are as follows.

**Reinforcement Ratio** is the number of reinforcement messages transmitted in an area divided by the number of event-sensing nodes in that area ($N_R$/ $N_{SN}$).

**Radius** is the average number of hop counts between any two nodes in an area ($Avg_{Hop}$).

In directed diffusion based sensor networks, each sensor node operates in the same manner. But in the proposed scheme, normal sensor nodes and a few master nodes are deployed together in the field. Each master node counts the number of event-sensing nodes and the number of path reinforcement messages transmitted in its area. It periodically calculates and sends the reinforcement ratio to the sink node. Fig. 4 presents the overview of the proposed scheme.

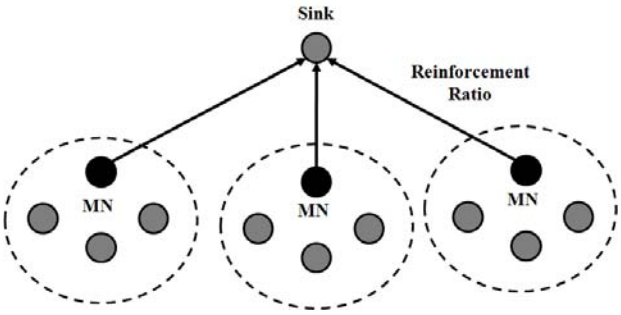



Fig. 4 Overview of proposed scheme

The sink node knows the location of all the master nodes and judges whether sinkhole attacks has occurred for each area using the data. In judgment, the sink node uses security threshold value that controls the degree of detection. Low security threshold value decreases the false negative ratio (probability of not detecting sinkhole attacks), but increases false positive ratio (probability of detecting non-existing sinkhole attacks).

### 3.4 Fuzzy Logic Design

The proposed scheme uses fuzzy logic to derive detection value for each area from given inputs. The two inputs are 1) reinforcement ratio and 2) radius of the area. From the two inputs, fuzzy logic can derive detection value. If the detection value is greater than the security threshold value which was previously set, sinkhole attack is detected.

In the proposed scheme, detection value becomes high when the reinforcement ratio is large and the radius is small, and vice versa. Fig. 5 illustrates the fuzzy inputs and output variables.

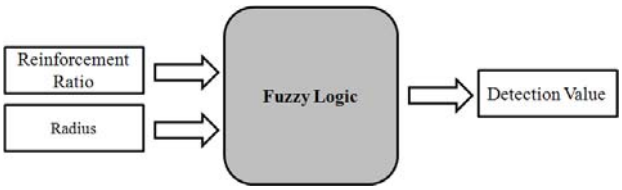
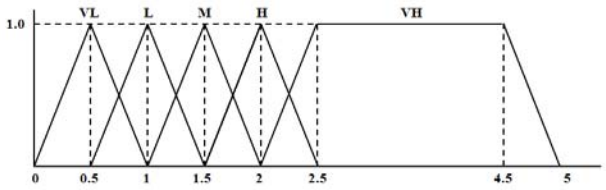
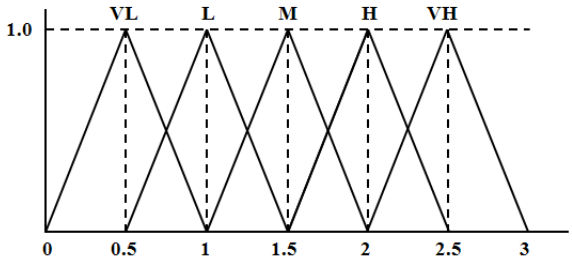



Fig. 5 Fuzzy input & output variables

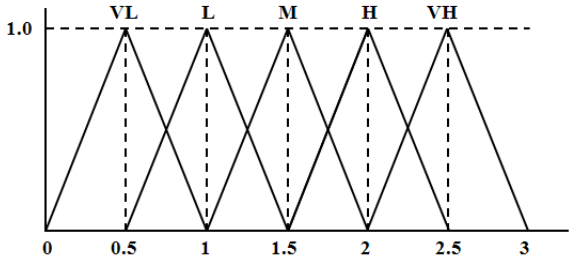
Fig. 6 shows the fuzzy membership functions. In the proposed scheme, the fuzzy membership functions of input and output variables have five fuzzy sets – VL(Very Low), L(Low), M(Medium), H(High), and VH(Very High).




(a) Reinforcement Ratio




(b) Radius




(c) Detection value

Fig. 6 Fuzzy membership functions

Table 1 shows some fuzzy rules for the proposed scheme.

Table 1. Fuzzy IF-THEN rules

| Rule No. | Reinforcement Ratio | Radius | Detection value |
|---|---|---|---|
| 2 | VL | L | VL |
| 6 | L | VL | M |
| 13 | M | M | L |
| 17 | H | L | H |
| 21 | VH | VL | VH |

## 4. Simulation result

In this section, we confirm that the proposed scheme provides high detection capability for sinkhole attacks.
The simulation model we have designed is as follows. The size of sensor network is 100 × 100 $m^2$ and 100 sensor nodes are deployed in the field. The sensor network is divided into four areas and a master node monitors each area. Two performance measures were used to evaluate the proposed scheme – 1) false positive ratio (FPR) and 2) false negative ratio (FNR). False positive ratio is the probability of detecting non-exist sinkhole attack, and false negative ratio is the probability of not detecting sinkhole attack. Fuzzy logic is used to derive detection value and free fuzzy logic library on the web [13] was used to implement fuzzy logic. Fig. 7 represents FPR and FNR of the proposed scheme for varying security threshold values.

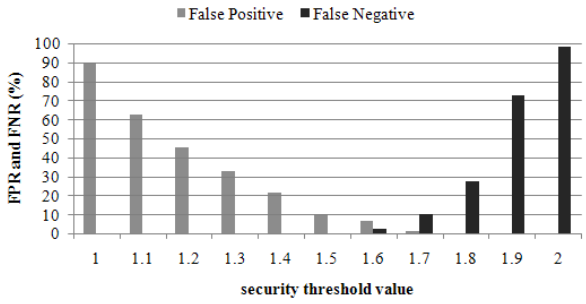



Fig. 7 False positive & False Negative ratio

Security threshold value varies from one to two. It can be shown that increase of security threshold value results in decrease of FPR and increase of FNR. If we choose proper security threshold value, we can achieve both low FPR and low FNR (that is, efficient detecting of sinkhole attacks) by using the proposed scheme.

## 5. Conclusion

In this paper, we proposed the intrusion detection scheme for detecting and defending sinkhole attacks in directed diffusion based sensor networks. In directed diffusion, an attacker can forge path reinforcement messages and send them to event sensing nodes for the purpose of attracting event messages. The attacker can try selective forwarding, denial of service (DoS) and false report attacks within the network. By monitoring the number of path reinforcement messages transmitted and event-sensing nodes in each area, we can judge whether sinkhole attack has occurred or not. A few master nodes perform the monitoring task and periodically send messages which include the number of path reinforcement messages transmitted in its area divided by the number of event-sensing nodes in the area to the sink node for detecting sinkhole attacks. By performing simulation, we confirmed that the proposed scheme can achieve both low FPR (false positive ratio) and low FNR (false negative ratio). Our future work is to consider more attack types and enhance the detection system by incorporating various algorithms.

### Acknowledgments

This work was supported by the Korea Research Foundation Grant funded by the Korean Government (KRF-2008-313-D00827).

## References

[1] N. Xu, “A Survey of Sensor Network Applications,” Tech. Rep., University of Southern California, 2002.
[2] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “A Survey on Sensor Networks,” IEEE Communications Magazine, vol. 40, no. 8, pp. 102-116, 2002.
[3] J.N. Al-Karaki, and A.E. Kamal, “Routing techniques in wireless sensor networks: a survey,” IEEE Wireless Communication Magazine, vol. 11, no. 6, pp. 6-28, 2004.
[4] C. Karlof, and D. Wagner, “Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures”, Elsevier, Elsevier's Ad Hoc Networks Journal, Special Issue on Sensor Network Protocols and Applications, vol. 1, no. 2-3, pp. 293-315, 2003.
[5] D. Djenouri, L. Khelladi, and N. Badache, “A Survey of Security Issues in Mobile Ad-Hoc and Sensor Networks,” IEEE Communications Surveys & Tutorials, vol. 7, no. 4, pp. 2-28, 2005.
[6] S. Datema, “A Case Study of Wireless Sensor Network Attacks,” Master’s Thesis in Computer Science, Delft University of Technology, 2005.
[7] J. Yen, R. Langari, “Fuzzy Logic,” Prentice Hall, 1999.
[8] C. Intanagonwiwat, R. Govindan, and D. Estrin, “Directed diffusion: a scalable and robust communication paradigm for sensor networks,” in Proceedings of ACM Mobicom, Boston, MA, pp. 56-67, 2000.
[9] C. Intanagonwiwat, R. Govindan, D. Estrin, J. Heidemann, F. Silva, “Directed Diffusion for Wireless Sensor Networking,” IEEE ACM T. Network vol. 11, no. 1, pp. 2-16, 2003.
[10] Xbow sensor networks, http://www.xbow.com
[11] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, and K. Pister, “System Architecture Directions for Networked Sensors,” in Proc. ASPLOS, pp. 93-104, 2000.
[12] Sang Hoon Chi and Tae Ho Cho, “Fuzzy Logic Anomaly Detection Scheme for Directed Diffusion Based Sensor Networks,” Lecture Notes in Artificial Intelligence, vol. 4223, 2006, pp. 725-734.
[13] jFuzzyLogic, http://jfuzzylogic.sourceforge.net

**Soo Young Moon** received the B.S. degree in Electrical and Computer Engineering from Sungkyunkwan University in 2007. He is a M.S. candidate in the School of Information and Communication Engineering at Sungkyunkwan University. His research interests include modeling and simulation, sensor network security, 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, modeling & simulation, and enterprise resource planning.