A Sinkhole Attack Detection Mechanism for LQI based Mesh Routing in WSN

Byung Goo Choi [1], Eung Jun Cho [2], Jin Ho Kim [3], Choong Seon Hong [4] and Jin Hyoung Kim [5]
[1 2 3 4] *Department of Computer Engineering, Kyung Hee University*
Seocheon, Giheung, Yongin, Gyeonggi, 446-701 Korea
{ bgchoi[1], ejcho[2], jinhowin[3], cshong[4]}@khu.ac.kr
[5] *Samsung Electronics*
jhyoung.kim@samsung.com[5]

Abstract— **In this paper, we propose a detection scheme for sinkhole attacks in wireless sensor networks. Sinkhole attack makes flowing packets to pass through attacker. As a consequence, Sinkhole attack can be extended to various kinds of attacks. We analyze sinkhole attack methods in the networks that use LQI based routing. We show the detection of sinkhole attack can be achieved by using a few detector nodes.**

I. INTRODUCTION

Wireless sensor network is one of the important technologies to become a base in future ubiquitous society. Sensor network can be used comprehensively in collection and measurement of data. Because sensor network can form self configurable networks, distribution and configuration are easy. However, sensor nodes can be subverted by variety of attacks due to limited computing resource and weaknesses of wireless communication. Especially, network can be easily made unstable by attacking the routing protocol. Moreover, defense techniques used in wire networks are hard to apply in wireless sensor network with limited processing power and resources.

In wireless sensor network, one of the severe routing attacks is sinkhole attack [1]. Malicious node wrongfully advertises itself more nearer to the Base Station or destination node. As a result, a lot of nodes start to use the attacker as a relay or destination node. Therefore, malicious node can control traffics of network that flow from it. Therefore, detection of sinkhole attack is important research field for security of wireless sensor network.

In this paper, we propose a method that can detect sinkhole attack for safe data transmission in wireless sensor network which uses LQI based routing. The remainder of the paper is organized as follows. Section II discusses some of the related works. Section III describes the proposed scheme. Section IV presents the simulation results. Finally, Section V concludes our work.

II. RELATED WORK

A. Distance Vector Routing Protocol

Distance vector routing protocol is used broadly in network that select optimum route based on various elements such as hop-count, link delay, bandwidth [2]. In this paper, we discuss Routing protocol that use LQI (Link Quality Indicator) to select optimum route. For example, LOAD Routing protocol is a distance vector routing protocol which is proposed for 6LowPAN [3]. LOAD routing protocol simplifies AODV routing protocol. However, LOAD uses LQI based routing to differ with AODV.

B. Link Quality Indicator

The LQI is measured by the strength or quality of a received packet. LQI can be calculated using receiver energy detection, a signal-to-noise ratio estimation, or a combination of these methods. The LQI measurement shall be performed for each received packet. The minimum and maximum LQI values (0x00 and 0xff) should be associated with the lowest and highest quality compliant signals detectable by the receiver. LQI values in between should be uniformly distributed between these two limits. A higher LQI value indicates a higher quality link. However, link cost inverts this relationship. In other words, a lower link cost indicates higher quality link.

C. Sinkhole Attack

Sinkhole attack feigns that attacking node is located on the shortest path that proceeds to important node or destination node such as Base Station. This attack can exert big negative impact to network even if there is just one attacking node [1]. Specially, in the case of dynamic routing protocol, which is designed to achieve automatic path discovery and maintenance between sensors according to the circumstances of the network, sinkhole attack has severe effects. Because, these protocols collect network information periodically and decide routing path and in the presence of sinkhole whole network can be compromised. Fig. 1 depicts the network state with Sinkhole attacks. This state is easy to be extended to attack of various forms including wormhole.

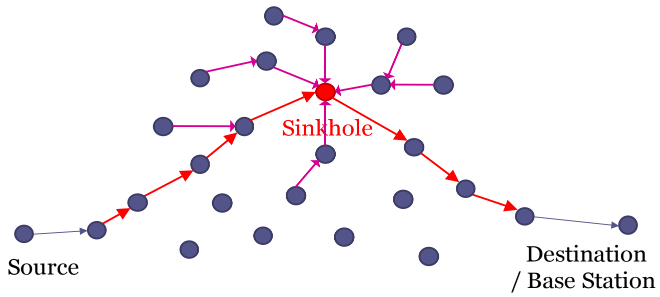


Fig. 1 Example of Sinkhole attack

D. Sinkhole attack detection for hop-count based routing

Existent sinkhole attack detection technique supposes hop-count based routing [5]. Also, existent detection method supposes that all sensor nodes transmit data to the Base Station periodically.

Selective Forwarding is one of the attacks which can ripple high its effect if it is cast with Sinkhole attack [6]. In Selective Forwarding, malicious node does not deliver some of the packets that pass through it, deliberately. In the case of this attack, Base Station can make a list of nodes which are not transmitting the data during some predefined period. Base Station gathers Next-hop information from all other nodes which are located in the attacking area. And reconstruct the network topology. For example, in Fig. 2, it can judge that node that is located in top-level in network tree is sinkhole attack node.

However, in the case of this detection method, Base Station cannot detect sinkhole attack though detection of additional attack that malicious node can achieve (Selective Forwarding in above situation) can be detected. In other words, Base Station cannot judge sinkhole attack presence if do not detect attack achieved with sinkhole attack. Also, it can not apply to LQI based mesh routing protocol. In addition, sensor nodes are exposed to attack before sinkhole attack is detected. Therefore, in this paper, we propose sinkhole attack detection method differing with existent method.

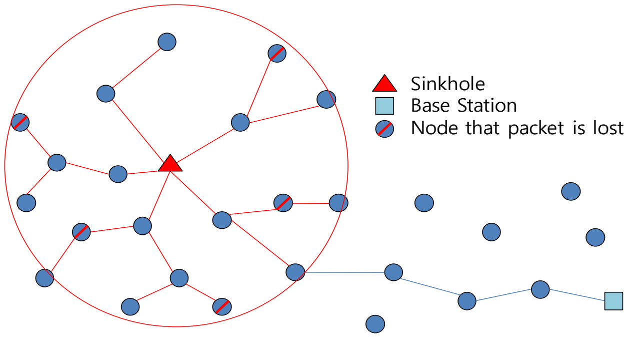


Fig. 2 Existent attack detection method

III. PROPOSED SCHEME

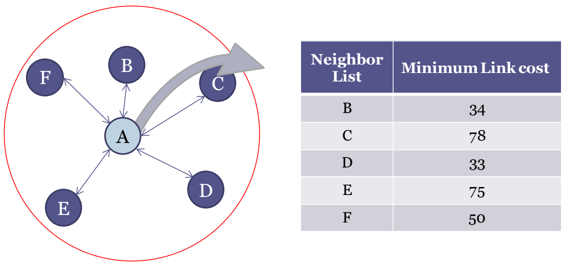
A. Assumption

The following five assumptions are used to proposed detection scheme.

- Network is consisted of general nodes and few detection nodes.
- Detector nodes have longer-lasting batteries than general sensor nodes.
- Detector nodes can intercommunicate through exclusive channel or other device.
- Detector nodes can act by promiscuous mode and watch all surrounding Routing Request/Reply messages.
- All sensor nodes have no mobility basically.

B. Network Initialization Phase

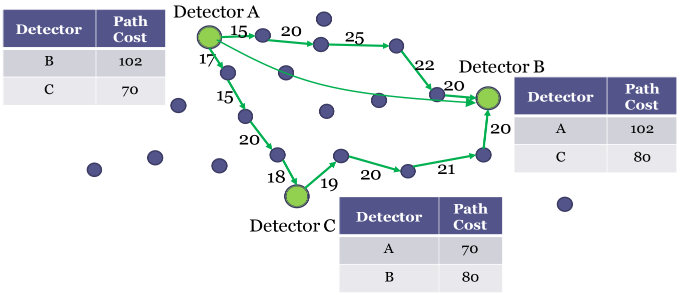
Each node calculates LQI value with neighborhood nodes at Network Initialization Phase. Each node calculates link cost by LQI value that was measured in communication with neighborhood node and keep smaller value comparing with previous link cost. If this process is repeated enough, each node can make minimum link cost table with neighborhood nodes. Fig. 3 shows minimum link cost table as an example. Minimum link cost table is used to detect attack when malicious node tries to change the routing path by sending very strong signal artificially.



Neighbor List	Minimum Link cost
B	34
C	78
D	33
E	75
F	50

Fig. 3 Example of Minimum Link Cost Table

Detector nodes perform following process additionally. Detector node searches surrounding detector nodes. And then, they records optimal path cost (accumulated link cost) between each detector node [7]. Fig. 4 shows that detector nodes search surrounding detector nodes and record minimum path cost.



Detector	Path Cost
B	102
C	70

Detector	Path Cost
A	102
C	80

Detector	Path Cost
A	70
B	80

Fig. 4 Example of Minimum Path Cost Table between detector nodes

C. Attack Detection Phase

Usually, LQI based Routing accumulates link cost of each routing path and calculates path cost. Then it selects route that have the smallest cost among them as the optimum path. Fig. 5 shows an example; path cost of optimal path is 204. But path cost of path that via sinkhole node is 249. Therefore, packet transfers following optimal path.

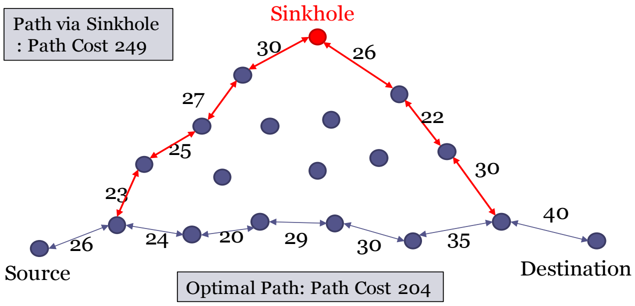


Fig. 5 Path cost between two nodes

In this situation, malicious node accomplishes sinkhole attack as follows:

Method 1: Transmit Routing Request/Reply packet abnormally strong so that neighborhood nodes may recognize that link quality is very good

Method 2: During Route Discovery phase, changes the LQI to the smallest value.

If malicious node uses these methods, it can perform sinkhole attack successfully. Fig. 6 shows an example; if malicious node uses above method, sinkhole attack can be successful because the modified total path cost is 201. However the original value is 249.

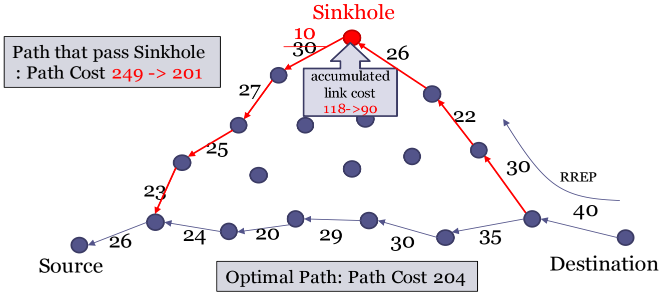


Fig. 6 Path cost when Sinkhole attack is attempted

To detect this attack, two methods are available.

For Method 1: When malicious node forges and sends routing request/reply message, receiving node refers minimum link cost table and examines strength of signal.

$$LinkCost_{cur} < LinkCost_{min} \times C \qquad (1)$$

Here, C means tolerance extent of the received signal. If above condition is found to be true, neighbor node can judge that message is forged.

For Method 2: If malicious node forges accumulated link cost in routing request/reply message, detection is impossible by the above first method. In this case, it can detect attack by using detector node. Detector nodes watch all routing reply messages in its range. In case of sinkhole attack, forged routing reply message is collected by surrounding detector nodes. Routing Reply packet is suitable for detection because RREP packets are uni-casted not broadcasted as RREQ.

$$Increment\ of\ LinkCost < PathCost_{DD} - LinkCost_{DN} \quad (2)$$

- Increment of LinkCost : Increment of accumulated link cost in routing reply message
- $PathCost_{DD}$: Minimum path cost between detector nodes
- $LinkCost_{DN}$: Link cost between detector node and node that send routing reply message

If the condition in 2 is true, it means that RREP message is transferred to better path than recorded optimum path. As a consequence, its result becomes false. Therefore, detector nodes able to find the sinkhole attack. For instance, in the Fig. 7, detector nodes observe accumulated link cost in RREP message which is transmitted from the neighbor nodes. The detector node I collects RREP message from the node A and the detector node II collects RREP message from the node B.

The accumulated link cost increment in that observed RREP messages of detector node I and II shows the path cost between node A and B; where the incremented value is 30(100-70=30).

On the other hand, in the network initialization phase, calculated minimum path cost between Detector node I and II is 102. And minimum link cost between Detector node I and A is 15. In addition, minimum link cost between Detector node II and B is 20. So minimum path cost between node A and B is 67(102-15-20=67) based on the calculated minimum path cost. As a consequence, if path cost which is calculated between node A and B is smaller than the minimum path cost, it is considered as an attack.

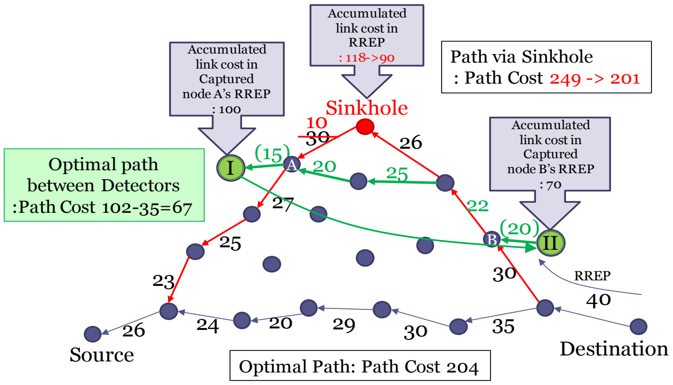

Accumulated link cost in Captured node A's RREP : 100
Accumulated link cost in RREP : 118->90
Path via Sinkhole : Path Cost 249 -> 201
Sinkhole
10
~~30~~
26
(15)
I
A
20
25
Optimal path between Detectors :Path Cost 102-35=67
Accumulated link cost in Captured node B's RREP : 70
27
22
(20)
B
II
25
23
30
RREP
40
26
24
20
29
30
35
Source
Destination
Optimal Path: Path Cost 204

Fig. 7 Example of sinkhole attack detection

IV. SIMULATION RESULTS

In order to verify the detection probability and false positive, we simulated our proposal. Our simulation is conducted over a 100m×100m rectangular flat space with randomly distributed sensor nodes. Table 1 presents the simulation environment.

Table 1. Simulation Parameters

Parameter	Value
Network Area	100m × 100m
Number of nodes	100
Transmission power	5.85e-5
Transmission range	15m
The number of Simulation	50

Fig. 8 shows False Positive rate with respect to tolerance extent C of formula 1. Fig. 8 also displays 5 trends according to degree of dispersion of variable link cost calculated in Detection Phase from minimum link cost calculated in Network Initialization Phase. Practical application need to adjust the constant C according to feature of node and environment of surrounding (radio noise and so on).

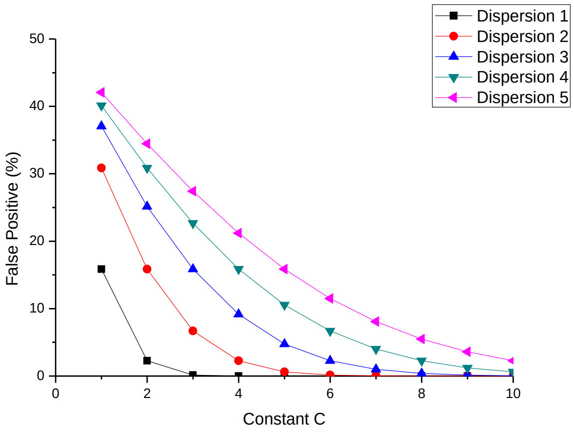


Fig. 8 False positive rate for Method 1

Fig. 9 shows the attack detection probability according to the number of detector nodes in case sinkhole node forges Routing Reply packet. Our proposed algorithm requires that detector node should be located between source node and sinkhole node and located between sinkhole node and destination node. Therefore, the attack detection rate is raised as density of detector node is higher. But, the attack detection rate does not get for 100% even if the number of detector nodes is enough. This is due to the fact that, sometimes there is no detecting node in the vicinity of sinkholes or source or destination nodes.

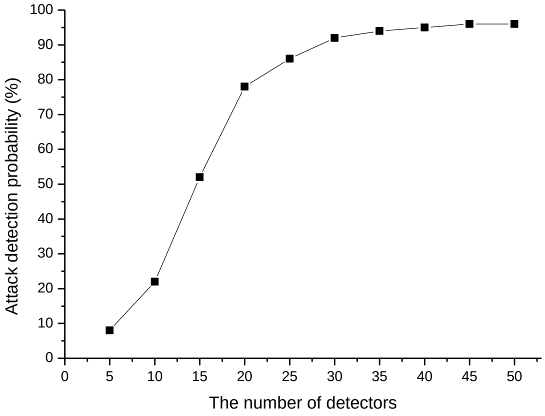


Fig. 9 Attack detection probability

V. CONCLUSION

Our proposal can detect sinkhole attack in wireless sensor network that uses LQI based routing. Our algorithm consists of network initialization phase and attack detection phase. Network initialization phase collects basic information for detection of sinkhole attack. General nodes collect minimum link cost between each neighborhood node. Detector nodes compute minimum path cost with surrounding detector nodes as well as link cost with each neighborhood node. In attack detection phase, we presented two attack detection methods according to the actions of malicious node. We use detector node and detect forgery of path cost in routing request message. And we detect abnormally strong signal by referring minimum neighbor link cost table.

ACKNOWLEDGEMENT

"This research was supported by the MKE under the ITRC support program supervised by the IITA"(IITA-2008-(C1090-0801-0016)).

Dr. CS Hong is corresponding author.

REFERENCES

[1] C. Karlof and D. Wagner, “Secure routing in wireless sensor networks: attacks and countermeasures,” Proc. First IEEE Int’l Workshop on Sensor Network Protocols and Applications, May 2003.

[2] C. Perkins, E. Belding-Royer, S. Das, “"Ad hoc On-Demand Distance Vector Routing,”" RFC 3561, July 2003.

[3] K. Kim, S. Daniel Park, G. Montenegro, N. Kushalnagar, "6LoWPAN Ad Hoc On-Demand Distance Vector Routing (LOAD)", Internet-Draft(Expired), June 19, 2007.

[4] IEEE Computer Society, “Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)”, IEEE 802.15.4 Standard, 2006.

[5] Edith C. H. Ngai, Jiangchuan Liu, Michael R. Lyu, "On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks", ICC 2006, Proceedings of the IEEE International Conference on Communications, Istanbul, Turkey, 2006.

[6] B. Yu, B. Xiao, “Detecting selective forwarding attacks in wireless sensor networks”, Proceedings of the Second International Workshop on Security in Systems and Networks (IPDPS 2006 Workshop), pp. 1-8, 2006.

[7] Ji-Hoon Yun, Il-Hwan Kim, Jae-Han Lim, and Seung-Woo Seo, "WODEM: Wormhole Attack Defense Mechanism in Wireless Sensor Networks", ICUCT 2006, LNCS 4412, pp. 200-209, 2007.