Journal Homepage: -www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI:10.21474/IJAR01/3226
DOI URL: http://dx.doi.org/10.21474/IJAR01/3226

*RESEARCH ARTICLE*

# NETWORK LIFETIME EXTENSION SCHEME USING MULTIPATH ROUTING IN FLOODING ATTACK DETECTION OF WIRELESS SENSOR NETWORKS.

**Won JinChung[1] and *Tae Ho Cho[2].**

1. College of Information and Communication Engineering, Sungkyunkwan University, Republic of Korea.
2. College of Software, Sungkyunkwan University, Republic of Korea.

## Manuscript Info

*Manuscript History*

Received: 19 December 2016
Final Accepted: 20 January 2017
Published: February 2017

***Key words:-***
Wireless sensor networks, Network security, Multipath routing

## Abstract

A malicious attacker can exploit a vulnerability of a sensor node within a wireless sensor networkto easily create a compromised node and attack the sensor network. The main purpose of a flooding attack, which is one kind of denial of service (DoS) attack, is to shorten the lifetime of the sensor network by exhausting the energy of the compromised node and of other sensor nodes along the path to the base station (BS).Existing security schemes to protect against flooding attacks do not take into account the amount of energy remaining in each sensor node. Therefore, in the case where the sensor network was installed long ago and its nodes have little remaining energy, such schemes are unsuitable because they are likely to completely drain individual nodes. In this paper, we propose a security scheme that includes multipath routing to reduce the load on each sensor node and thereby increase the sensor network lifetime. Experimental results herein confirm that the proposed scheme extends the network lifetime, increasing the energy efficiency of one sensor node included in the path by 40% compared with an existing scheme and reducing the number of exhausted sensor nodes by more than 60%.

## Introduction:-

A wireless sensor network (WSN) consists of a number of small sensor nodes that detect events and a base station (BS) that receives and analyzes data collected by the sensor nodes. WSNs are deployed in areas that are hardtoreach or where information needs to be received in real time. When a relevant event occurs in the region where the WSN is deployed, the sensor node located closest to the region is selected as the source node, and the event is detected. The source node collects the detected event information, generates an event packet, and transmits the event packet to the BS [1]. However, sensor nodes are vulnerable to attack because they have limited computing power, low energy, and use wireless communication. Using these vulnerabilities, an attacker can easily compromise a node. Using a compromised node, attackers can subject the sensor network to various attacks such as eavesdropping or other attacks that do not yield important event messages in the network. Typical attacks include denial of service (DoS), selective forwarding, sybil, sinkhole, and wormhole attacks [2-4]. Security techniques that can detect or prevent attacks continue to be studied. In this paper, we propose the energy efficiency of each node and the lifetime extension of the sensor network when a flooding attack, which is one kind of DoS, attacks the sensor network. The rest of this paper is organized as follows. Section 2 describes flooding attacks and multipath routing. Section 3

**Corresponding Author:- Tae Ho Cho.**
Address:- College of Software, Sungkyunkwan University, Republic of Korea.

explains the proposed scheme including multipath routing, and Section 4 presents experimental results and analysis of the existing and proposed schemes. Section 5presents our conclusions and future plans for this work.

## Related Works:-

### Flooding attack:-

WSNs are mainly deployed in open environments. Therefore, a malicious attacker can easily damage a sensor node and attempt various attacks on the sensor network using the compromisednode. The flooding attack, which is one kind of DoS attack, is an attack on the network layer of the sensor network. In a flooding attack, a continuous false event is generated to paralyze the network and exhaust the energy of the sensor nodes included in the path, thereby shortening the sensor network lifetime. In general WSN communication, when an event occurs, the sensor node closest to the event area collects data on the event and is selected as the source node. This source node creates a packet containing the event information, selects the shortest path to the BS, and sends the event through the network to the BS. However, in a flooding attack, the malicious attacker uses the compromised node to forward false event packets to the BS. The sensor nodes included in the path send and receive false event packets, thereby consuming energy continuously. The network lifetime is shortened when the energy of a sensor node included in the path is exhausted.

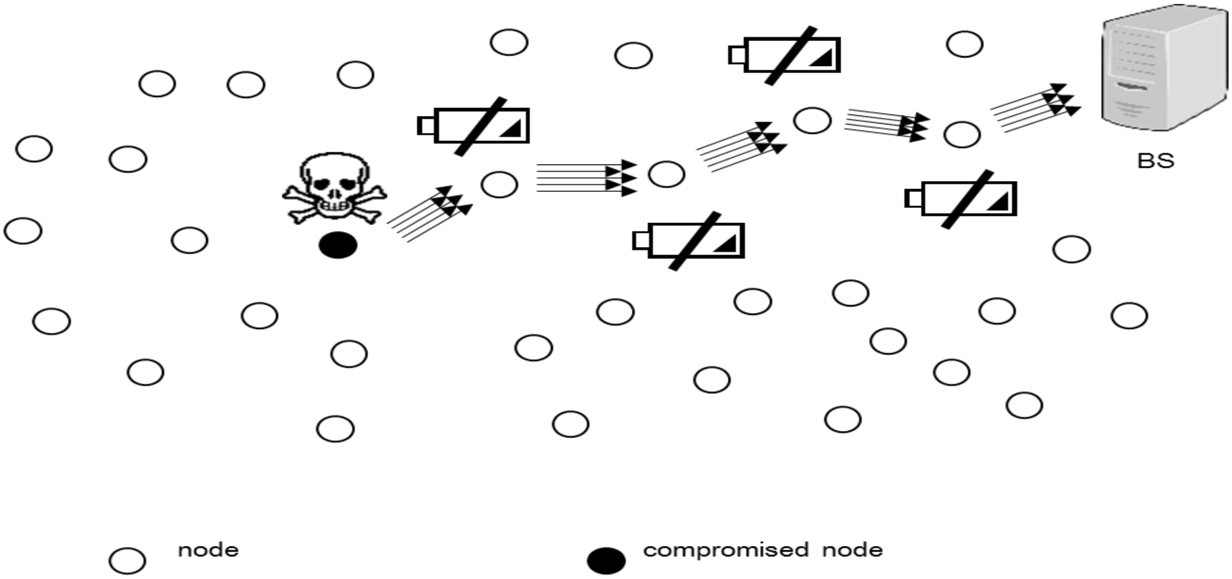

**Fig. 1:-**Flooding attack

After this, even if an important event occurs, a sensor node whose energy is exhausted due to a flooding attack may be included in the path but cannot transmit to the BS.

### Multipath routing:-

When single-path routing is used, the node included in the path set by the nature of the sensor network carries the load. For this reason, when a flooding attack occurs, the energy of the sensor node can be easily exhausted. One way to solve this problem is to use multipath routing [5-6]. Multipath routing is a method of establishing multiple available routes and forwarding packets to the BS.In this type of routing, packets are routed in a distributed manner that more evenly distributes the load among sensor nodes.In this way, the energy efficiency of each sensor node included in the path is increased, and the lifetime of the sensor network is extended.

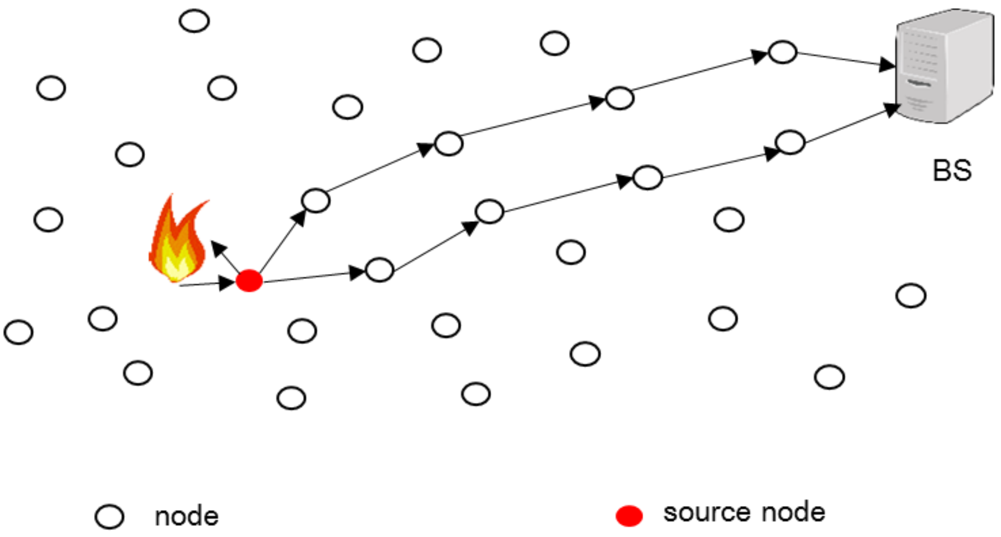

**Fig. 2:-**Multipath routing

Multipath routing configurations of sensor networks are divided into various types depending on the number of nodes arranged in the sensor field and their density. Typical multipath routing schemes are divided into three types: those based on node-disjoint paths, link-disjoint paths, and partiallydisjoint paths. In the node-disjoint path scheme, data is transferred using different paths. If a sensor node or link has a problem, only the path to which the corresponding node or link belongs is affected. In the link-disjoint path scheme, backup links exist, but all paths include at least one common sensor node in the path. The problem with this scheme is that the entire path can be affected when a problem occurs in that one common sensor node. Finally, in the partiallydisjoint path scheme, each data transmission path includes multiple paths resistant to the failure of any single node or link. Multipath routing can be more reliable than single-path routing but also has drawbacks. The number of hops may be greater than in the case of single-path routing. Thus, the network may consume more energy overall when multipath routing is used.

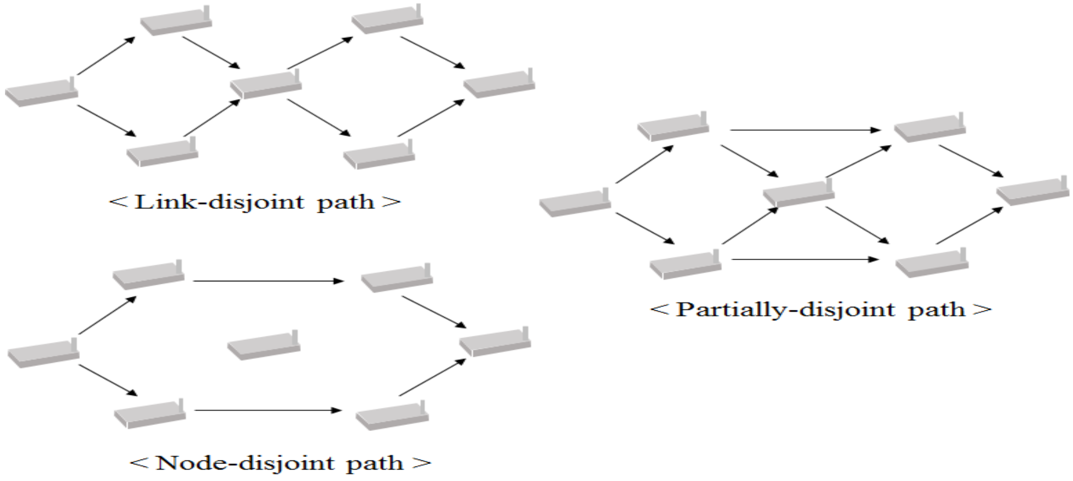

**Fig3:-**Multipath routing types

**Proposed Scheme:-**

When a WSN is subjected to a flooding attack, a large number of packets are transmitted to the BS, which can allow detection of the attack. However, because many packets are sent in a short time, the nodes in the path may consume a great deal of energy before verification can be completed at the BS. Once a WSN is configured, the sensor nodes are typically not recharged. Thus, the older is the WSN configuration, the less energy there is remaining in each sensor node. For this reason, we propose a multipath routing scheme to increase the energy efficiency of each sensor node and increase the lifetime of the sensor network. The proposed scheme compares the lifetime of the sensor network in aflooding attack occurring in single-path routing and multipath routing and the energy efficiency of the sensor node included in the path.

In the present work, we used a grid-based cluster routing environment to model single-path and multipath WSN routing schemes. The energy of each node in the sensor field was set to 1/100 of the initial energy of the sensor node to indicatethat the WSN configuration was out of date. Each node consumed 16.25 µJ and 12.25 µJper byte when transmitting and receiving, respectively. False event packets were large TinyOS packets of 29 bytes each [7].The chosen detection scheme adapted the algorithm of Flooding Attack Prevention (FAP) to detect a flooding attack in the ad-hoc network for use in the sensor network [8].

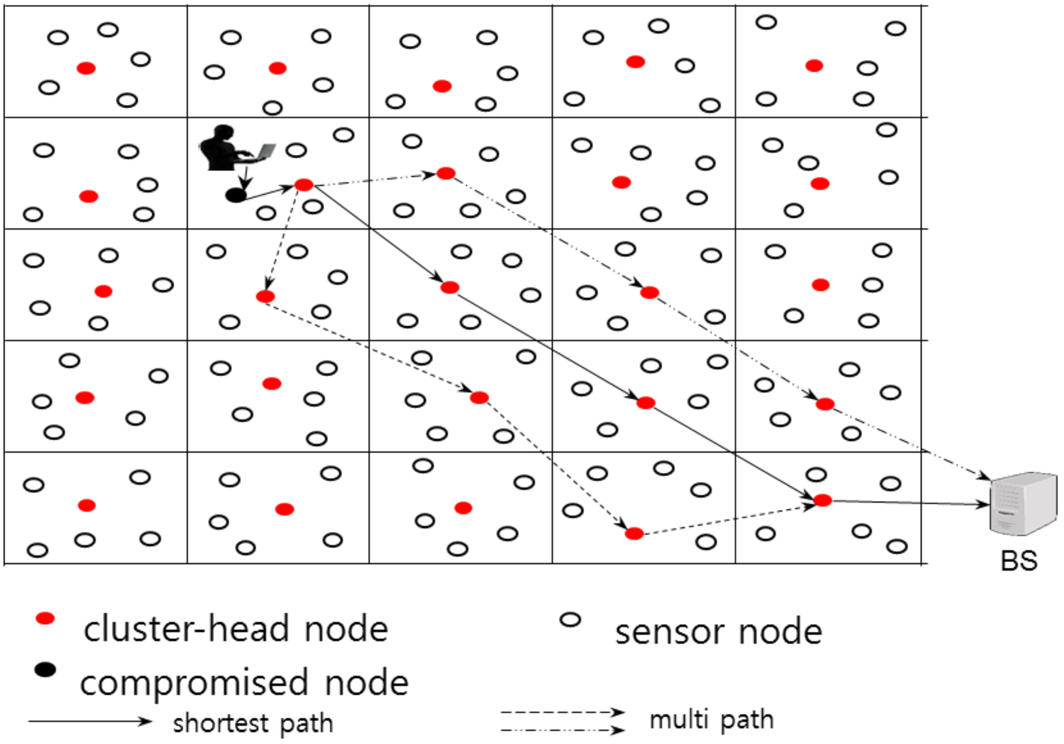

**Fig4:-** Flooding attack in multipath routing

```
Algorithm 1:-   Detection of flooding attack by the BS
    Step 1.     Collect events from the source node.
    Step 2.     Check the source ID in the cluster head node and compare it to source IDscontained in
                the blacklist.
    Step 3.     Check the forwarding time and source ID of the packet delivered to the BS.
    Step 4.     Increase the flooding attack count (FAC) if the previous and present packets equal source node
          IDs and the packet arrival times differ by 1 second or less.

Algorithm 2:-   Attack detection and blocking
    Step 1.     If the FAC exceeds a threshold value, this signals a flooding attack.
    Step 2.     The BS determines the node originating the attack, adds that node's ID to the blacklist,
          andforwards the blacklist to the cluster head node.
    Step 3.     The cluster head node receives the blacklist from the BS and drops transmissions from
          any source node on the list.
    Step 4.     The BS resets the FAC to zero.
```

Fig. 5 showsa flowchart of the overall algorithm.

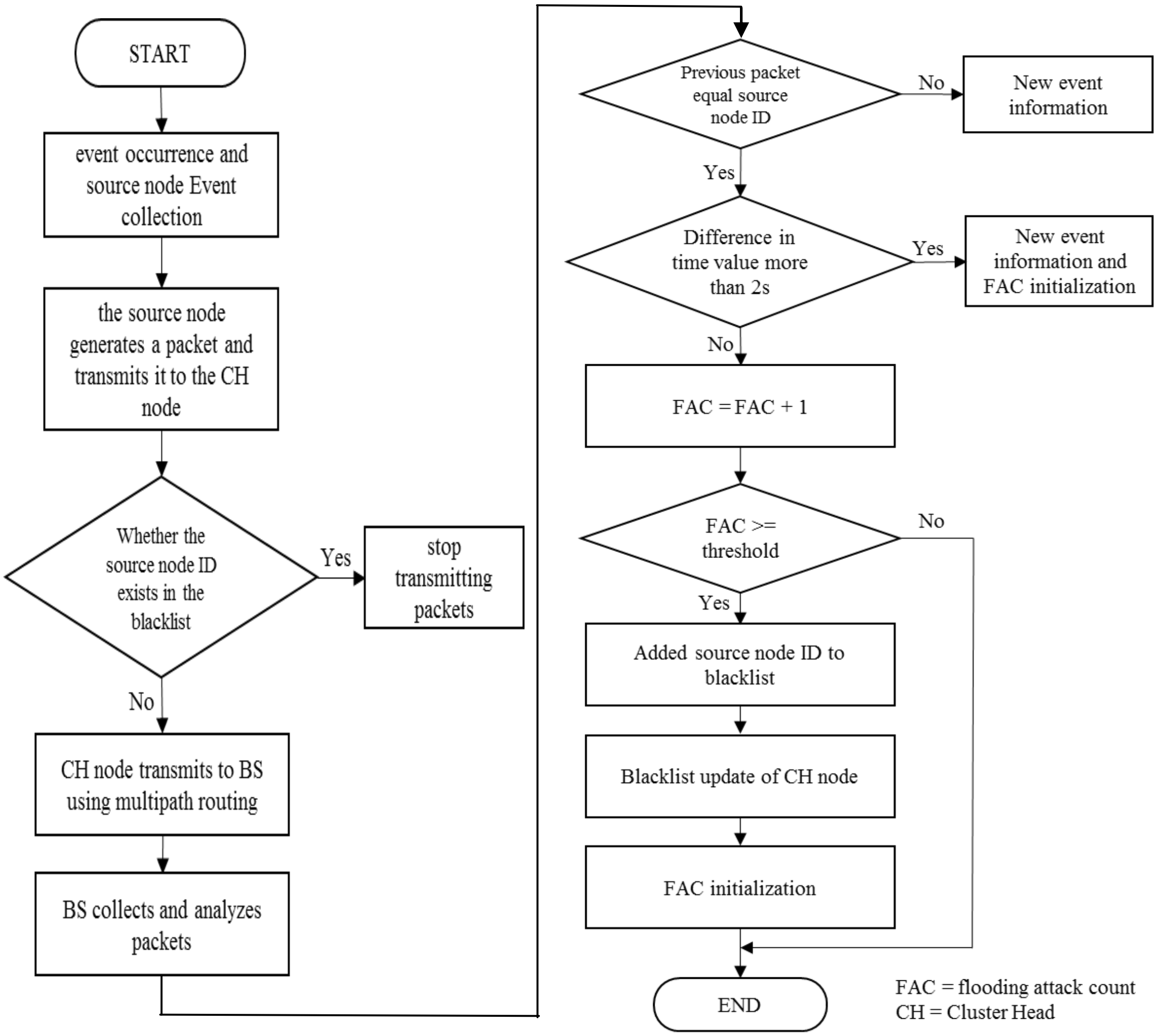
START
event occurrence and source node Event collection
the source node generates a packet and transmits it to the CH node
Whether the source node ID exists in the blacklist
Yes
stop transmitting packets
No
CH node transmits to BS using multipath routing
BS collects and analyzes packets
Previous packet equal source node ID
No
New event information
Yes
Difference in time value more than 2s
Yes
New event information and FAC initialization
No
FAC = FAC + 1
FAC >= threshold
No
Yes
Added source node ID to blacklist
Blacklist update of CH node
FAC initialization
END
FAC = flooding attack count
CH = Cluster Head

**Fig. 5:-** Algorithm flow chart

## Experimental Results:-

The proposed scheme was implemented using C++. Table 1 lists the parameters used in the experiments.

**Table 1:-**Sensor network parameters

| Item | Value |
|---|---|
| Sensor field size | 200 × 200 |
| Number of sensor nodes | 100 |
| Number of cluster head nodes | 25 |
| Sensor node type | Mica2 |
| Transmission range | 150m |

The FAC threshold of 15 was used in the experiments. Also, the probability of successful packet deliverywas set to 96%. The number of flooding attacks was set to 10, 20, and 30. The sensor network lifetime for each case was analyzed based on the results.

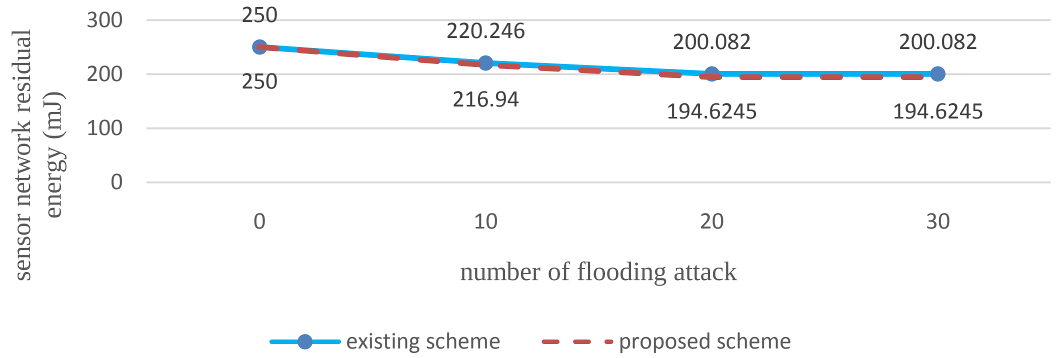

**Fig. 6:-**Sensor network residual energy after flooding attack

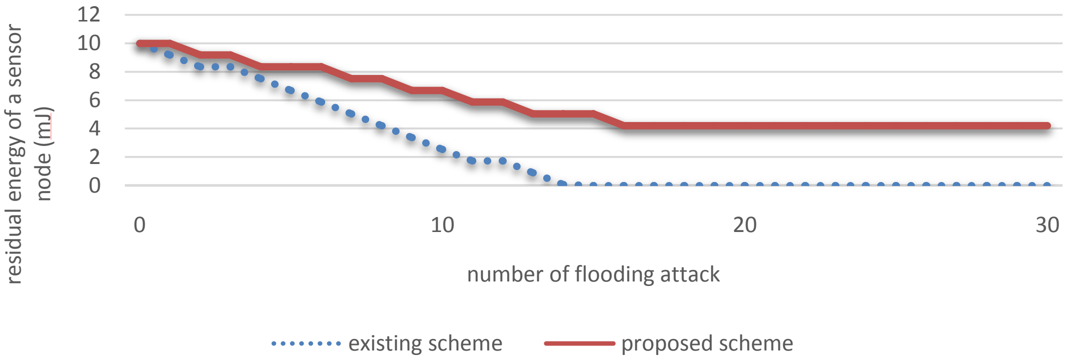

**Fig. 7:-**Residual energy of one sensor node included in the path after various numbers of flooding attacks

In the modeled flooding attack experiments, the proposed scheme consumedslightly more energy overall throughout the sensor network (Fig. 6). The reason for this is that more hops between the source node and the BS were used in the proposed multipath routing scheme. However, under the proposed scheme, the energy consumption was spread more evenly throughout the network. Thus, the proposed scheme avoided the exhaustion of some single nodes that would have been completely exhausted of energy under the existing scheme during an attack, and flooding attacks of 15 packets and more were detected and stopped, thereby avoiding further energy consumption (Fig. 7).

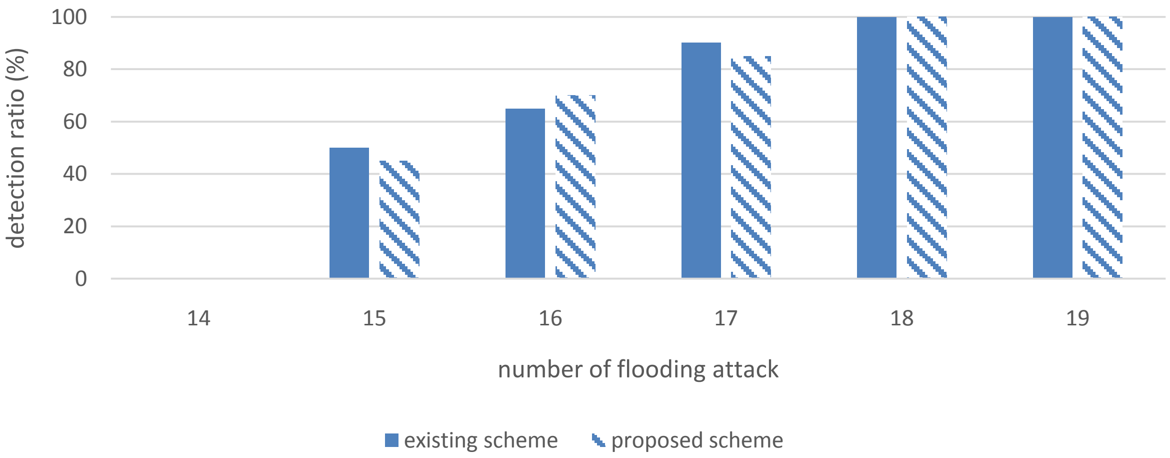

**Fig. 8:-** Flooding attack detection ratios

The existing and proposed schemes had similar attack detection ratios (Fig. 8). Both schemes detected all flooding attacks numbering 18 or more.

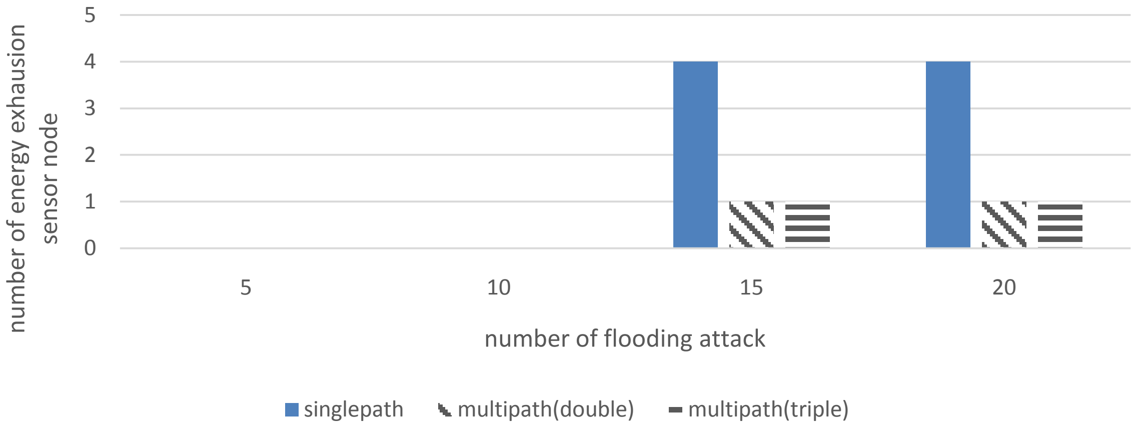

**Fig. 9:-**Number of exhausted sensor nodes after the flooding attack

Analysis of the experimental results showed that the energy of the cluster head node of the cell containing the compromised node was exhausted in the case applying proposed scheme. In the existing scheme, the proposed scheme includes depleted sensor nodes and additionally depletes the energy of the cluster head nodes included in the path. Therefore, the energy consumption of the sensor node is lower when the proposed scheme is used. The number of sensor nodes that are depleted of energy depends on the location of the compromised node. However, when comparing the existing scheme with the proposed scheme, the proposed scheme reduces the number of exhausted energy sensor nodes. The number of exhausted sensor nodes is the same when using either twopaths orthreepaths (Fig. 9); therefore, double path routing is sufficient for the present detection scheme. When the energy of a cluster head node is depleted, it is replaced with a sensor node having the mostenergy among thoseremaining in the cell. However, if the other sensor nodes in the cell have littleor no remaining energy, the cluster head nodes cannot be replaced. Therefore, other sensor nodes included in the path will be depleted of energy before the flooding attack is detected. Then, even if an important event occurs later, the sensor nodes will be exhausted and thus unable to transmit data.

## Conclusions:-

In this paper, we proposed a scheme to detect flooding attacks in WSNs, including multipath routing to reduce the load on sensor nodes and extend the network lifetime.In a flooding attack, an attacker uses a compromised node to transmit many false packets to the sensor network, depleting the energy of the sensor nodes included in the path to the BS and shortening the lifetime of the sensor network. Existing schemes to detect flooding attacks include the use of single-path routing, but this results in high energy consumption at individual nodes, which is a problem in old networks whose individual nodes have little remaining energy. The proposed scheme includes multipath routing to distribute the energy consumption among sensor nodes, increasing energy efficiency and thus the overall network lifetime. Future work is needed to reduce the energy consumption of the cluster head nodes located in the same cell as the compromised node and that of cluster head nodes located in other cells along the path to the BS.

## 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. NRF-2015R1D1A1A01059484)

## 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, pp. 293-315, 2003.
3. 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
4. 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
5. M. Radi, B. Dezfouli, K.A. Bakar and M. Lee, “Multipath routing in wireless sensor networks: survey and research challenges,” Sensors, vol. 12, pp. 650-685, 2012
6. J. N. Al-Karaki and A. E. Kamal, “Routing techniques in wireless sensor networks: a survey,” IEEE wireless communications, vol. 11, pp. 6-28, 2004
7. J. Deng, R. Han and S. Mishra, “Defending against path-based DoS attacks in wireless sensor networks” Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks, pp. 89-96, 2005
8. 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, pp. 410-416, 2006