A MULTI-PATH ROUTING DETERMINATION METHOD FOR IMPROVING THE ENERGY EFFICIENCY IN SELECTIVE FORWARDING ATTACK DETECTION BASED MWSNS

Won Jin Chung[1] and Tae Ho Cho[2]

[1&2]Department of Electrical and Computer Engineering, Sungkyunkwan University, Suwon, Republic of Korea

ABSTRACT

A selective forwarding attack in mobile wireless sensor networks is an attack that selectively drops or delivers event packets as the compromised node moves. In such an attack, it is difficult to detect the compromised node compared with the selective forwarding attack occurring in the wireless sensor network because all sensor nodes move. In order to detect selective forwarding attacks in mobile wireless sensor networks, a fog computing-based system for a selective forwarding detection scheme has been proposed. However, since the proposed detection scheme uses a single path, the energy consumption of the sensor node for route discovery when the sensor node moves is large. To solve this problem, this paper uses fuzzy logic to determine the number of multi-paths needed to improve the energy efficiency of sensor networks. Experimental results show that the energy efficiency of the sensor network is improved by 9.5737% compared with that of the existing scheme after 200 seconds when using the proposed scheme.

KEYWORDS

mobile wireless sensor networks, selective forwarding attack, network security, fuzzy logic, AOMDV routing protocol

1. INTRODUCTION

Wireless sensor networks (WSNs) are composed of many small sensor nodes that detect temperature, humidity, vibration, etc., and a base station (BS) that collects detected event data [1][2]. Since the price of the sensor node is low, it is possible to arrange many sensor nodes in a large area. The deployed sensor node senses an event and transmits a packet including event information to the BS through a set path. In this way, WSNs are used in various fields such as battlefields, military and industrial monitoring, and smart cities. However, there are also problems with WSNs [3]. First, WSNs are sometimes deployed in hostile territories. In this case, the sensor nodes are randomly placed through the aircraft. Randomly placed sensor nodes may not be able to cover all of the areas that they want to sense. Second, the sensor node is energy limited, so if many sensor nodes are depleted of energy, the area becomes a coverage hole. Since the position of the sensor node is fixed once it is deployed, a new sensor node must be placed in order to sense the coverage hole. Finally, in order to sense a moving object, the sensor node should be placed in the moving direction. However, since the sensor nodes are randomly placed, there is no guarantee that there is a sensor node in the direction that the object is moving. Mobile wireless sensor

DOI: 10.5121/ijwmn.2018.10402

networks (MWSNs) have been proposed to solve these problems [4][5]. Figure 1 shows how MWSNs detect the occurrence of an event.

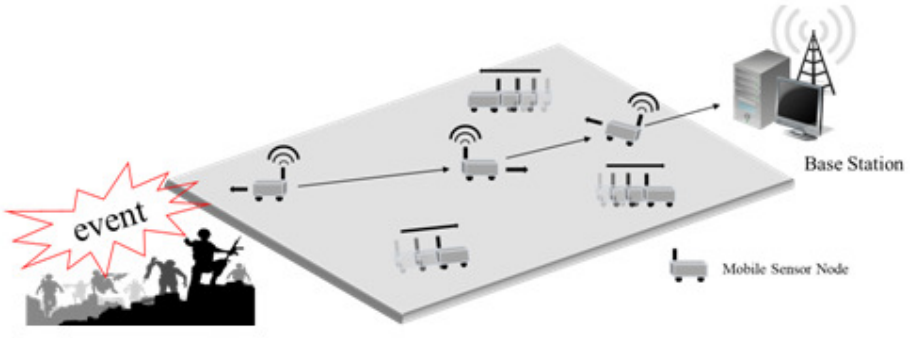

Figure 1. Mobile wireless sensor networks

MWSNs are special WSNs with sensor nodes that are in motion. The MWSNs solve the coverage hole problem when the mobile sensor node moves. In addition, since the number of hops is reduced due to the movement of the sensor node, the packet transmission success probability is higher than the packet transmission success probability of the static sensor node. In WSNs, the sensor nodes around the BS receive the packets intensively, so they consume more energy than the sensor nodes in other regions. In MWSNs, this problem is solved by the movement of the sensor nodes. The movement of the sensor node can load balance the sensor node because the data transmission is not concentrated, as is the case for a static sensor node around the BS. However, MWSNs also have a disadvantage in that they are placed in low computing power areas with limited energy in the external environment of the sensor node. Therefore, an attacker can attempt node capture or a clone node attack to compromise sensor nodes deployed at key facilities. The attacker can then use a compromised node to attempt various attacks such as selective forwarding attacks, wormhole attacks, sinkhole attacks, and cybil attacks [6][7]. Among the various kinds of attacks, selective forwarding attacks are attacks that selectively drop or deliver packets forwarded through the compromised node. In the case of selective forwarding attacks in MWSNs, it is difficult to detect compromised nodes due to the movement of all the sensor nodes. This paper uses a fog server-based system for selective forwarding detection to detect such attacks. However, since this detection method uses a single-path ad-hoc on-demand distance vector (AODV) for its routing protocol, the energy efficiency of the sensor node is degraded when route discovery is used in frequent MWSNs [8]. In addition, when the ad-hoc on-demand multipath distance vector (AOMDV) routing protocol is used to solve this problem, unnecessary multi-path routing degrades the energy efficiency of the sensor network [9]. Therefore, the proposed scheme improves the energy efficiency of the sensor network by determining the number of multi-paths using fuzzy logic. The composition of this paper is as follows. Section 2 describes the selective forwarding attack and detection scheme and the AOMDV routing protocol. Section 3 describes the proposed scheme. Section 4 shows the performance of the proposed scheme through experiments. Finally, Section 5 presents conclusions and future research.

2. RELATED WORKS

The section describes the selective forwarding attack, selective forwarding attack countermeasure, and AODMV routing protocol.

2.1. Selective Forwarding Attack

A selective forwarding attack occurs through a compromised node or an external electronic device. When an event occurs, the sensor node that detects the event generates an event notification packet and delivers it to the BS. The selective forwarding attack selectively passes or drops event packets from the compromised node when the event notification packet passes the compromised node. In a military confidential or battleground environment where an event notification packet must be reached, an attacker attempts a selective forwarding attack through a compromised node. If an attack occurs in an area where an event notification packet must be reached, event packets may be selectively reached, which may cause confusion. While selective forwarding attacks occur in both WSN and MWSN environments, selective forwarding attacks occurring in MWSNs are treated as more threatening attacks [10]. The reason is that all sensor nodes move, as the MWSNs form a mobile environment. In a mobile environment, compromised nodes are difficult to detect because they can move and attempt selective forwarding attacks in various areas. Figure 2 shows a selective forwarding attack occurring in an MWSN environment.

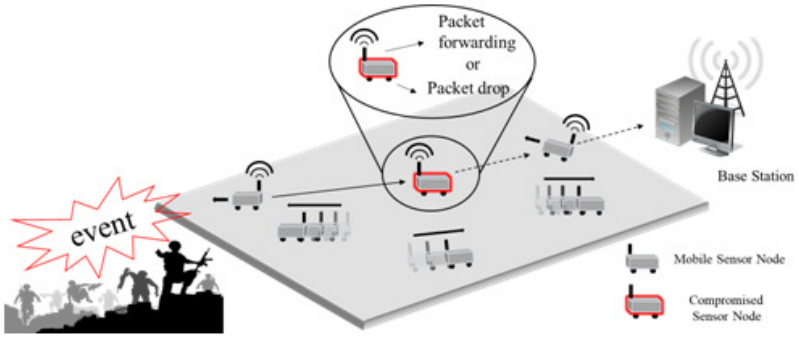

Figure 2. Selective forwarding attack

2.2. Fog Computing-based System Selective Forwarding Detection

Many types of research have been conducted to detect selective forwarding attacks. However, most research involves schemes for detecting selective forwarding attacks in WSN environments using static sensor nodes. These detection schemes are difficult to apply in MWSNs. Q. Yaseen proposed a fog computing-based selective forwarding detection scheme to detect selective forwarding attack in mobile environments [10]. The detection scheme is a technique that uses a watchdog that was used to detect selective forwarding attacks in WSNs. The watchdog monitors the transmission of the sensor node and measures the packet drop rates within the transmission range of the sensor node to detect whether a selective forwarding attack occurs. When using the watchdog, it is necessary to continually measure the packet drop rates within the transmission range of the sensor node. However, it is difficult to apply this technique in the MWSN environment in which the sensor node moves. This is because when the sensor node moves, the transmission range of the sensor node is out of range. A fog computing-based system for selective forwarding detection solves this problem by using a fog server. A selective forwarding attack detection scheme consists of three layers, as shown in Figure 3.

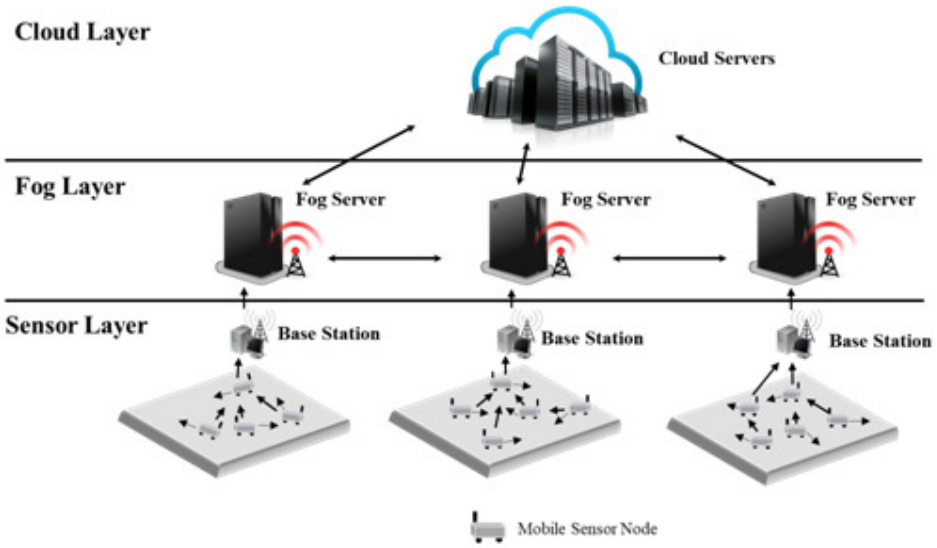

Figure 3. Fog computing-based system for the selective forwarding detection scheme

The cloud computing layer is used for data mining and management purposes and is used to analyze the intrusion patterns of attacks. The fog layer is a virtualization platform that provides a variety of services. The fog layer is the most important part of the fog computing-based system for selective forwarding attack detection. The fog server configured in the fog layer collects information monitored by the watchdog. Since the fog server must be continually monitored by the watchdog to detect the compromised nodes, the fog servers exchange the monitoring information of the sensor nodes in cooperation with each other. In addition, the fog server analyzes the information monitored by the watchdog and performs voting to distinguish it as either a normal node or a compromised node. Finally, at the wireless sensor layer, the sensor node consists of an IDS that monitors the forwarding packets (FP) and receives the received packets (RP). Thus, a fog computing-based system for selective forwarding attack detection can detect selective forwarding attacks occurring in MWSNs.

2.3. AOMDV Routing Protocol

The AOMDV routing protocol is a special routing protocol that sets and routes multi-paths in the AODV routing protocol. The AODV routing protocol initiates a route discovery process when the source node needs to route to the destination node. Route discovery floods a route request (RREQ) packet at the source node, and when the RREQ packet is received at the destination node, the route is set by sending a route reply (RREP) packet in the reverse direction. A number of intermediate nodes between the source node and the destination node send RREP packets only to valid paths, and otherwise, flood the RREQ packets to find the route. In the AODV routing protocol, maintenance of routes is done through route error (RERR) packets. If a path failure occurs, it must be reset to a new path. Rerouting removes the failed path using the RERR packet and sets the path through a new RREQ packet. Since the sensor node moves in the MWSNs, many path failures occur, and a new path reset is required through the RERR packet and the RREQ packet. However, since the sensor node is energy limited, if rerouting due to the movement of the sensor node continues, the energy efficiency of the sensor node is degraded. Therefore, an AOMDV routing protocol that sets up multi-paths has been proposed. The AOMDV routing protocol is a routing protocol designed for use in networks where link failures occur frequently. When route discovery occurs frequently, overhead and waiting time of the network occurs, and energy consumption occurs because packets for routing are generated. To

reduce this problem, the AOMDV routing protocol sets up multiple paths and performs route discovery to discover new paths only when all paths fail. Figure 4 shows the table structure of the AODV and AOMDV routing protocols.

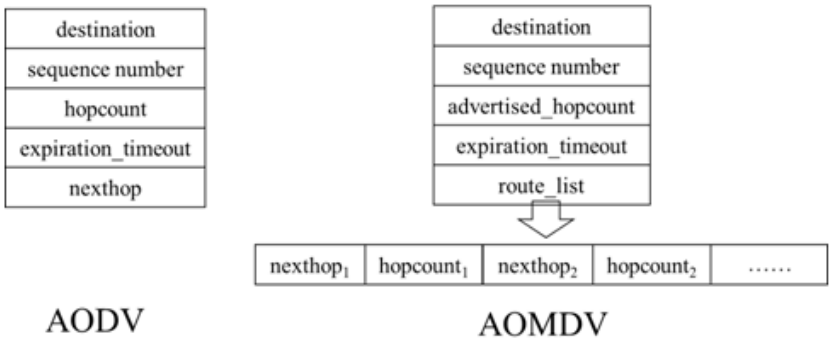

Figure 4. Structure of routing tables

The hopcount in the AODV routing protocol is replaced by advertised_hopcount in the AOMDV routing protocol. The advertised_hopcount is initialized only when the sequence number is updated. Also, the nexthop in the AODV routing protocol is replaced with the route_list in the AOMDV routing protocol. Route_list stores multiple routes in a list with hopcount.

3. PROPOSED SCHEME

3.1. Motive

The fog computing-based system for selective forwarding detection schemes is a technique for detecting selective forwarding attacks occurring in MWSNs. However, the selective forwarding attack detection method uses the AODV routing protocol. Since the AODV routing protocol uses a single path, when it is applied to MWSNs composed of sensor nodes with mobility, the path failure occurs due to the movement of the sensor node, and route discovery frequently occurs to solve the problem. Therefore, energy consumption for route discovery is continuously generated in the sensor network. To solve this problem, the proposed scheme uses an AOMDV routing protocol that takes full advantage of the AODV routing protocol and reduces route discovery by multiple paths. The AOMDV routing protocol can be used to reduce energy consumption for route re-establishment, but since all routing needs to be set to multi-paths, multi-path routing should be set up in areas where multiple routing settings are not needed. Therefore, the proposed scheme improves the energy efficiency of the sensor network by reducing the energy for route discovery by determining the number of multi-paths using fuzzy logic and controlling the number of multi-paths in the area where multi-paths are unnecessary.

3.2. Assumption

The initial energy of the sensor node is set at random, and the movement of the sensor node uses a random waypoint (RWP) model. Selective forwarding attacks occur only on compromised nodes. BS and fog servers are not attacked.

3.3. Fuzzy System

The proposed scheme improves the energy efficiency of the sensor network for routing the establishment energy and routing by determining the number of multi-paths using fuzzy logic in the selective forwarding attack detection scheme in MWSNs.

3.3.1. Input Parameter and Output Value

The proposed scheme uses the fuzzy logic used to determine the number of multi-paths. In fuzzy logic, the input parameters are density of sensor nodes (DN), the residual energy of sensor nodes (RE), the distance between the sensor node and a base station (DB) and the output value is number of Multi-paths (NP).

Input parameters

DN = {L(Low), A(Average), H(High), VH(Very_High)}

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

DB = {N(Near), A(Average), F(Far)}

Output value

NP = {P1(Path1), P2(Path2), P3(Path3), P4(Path4), P5(Path5)}

Since the input parameter DN uses the RWP model to move the sensor node, sensor nodes may be concentrated in one area. In the area where the sensor nodes are dense, the movement of the sensor node is limited. When the multi-paths are set, the sensor nodes in the dense area set many multi-paths. If the density of the area decreases due to the movement of the sensor node after a lapse of time, many sensor nodes must perform the route resetting. This routing is an unnecessary setting. Therefore, the energy efficiency of the sensor network is improved if the number of multi-paths is set to a smaller value in a higher density area. The input parameter RE is associated with the lifetime of the sensor network. If the energy of the sensor node is depleted, the sensor node cannot deliver the packet from the point of time when the energy is depleted. When many sensor nodes are exhausted, a coverage hole is generated. This is the same for mobile sensor nodes. Therefore, when the energy of the sensor node is low, the load balancing of the sensor node should be performed using multi-paths. When multiple paths are set, the sensor nodes are load-balanced by sequentially distributing and delivering packets through the set multi-paths [11]. If the load balancing of the sensor node is smooth, the network lifetime of the sensor network increases. However, load balancing is unnecessary when there are many sensor nodes with a large amount of energy remaining. In these areas, less energy is spent on routing due to the smaller number of multi-path configurations. The input parameter DB does not require multiple paths because sensor nodes near the BS can directly forward the packet to the BS. The number of multi-paths reduces the energy consumption for routing by setting the number of multi-paths to be smaller as the distance between the BS and sensor node decreases. Finally, the output value NP represents the number of multi-paths. A total of 1 to 5 multi-paths can be set. p1 represents one path setting, and p5 represents five path settings. The proposed scheme improves the energy efficiency of the sensor network by reducing the energy consumed in path search and the multi-path setup when detecting selective forwarding attack by setting multi-paths through output value NP.

3.3.2. Membership Function and Fuzzy Rule Base

The proposed method transforms input and output values into membership functions through fuzzification and determines the number of multi-paths of AOMDV routing protocol through defuzzification. Figure 5 is a membership function that schematically shows the fuzzy set in the proposed scheme.

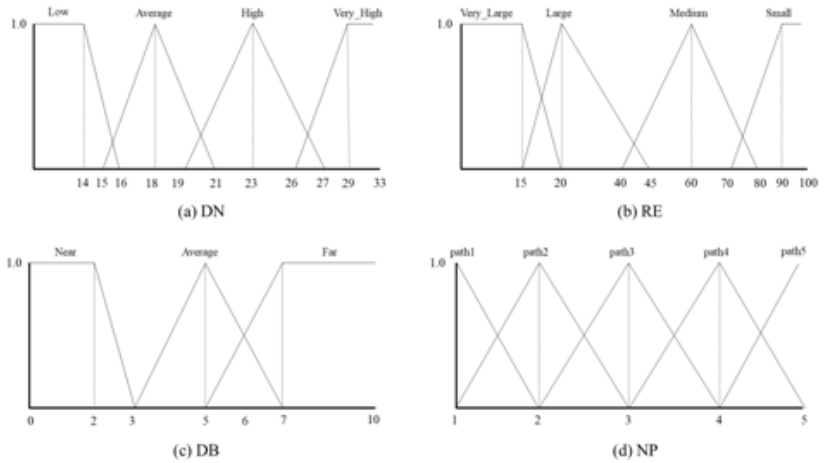

Figure 5. Fuzzy membership function

Then, the fuzzy rule base is created by using an input parameter and the output value of the fuzzy logic. Table 1 shows the part of the fuzzy rule base set in the proposed scheme.

Table 1. Fuzzy rules

Rule	Input			Output (NP)
	DN	RE	DB	
0	L	VL	N	P1
1	L	VL	M	P1
2	L	VL	F	P2
3	L	L	N	P1
⋮	⋮	⋮	⋮	⋮
17	A	L	F	P2
18	A	M	N	P3
19	A	M	M	P2
⋮	⋮	⋮	⋮	⋮
33	H	S	N	P3
34	H	S	M	P4
35	H	S	F	P5
⋮	⋮	⋮	⋮	⋮
44	VH	M	F	P5
45	VH	S	N	P4
46	VH	S	M	P5
47	VH	S	F	P4

4. EXPERIMENTAL RESULTS

The proposed method is verified through simulation written in C++ using Visual Studio. The size of the sensor field used in the proposed scheme is 300 x 300(㎡), and the total number of sensor nodes is 200. The movement of the sensor furnace is based on the RWP model, and the energy of the sensor node does not exceed 1 Joule. There are three base stations and three fog servers which receive event packets sent from the sensor nodes and grasps events. The compromised node is located at random. The movement speed of the sensor node is set to [0, Vmax] km/h and the direction is set to [0,2π]. The threshold of the proposed scheme is set to 15, the same as the fog computing-based system for selective forwarding detection. Eelec = 50 nano Joule/bit is consumed to transmit the packet wirelessly in the sensor node, and εelec = 100 pico Joule/bit/㎡ is consumed in the transmission amplification [12]. Therefore, the energy consumed when transmitting the data of the k bit packet from the sensor node is calculated according to Eq. (1).

$$E_{Tx}(K, d) = E_{elec} * k + \varepsilon_{elec} * k * d^2 \quad (1)$$

The energy consumed when receiving from the sensor node is calculated according to Eq. (2).

$$E_{Rx}(K) = E_{Rx\text{-}elec}(K) \quad (2)$$

Figures 6-8 shows the sensor network energy efficiency according to the movement speed of the sensor node.

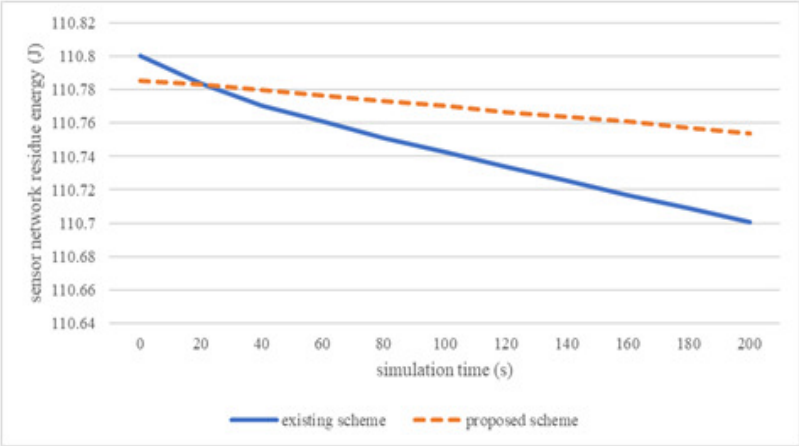

Figure 6. Sensor network efficiency (Vmax = 20)

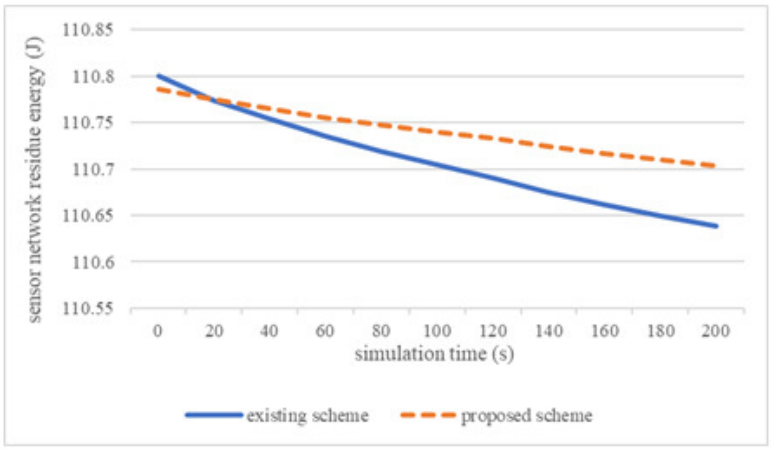

Figure 7. Sensor network efficiency (Vmax = 40)

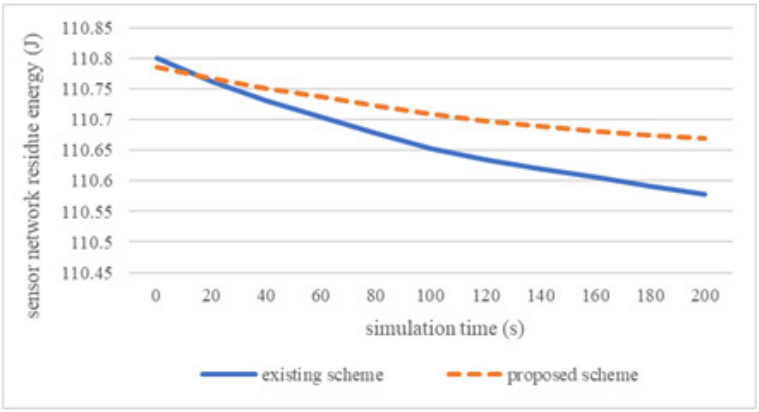

Figure 8. Sensor network efficiency (Vmax = 60)

Figure 9 shows the number of packets drops with simulation time when the sensor node speed is [0, 60] km/h.

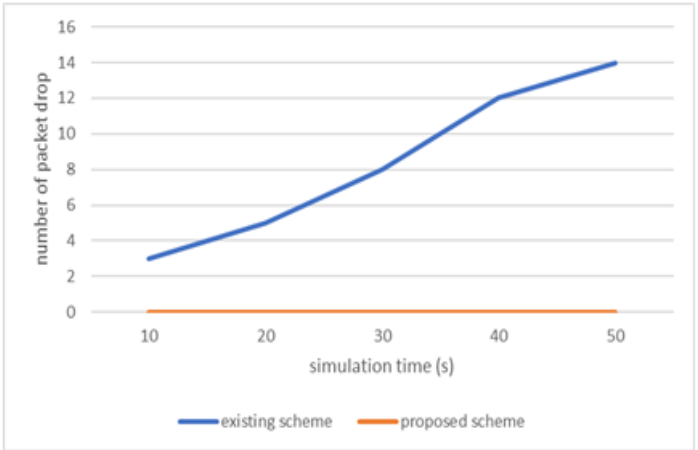

Figure 9. Number of packet transmission failures to BS (Vmax = 60)

If the simulation time is 50 seconds, the packet drop occurs 14 times in the conventional scheme. However, since the proposed scheme uses multipath, it can be confirmed that the packet is not dropped.

4. CONCLUSION

Selective forwarding attacks in MWSNs are difficult to detect because all sensor nodes move. In addition, the selective forwarding attack detection scheme researched in WSNs is not applicable to MWSNs because they do not consider the movement of sensor nodes. A fog computing-based system for selective forwarding detection scheme is a technique for detecting selective forwarding attacks occurring in MWNS based on the movement of the sensor nodes. Since this detection scheme transmits packets using the AODV routing protocol, energy consumption of the sensor node for route discovery is large when the detection scheme is used in MWSNs. The proposed scheme improves the energy efficiency of the sensor network by determining the number of multi-paths using fuzzy logic. Experimental results show that the energy efficiency of the sensor network is 9.5737% higher than that of the existing method when the attack occurs for n seconds. Future research will be carried out to establish multi-paths suitable for the situation considering the change in the MWSNs.

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] K. Akkaya and M. Younis, “A survey on routing protocols for wireless sensor networks,” Ad Hoc Netw., vol. 3, pp. 325–349, 2005.

[3] R.Javad, M.Moradi and A.S.Ismail, "Mobile wireless sensor networks overview," International Journal of Computer Communications and Networks vol. 2, no. 1, pp. 17-22, 2012

[4] 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

[5] I. Amundson and X. D. Koutsoukos, "A survey on localization for mobile wireless sensor networks." Mobile entity localization and tracking in GPS-less environnments. Springer, Berlin, Heidelberg, 235-254, 2009

[6] 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

[7] J. Sen, "A survey on wireless sensor network security," arXiv preprint arXiv:1011.1529, 2010.

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

[9] N 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

[10] 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

[11] 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, Jan. 2012

[12] R.U.Anitha and P. Kamalakkannan, "Enhanced cluster based routing protocol for mobile nodes in wireless sensor network," Pattern Recognition, Informatics and Mobile Engineering (PRIME), 2013 International Conference on. IEEE, pp. 187-193, 2013

Authors

Won Jin Chung Received a B.S. degree in Information Security from Baekseok University, Korea, in 2016 and is now working toward a Ph.D. degree in the Department of Electrical and Computer Engineering at Sungkyunkwan University, Korea.

Tae Ho Cho Received a Ph.D. degree in Electrical and Computer Engineering from the University of Arizona, USA, in 1993, and B.S. and M.S. degrees in Electrical and Computer Engineering from Sungkyunkwan University, Republic of Korea, and the University of Alabama, USA, respectively. He is currently a Professor in the College of Software, Sungkyunkwan University, Korea.