DOI: http://dx.doi.org/10.26483/ijarcs.v8i9.5109

ISSN No. 0976-5697

Volume 8, No. 9, November-December 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

IMPROVING THE ENERGY EFFICIENCY OF FOG COMPUTING-BASED SYSTEM FOR SELECTIVE FORWARDING DETECTION IN MOBILE WIRELESS SENSOR NETWORKS USING MULTIPATH ROUTE

Won-Jin Chung
College of Information and Communication Engineering
Sungkyunkwan University
Suwon, Republic of Korea

Tea-Ho Cho
College of Software
Sungkyunkwan University
Suwon, Republic of Korea

Abstract: Selective forwarding attacks in mobile wireless sensor networks are difficult to detect because they selectively delete packets. Such attacks are more dangerous than selective forwarding attacks in wireless sensor networks because it is difficult to detect a selective forwarding attack that occurs on sensor nodes with high mobility. In order to detect such attacks, a fog computing-based selective forwarding attack detection technique has been proposed. However, in the ad hoc on-demand distance vector (AODV) routing scheme using a single path, all packets are dropped until a selective forwarding attack is detected. In addition, energy consumption for path re-setting is significant because sensor nodes move frequently. To solve this problem, we propose a selective forwarding attack detection method using an ad hoc on-demand multipath distance vector **(**AOMDV) routing technique. The proposed scheme increases the packet transmission probability to the BS and increases the energy efficiency of the sensor network. Experiments with the proposed method show that the energy efficiency of the sensor network is improved by about 10%.

Keywords: mobile wireless sensor network, selective forwarding attack, multipath routing, fog computing, network security

1. INTRODUCTION

Wireless Sensor Networks (WSNs) consist of a number of sensor nodes and a base station (BS). Since sensor nodes are low in value, a large number of sensor nodes are arranged in a wide area, and when an event occurs, it is sensed by a nearby sensor node [1]. The detected event information is transmitted to the corresponding sensor node using the routing information in the routing table. The sensor node communicates via wireless communication and eventually announces the event to the BS. In this way, WSNs are used in various fields such as military and industrial monitoring. However, when sensor nodes are concentrated in one zone, transmission of event packets to the BS can fail. Mobile Wireless Sensor Networks (MWSNs) are used to solve these problems [2]. The MWSNs is a special WSN in which the sensor nodes can move. Even if the sensor nodes are concentrated in one zone in the MWSNs, event packets can be transmitted to the BS due to movement of the sensor node. There is also a situation where a shaded area occurs in the WSNs. The shaded area is a problem in which sensor nodes around the event area fail to transmit events due to energy exhaustion. In MWSNs, the problem of the shaded area can be solved because the sensor nodes move. In addition, the static node used in WSNs consumes more energy than other sensor nodes because sensor nodes around the BS transmit all sensing data to the BS. However, in the MWSNs, when all the sensor nodes move around the BS, they transmit their sensed data to the BS, so that a large number of sensor nodes consume energy evenly. Therefore, mobile sensor nodes can load-balance better than static sensor nodes. Further, the movement of the sensor node reduces the probability of packet drop, since it reduces the number of hops delivered to the BS. However, MWSNs have disadvantages compared with WSNs. Because the sensor node uses a battery, it has limited energy, low computing power, and is usually deployed in an external environment that is not protected from attack [3]. Because of this problem, a malicious attacker can easily compromise a sensor node through Node Capture or Replication/ Clone Node Attack [4]. The movement of the sensor node makes it more difficult to detect the compromised node in the MWSNs than to detect the compromised node in the WSNs. The attacker attempts a selective forwarding attack using the compromised node. A selective forwarding attack is an attack that selectively deletes or transmits a packet when received by the compromised node [5]. This attack can be seen as a threatening attack in a military or hostile environment because important packets are lost. Selective forwarding attack detection based on fog computing is a technique to detect selective forwarding attacks using a fog server and watchdog in a MWSN environment [6]. However, since a single path is used, important packets are dropped during selective forwarding attack detection. In addition, since a mobile sensor node is used, frequent path resetting is performed. Therefore, energy consumption is significant when a single path is used. In this paper, we propose a method to solve the above problem by using multipath when detecting selective forwarding attacks. The contributions of the paper are as follows.

1. The use of multipath minimizes the number of packets that cannot be transmitted to the BS before detecting a selective forwarding attack, thereby increasing the probability of successful packet transmission to the BS.
2. Multipath increases the energy efficiency of the sensor network by reducing the sensor network energy consumption during the path re-setting process.

The composition of the paper is as follows. The following section describes the selective forwarding attack and detection scheme and the ad hoc on-demand multipath

distance vector (AOMDV) scheme, a multipath routing scheme. Section 3 describes the proposed scheme. Section 4 shows the experimental results of the proposed scheme. The final section explains conclusions and future research.

2. RELATED WORKS

A. *Selective forwarding attack*

Selective forwarding attacks occur at the network layer using compromised nodes or external electronic devices. When an event detection packet is transmitted from a sensor node that detects an event, if a compromised node is included in the path, a selective forwarding attack is attempted on the compromised node. Selective forwarding attacks are difficult to detect because they selectively drop packets to disrupt event notifications and selectively remove packets. If important event information that must arrive at the BS is blocked by a selective forwarding attack at the compromised node, it is exposed to the danger in areas where important packets are not received. Selective forwarding attack in MWSNs with sensor node mobility is more threatening than selective forwarding attack in existing WSNs. The reason is that the flexible path of the sensor node is established in MWSNs, unlike the path of the WSNs, where the position of the sensor node is fixed. Therefore, since the MWSN changes its path with time, the path often includes the compromised node. Therefore, the path including the compromised node is no longer attacked by the movement of the compromised sensor node, but the normal path is changed to one that includes the compromised node. Thus, a path that does not cause an attack in the WSNs might be attacked in the MWSNs, resulting in the possible loss of important packets. Therefore, it is difficult to detect a selective forwarding attack occurring in MWSNs. Figure 1 shows the selective forwarding attack occurring in MWSNs.

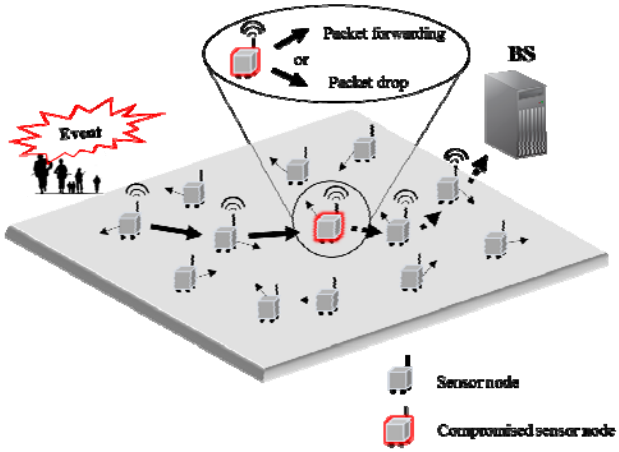

Figure 1. Selective forwarding attack

B. *Selective forwarding attack detection*

Selective forwarding attacks have been studied for a long time in WSNs, and a number of selective forwarding attack detection techniques using efficient algorithms have been discussed. However, selective forwarding attack detection techniques in WSNs do not consider the mobility of sensor nodes. Therefore, MWSNs that are free to move sensor nodes cannot use the selective forwarding attack detection technique used in WSNs. Because of this problem, a new MWSN detection scheme is needed. Qussai Yaseen et al. proposed fog computing-based selective forwarding attack detection [6]. This technique detects selective forwarding attacks in MWSNs using fog computing and watchdog. The watchdog is a selective forwarding attack detection technique used in WSNs. The watchdog monitors the packet transmission of the sensor node and measures the packet drop rate of the sensor node in the transmission range. It is a method to detect selective forwarding attack using the measured packet drop rate with watchdog. However, it is difficult to detect selective forwarding attack using only watchdog due to continuous changes in sensor node position. The monitored sensor node can move out of the monitoring range of the watchdog. Conversely, the movement of the watchdog can move out of the monitoring range of the monitored sensor node. In this case, the watchdog will no longer be able to measure the packet drop rate, causing problems in detection of selective forwarding attacks. To solve this problem, we used the fog computing system. Fog computing-based selective forwarding attack detection consists of a Cloud layer, Fog layer, and Sensor layer. Figure 2 shows a three-tiered view of fog computing-based selective forwarding attack detection.

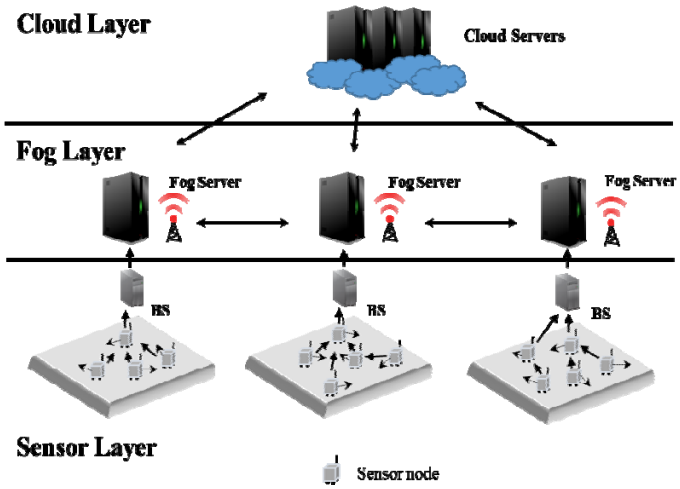

Figure 2. Fog computing based-selective forwarding attack detection

The most important of the three layers is the Fog layer. In the Fog layer, the information from the sensor nodes monitored by the watchdog is collected, and the information from the sensor nodes including reception of the monitored nodes and the transmitted packets is shared through the Fog server. Therefore, even if the monitored sensor node moves out of the monitoring range of the watchdog, the sensor node can be continuously monitored using another watchdog through the shared information on the Fog server.

C. *AOMDV*

The AOMDV routing scheme is an extended routing scheme that reduces packet loss by using multipath in the ad hoc on-demand distance vector (AODV) routing scheme [7][8]. AOMDV is stored as a route list to store multiple routes. Figure 3 shows the AODV and AOMDV routing tables.

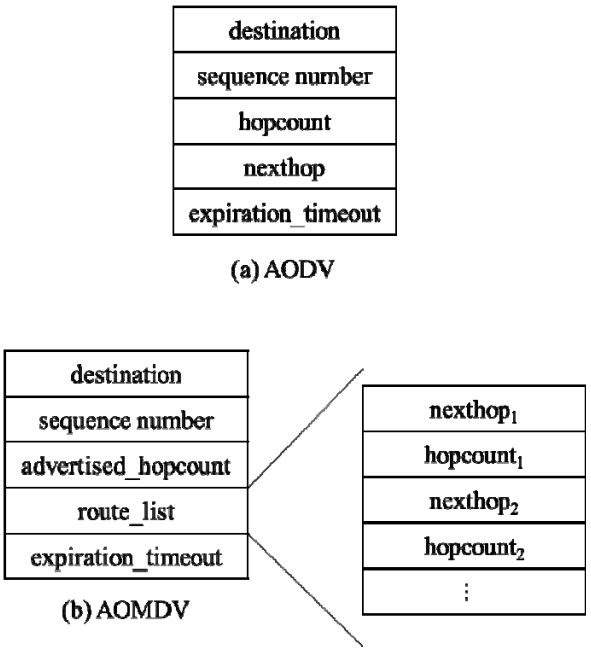

Figure 3. Structure of routing tables

The AODV routing scheme sets the path from the source node to the destination node using the route request (RREQ) packet and the route reply (RREP) packet. The source node floods the RREQ packet and transmits it to the destination node through the intermediate nodes. The destination node that receives the RREQ packet sets the route with the least number of hops from the source node as the valid route and sets the route by transmitting the RREP packet in the reverse direction through the set route. In the routing process, the intermediate node can overlap the flooded RREQ packet, and the AODV routing scheme includes a process for deleting the redundant RREQ packet. However, the AOMDV routing scheme does not delete the packet to establish the multipath when receiving the duplicated RREQ packet in the intermediate node. Then, when the RREQ packet is transmitted to the destination node, the destination node transmits the RREP packet through the reverse path. The method of routing is shown in Figure 4 and Figure 5.

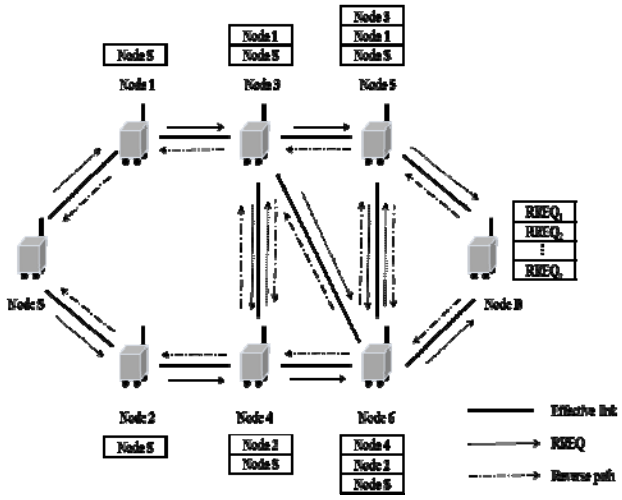

Figure 4. Routing path detection-1 (RREQ)

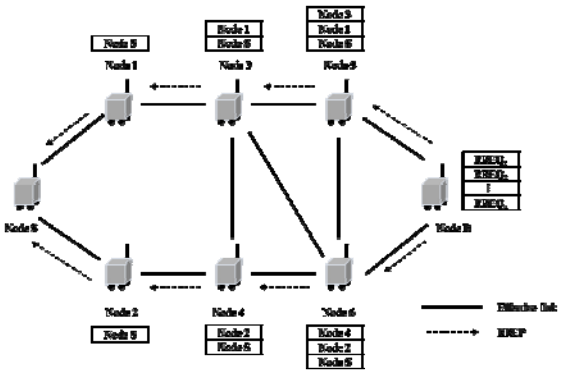

Figure 5. Routing path detection-2 (RREP)

In this way, the node has a multipath. The AOMDV routing scheme can reduce the energy consumption for path re-setting because the packet is transmitted using a different path without re-setting when a packet transmission problem occurs in the path. This is because, unlike the AODV routing scheme, which requires path re-setting every time a problem occurs in the path, the AOMDV routing scheme re-sets the path only when all the paths contain a problem.

3. PROPOSED SCHEME

D. Motive

The fog computing-based selective forwarding attack detection scheme is dropped before a packet is transmitted to the BS until a selective forwarding attack is detected. Even when an important packet needs to be transmitted, a packet drop occurs. Therefore, important packets must be delivered to the BS without being dropped. Another problem is that of energy. Because of the movement of the sensor node, the path is changed from time to time, and a path re-setting process through route re-search is necessary. In this case, MWSNs composed of sensor nodes with low energy experience a fatal problem to the sensor network energy factor. Therefore, in order to solve the above problem, the proposed scheme will introduce a multipath technique. The fog computing-based selective forwarding attack detection method is an AODV routing method that uses a single path. In this paper, we propose a technique to detect the selective forwarding attack that solves the above problem using AOMDV routing techniques with multipath.

E. Assumptions

Selective forwarding attack occurs only in a MWSN environment, and other attacks do not occur simultaneously with selective forwarding attack. Also, the Fog server is not attacked.

F. The Proposed Scheme

The fog computing-based selective forwarding attack detection method is based on an AODV routing technique using single path. When a single path is used, important packets might be dropped when a selective forwarding attack occurs. Also, since a mobile sensor node is used, the path is frequently changed. As the path changes, the sensor network energy for path re-setting is continuously consumed. In order to overcome these drawbacks, we propose a technique to detect selective forwarding attack using an AOMDV routing technique that uses multipath instead of the AODV routing method, which uses a single path. Figure 6 is an overall flowchart of the proposed scheme.

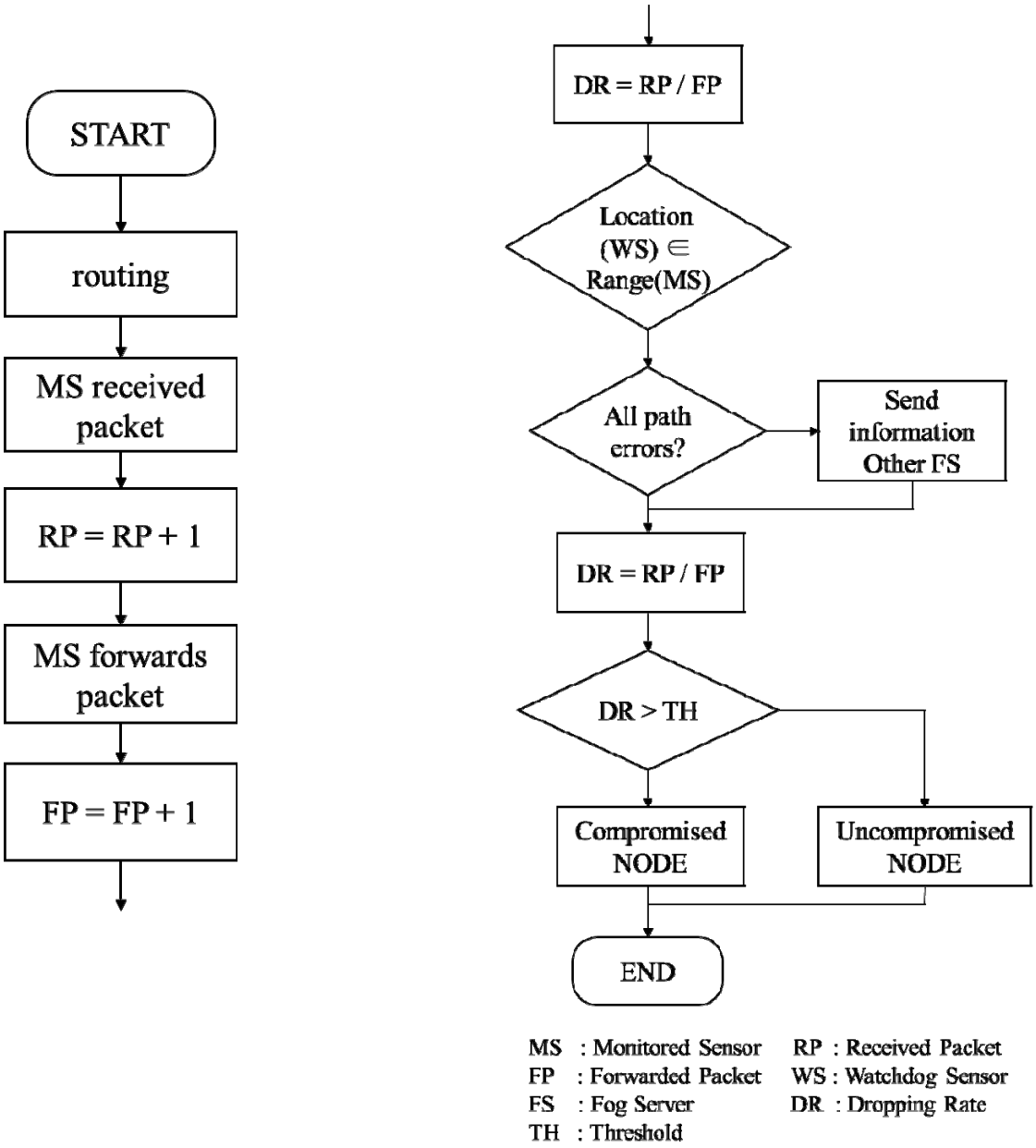

Figure 6. Flow chart of the proposed scheme

The proposed scheme computes the transmitted and received packets of the monitored sensor node through the watchdog. If the path changes due to the movement of the sensor node over time, check whether all paths are connected to the watchdog. In the case of the existing scheme, the monitored sensor node can be continuously monitored through the fog server when the monitored node is out of the monitoring range of the watchdog. The proposed method adds a process for checking whether a watchdog is connected, so that the monitored sensor node can monitor through other paths even if it is out of the monitoring range of the watchdog. Afterward, the packet drop rate is calculated and compared to the threshold value. If the packet drop rate is greater than the threshold value, it can be regarded as a selective forwarding attack. When using a single path in the selective forwarding attack detection scheme, all packets are dropped until the attack is detected. However, the proposed technique has minimized this case. If a packet is dropped in one path, it is transmitted through another normal path. This consumes more energy than a single path, but can deliver packets securely to the BS. In addition, since multiple packets are transmitted in this process, if a path containing a damaged node is overlapped in a packet transmission process, a selective forwarding attack can be detected faster than a detection method using a single path. The AOMDV routing scheme using multipath routing consumes more routing energy than the AODV routing scheme that uses a single path because it constructs multiple routes in the initial routing configuration. However, the AOMDV routing scheme re-sets the path only when all the paths in the routing table are having a problem. Therefore, compared with AODV, overhead for path re-setting and energy consumption can be reduced. In the selective forwarding attack detection method, the sensor node moves out of the transmission range frequently. In this case, the sensor node re-sets the path by re-searching the path. The fog server should then pass the information on the sensor nodes monitored by the watchdog to the next fog server. In this process, sensor network energy is continuously consumed. In the proposed scheme, energy

consumption can be reduced through the multipath method. When the monitored sensor node is outside the transmission range, the path set in the AOMDV routing table is set to *k*, so the path re-set probability is reduced to 1 / *k*. Therefore, it is possible to send information to the fog server until the path is re-set.

4. EXPERIMENTAL RESULTS

The sensor field size used to test the proposed scheme is 300 X 300 (m^2), and the number of sensor nodes is 200. The experiment uses C ++ language in Visual Studio, simulates a MWSN environment with a selective forwarding attack and detection technique through a program. The number of initially deployed sensor nodes is evenly distributed in nine zones, and the locations are randomly dispositioned. The initial energy of the sensor node is randomly set within a range not exceeding 1 J. Three BSs and three fog servers receive sensor node information. When the sensor node moves, the speed is set to [0, V_{max}] km / h, and the direction is set to [0, 2π] because the speed varies depending on the model of the sensor node. In the selective forwarding attack detection method, the threshold is set to 15. The number *k* of multipaths in AOMDV is set to 3, which was set in the AOMDV related paper [9]. Each packet transferred to the sensor node requires 12.25 μj of energy, and each packet received by the sensor node requires 16.25 μj [10].

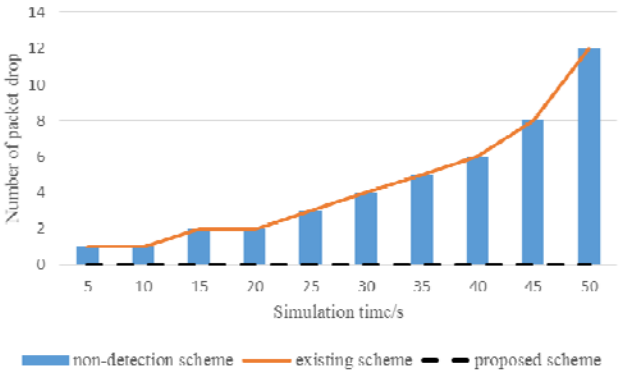

Figure 7. Number of packet transmission failures to BS (V_{max} = 20)

Error!

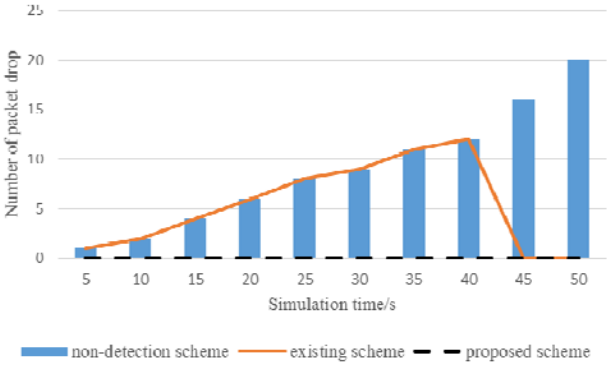

Figure 8. Number of packet transmission failures to BS (V_{max} = 40)

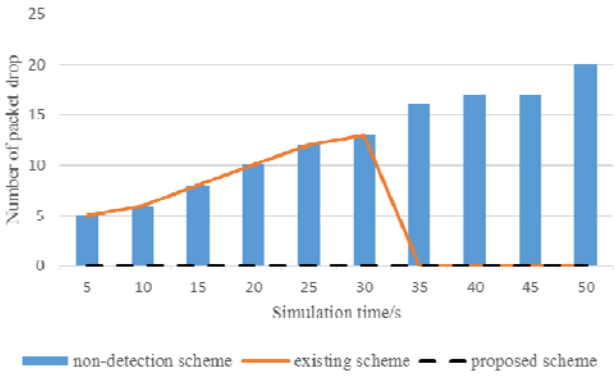

Figure 9. Number of packet transmission failures to BS (V_{max} = 60)

Figure 7 to Figure 9 show the packet transmission success rate to the BS according to node speed. Selective forwarding attack detection using a single path drops packets during an attack until the attack is detected. In the above figure, when the packet drop rate is greater than the threshold value of 15, the existing scheme detects the selective forwarding attack and the drop rate becomes zero. In the proposed scheme, not only the drop rate of the packet is calculated, but also the packet is transmitted to the BS securely because the packet is transmitted through the normal path. In the experiment, the proposed scheme detects the event and confirms that the probability of packet delivery failure to the BS is 0%.

Error!

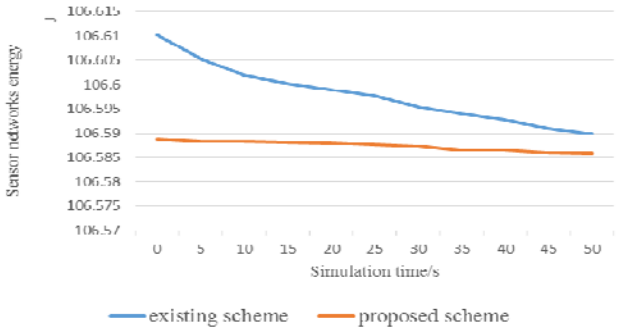

Figure 10. Sensor network energy efficiency (V_{max} = 20)

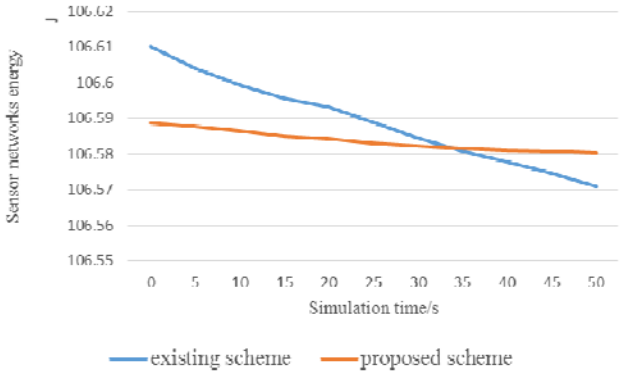

Figure 11. Sensor network energy efficiency (V_{max} = 40)

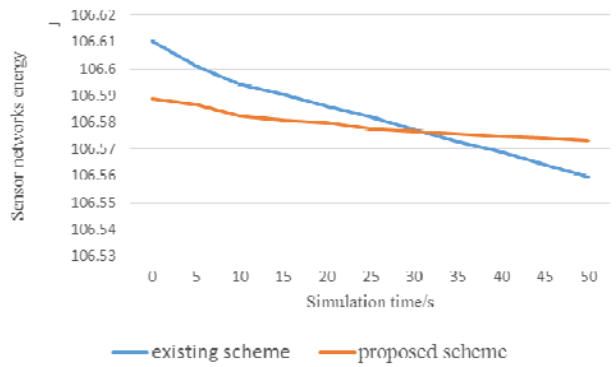

Figure 12. Sensor network energy efficiency (V_{max} = 60)

Figure 10 to Figure 12 show the network energy consumption of the MWSNs. Since the initial energy sets multiple paths in the proposed scheme, it consumes more energy than the existing scheme. However, as time passes, the proposed scheme can confirm that less energy is consumed. Also, since the path is frequently re-set as the speed increases, the proposed scheme consumes less energy than the existing scheme. Therefore, the proposed scheme improves the energy efficiency of the sensor networks over time. For example, if the speed is 60 km / h and the time is 50 seconds, the proposed scheme increases the network energy efficiency by about 10% compared to the existing scheme.

5. CONCLUSIONS

The fog computing-based selective forwarding attack detection technique is an efficient technique to detect selective forwarding attack in MWSNs. However, since the fog computing-based selective forwarding attack detection method uses a single path, packets are dropped due to attack until the selective forwarding attack is detected, resulting in the possible loss of an important packet. In addition, the energy consumption of the sensor node is large because path re-setting is frequently performed with ample movement of the sensor node. In order to solve this problem, we propose a selective forwarding attack detection method based on fog computing using multipath routing. Even if a packet is dropped in a path where a selective forwarding attack occurs, the packet is transmitted along a different path using a multipath routing technique. In AODV, which uses a single path, path re-setting is performed whenever a path problem occurs. However, AOMDV using multipath routing does not re-set the path until a problem occurs in all paths set in the routing table. Therefore, there is less overhead for path re-setting and less energy consumption. However, multipath routing uses significant energy to set up multiple paths. Also, it is difficult to detect selective forwarding attack by packet drop rate using watchdog when another layer such as jamming attack simultaneously attacks. Therefore, future research will propose a new detection technique that can detect selective forwarding attacks when attacks of different layers occur at the same time.

6. ACKNOWLEDGMENT

This research was supported by the MISP (Ministry of Science, ICT & Future Planning), Korea, under the National Program for Excellence in SW) (2015-0-00914) supervised by the IITP (Institute for Information & communications Technology Promotion)"(2015-0-00914)

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. Zhu, et al. "A survey on communication and data management issues in mobile sensor networks", Wireless Commun. Mobile Computing, vol. 14, no. 1, pp. 19-36, 2014.
[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] G. Padmavathi and D. Shanmugapriya, "A survey of attacks, security mechanisms and challenges in wireless sensor networks", International Journal of Computer Science and Informtation Security (IJCSIS), vol. 4 issue 1, 2009.
[5] 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
[6] Q. Yaseen, F. AlBalas, and Y. Jararweh, "A fog computing based system for selective forwarding detection in mobile wireless sensor networks". Foundations and Applications of Self* Systems, IEEE International Workshops on. IEEE, 2016.
[7] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc on-demand distance vector (AODV) routing," IETF RFC 3561, 2003
[8] M. Marina and S. Das, "On-demand multipath distance vector routing in ad hoc networks", IEEE International Conference on Network Protocols (ICNP), pp. 14–23, 2001.
[9] A. Nasipuri, R. Castaneda, and S. R. Das, "Performance of Multipath Routing for On-demand Protocols in Mobile Ad Hoc Networks," ACM/Kluwer Mobile Networks and Applications(MONET), Volume 6, Issue 4, pp. 339-349, 2001.
[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