Journal Homepage: - www.journalijar.com
INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)
Article DOI: 10.21474/IJAR01/7421
DOI URL: http://dx.doi.org/10.21474/IJAR01/7421
ISSN NO. 2320-5407

RESEARCH ARTICLE

CASCADED FUZZY LOGIC BASED ROUTING DETERMINATION METHOD TO REDUCE THE ENERGY CONSUMPTION OF SELECTIVE FORWARDING ATTACK DETECTION IN MWSNS.

Won Jin Chung and Tae Ho Cho.
Department of Electrical and Computer Engineering, Sungkyunkwan University, Suwon, Republic of Korea.

Manuscript Info

Manuscript History

Received: 15 May 2018
Final Accepted: 17 June 2018
Published: July 2018

Keywords:-
wireless sensor networks, mobile wireless sensor networks, selective forwarding attack, network security, ad-hoc on-demand multipath distance vector, fuzzy logic system.

Abstract

Selective forwarding attacks in mobile wireless sensor networks are classified as threat attacks because the compromised node moves to various areas and attempts to attack. A fog computing-based system has been proposed to detect selective forwarding attacks. However, since the detection scheme uses a single path, the energy consumption of the sensor node for route discovery is large. To solve this problem, multipath can be used. However, in regions where the multipath setting is not needed, this setting causes the sensor node to consume energy unnecessarily. The proposed scheme improves the energy efficiency of the sensor network by using fuzzy logic to determine whether to use multipath. The experimental results demonstrate that the proposed scheme achieves an energy improvement of about 8.3374% over 200 seconds.

Introduction:-

Wireless sensor networks (WSNs) are composed of inexpensive sensor nodes that monitor, calculate, and transmit temperature, humidity, and vibration data, and a base station (BS) that receives event messages from the sensor nodes and processes the data. WSNs are used in a variety of fields that require continuous monitoring, such as the military, agriculture, factories, and transportation systems [1][2]. In a large or inaccessible battlefield where it is difficult to deploy sensor nodes directly, an aircraft is used to deploy the sensor nodes randomly. Since the sensor nodes are randomly placed, it is not always possible to monitor all the sensor fields. Also, since sensor nodes are difficult to charge, their energy becomes depleted when they are used for long periods of time. Areas with many energy-exhausted nodes become coverage holes. Another problem is that the sensor nodes around the BS must transmit all the events to the BS, so they are more easily depleted than other sensor nodes [3]. To solve this problem, mobile wireless sensor networks (MWSNs) composed of mobile sensor nodes have been proposed [4]. MWSNs can solve the problems that occur in WSNs by moving the sensor nodes and can increase the channel capacity used by the WSNs by 3- to 5-fold. Also, since the hop count decreases as the sensor node moves, the probability of packet transmission error decreases [5].

Since the sensor nodes used in MWSNs have low computing power and send packets to the BS wirelessly, malicious attackers can compromise the sensor nodes by using these loopholes. Attackers can then attempt various attacks using the compromised nodes [5]. Selective forwarding attacks selectively drop or transmit packets to the BS by selectively dropping attack notification event packets into this hostile environment. As a result, the area that defends against the attack can cause confusion because the event notification packet is partially propagated [6]. In MWSNs, selective forwarding attacks are difficult to detect because the compromised node moves and selectively drops

Corresponding Author:-Tae Ho Cho.
Address:-Department of Electrical and Computer Engineering, Sungkyunkwan University, Suwon, Republic of Korea.

packets in various regions. In addition, the intrusion detection systems (IDSs) applied to WSNs do not consider the movement of the sensor node, and thus are difficult to apply to MWSNs.

A fog server-based system has been proposed to detect selective forwarding attacks based on the movement of the sensor nodes [7]. This method detects selective forwarding attacks by measuring the drop rate of a packet transmitted in a sensor node for a predetermined time. However, since this detection method uses the ad-hoc on-demand distance vector (AODV) routing protocol, many routing problems occur due to the movement of the sensor nodes [8]. To solve this problem, the sensor node executes route discovery, but it must continuously consume energy to do so. This problem can be solved by use of the ad-hoc on-demand multipath distance vector (AOMDV) routing protocol using multipath [9]. However, when multipath is set, it is also set in unnecessary areas. In this paper, the energy efficiency of the sensor network is improved as fuzzy logic is used to determine whether to use multipath.

The composition of this paper is as follows. Section 2 describes the selective forwarding attack detection scheme and the AOMDV routing protocol. Section 3 describes the proposed scheme. Section 4 displays the experimental graph for the verification of the proposed scheme. In the last section, conclusions and future research are presented.

Background:-

In this section, we briefly describe the operation of the selective forwarding attack detection scheme and the AOMDV routing protocol.

Selective Forwarding Attack Detection Scheme:-

Selective forwarding attacks in WSNs are attacks that selectively forward or drop packets when a notification packet arrives at a sensor node that the attacker has previously compromised. These attacks can cause great chaos because packets are selectively delivered in areas such as hostile environments where packets must be delivered. Figure 1 displays the scenario in which a selective forwarding attack occurs in an MWSN.

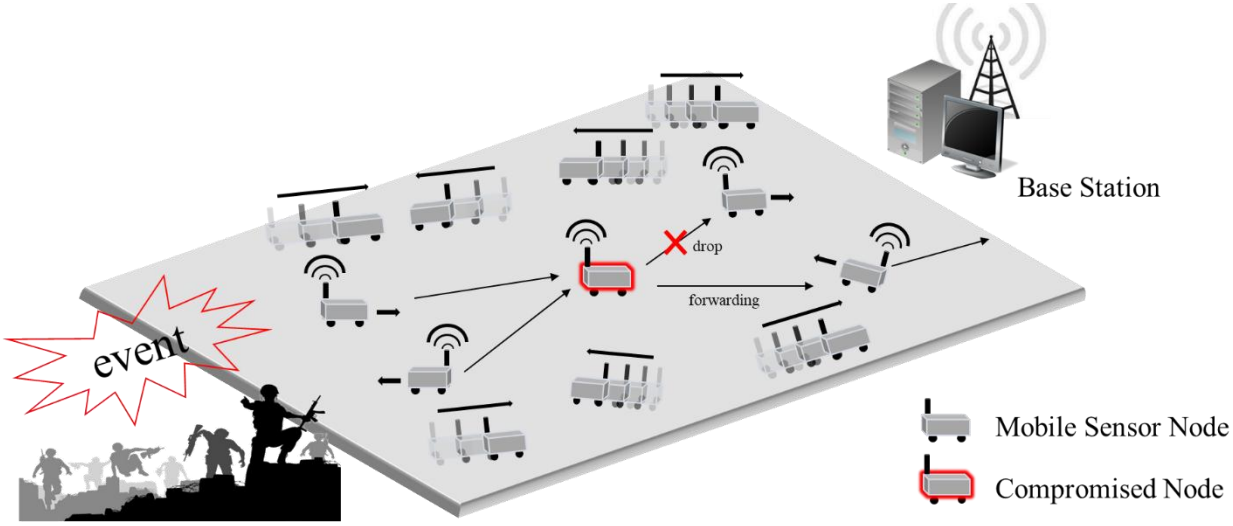

Figure 1:-Selective Forwarding Attack in a MWSN

Selective forwarding attacks that occur in MWSNs where all the sensor nodes move are more difficult to detect than those in WSNs, because selective forwarding attacks are attempted in all regions while the compromised node moves. In WSNs, many kinds of IDSs have been introduced to detect selective forwarding attacks [10].

The authors proposed a selective forwarding detection scheme using an entropy function based on the forwarding speed of a sensor node by arranging the monitoring node. However, in MWSNs, the next hop changes frequently because the sensor node is moving. Therefore, this detection scheme is difficult to apply to MWSNs [11]. The authors proposed a scheme to compare message exchange times using a hypothesis and to identify a selective delivery attack if the threshold is less than a set threshold. This detection technique assumes that the compromised node is a mobile sensor node and the non-compromised node is a static sensor node. However, this assumption is not

applicable to MWSNs where all the sensor nodes are moving. In other words, it is difficult to apply selective forwarding attack detection techniques studied in WSNs to MWSNs.

Therefore, among the detection schemes applicable to MWSNs, the fog computing-based system for selective forwarding detection proposed by Q. Yaseen is used in this paper. This detection scheme uses fog computing and a watchdog to detect selective forwarding attacks. The Fog servers share information with each other so that the watchdog can continuously monitor, even if the mobile sensor node moves. The watchdog continuously monitors the sensor node to measure its packet drop rate for a certain period. The fog computing-based system for selective forwarding detection consists of a Cloud computing layer, a Fog layer, and a Wireless sensor layer. The most important of these three layers is the fog layer. In this layer, the fog servers cooperate with each other to exchange monitoring information about the sensor node, analyze the monitoring information, and determine whether the node is a normal node or a compromised node through voting. In this way, selective forwarding attacks can be detected.

AOMDV Routing Protocol:-
The AODV routing protocol is used in ad-hoc networks. This routing technique solves the routing loop generation problem of the Distance Vector algorithm. The AODV routing protocol initiates the route discovery process when the source node needs a route to the destination node. The AODV routing protocol uses a route request (RREQ) packet to find the destination node, and the intermediate node that receives the RREQ packet transmits a route reply (RREP) packet back to the valid route to the destination node. Otherwise, the intermediate node floods the RREQ packet. Through the repetition of this method, the path from the source node to the destination node is established. The AODV routing protocol sends a route error (RERR) packet for maintenance. If path failure occurs, the RERR packet is used to remove the failed path, and the RREQ packet is transmitted to find a new path.

When the AODV routing protocol is used in MWSNs, path failure occurs frequently due to the frequent movement of the sensor nodes. The sensor node must transmit the RERR packet and the RREQ packet to maintain the routing path, so energy is continuously consumed for packet transmission. Energy-constrained sensor nodes need a solution to reduce energy consumption when the AODV routing protocol is used. The AOMDV routing protocol has been proposed to solve this problem. This technique sets up multiple paths using the function of the AODV routing protocol. The AOMDV routing protocol executes route discovery only if all configured paths fail. Therefore, the AOMDV routing protocol can be an effective routing protocol for maintaining the energy efficiency of sensor nodes in MWSNs where the sensor nodes move frequently.

Proposed Scheme:-

Motive:-
The fog computing-based system for selective forwarding detection is a technique used to detect selective forwarding attacks in MWSNs. However, because the AODV routing protocol is used for attack detection, path failure occurs due to the movement of the sensor node, and a new path is needed to transmit the packet to the BS. Therefore, the energy consumption of the sensor node for route discovery is large. The AOMDV routing protocol using multipath can be applied to reduce the energy consumption of the sensor node. However, the detection technique using the AOMDV routing protocol will use the multipath continuously, even when it is unnecessary. Multipath setup consumes more energy than single-path setup. A sensor node that is relatively close to the BS can transmit the packet to the sensor node nearest to the BS, which can then transmit it to the BS. In such a scenario, the multipath setting is unnecessary. To solve this problem, the proposed method uses fuzzy logic to determine whether to set up the multipath of the sensor node.

Assumption:-
The energy and the initial position of the sensor node are set at random. Selective forwarding attacks occur only on compromised nodes. The BS and fog servers are not attacked. The ID of the initially set sensor node cannot be changed. The movement of the sensor node uses a random waypoint (RWP) model.

Fuzzy System:-
The proposed selective forwarding attack detection scheme for MWSNs determines the path setting cycle and multipath setting through fuzzy logic to improve the energy efficiency of the sensor network.

Input Parameters and Output Values:-

In the proposed scheme, a dual fuzzy logic system is used to determine the setting period and the multipath setting. In the first fuzzy logic system, the input parameters are the sensor movement speed of the sensor node (SN), the frequency of events (FE), and the sensor node density (DN), while the output value is the fuzzy logic application cycle (AC). In the second fuzzy logic system, the input parameters are AC (the output value of the first fuzzy logic system), the hop count (HC) from the source node to the BS, and the sensor node residual energy (RE), while the output value is the multipath setting (MS). Figure 2 displays the fuzzy rule-based system used in the proposed scheme.

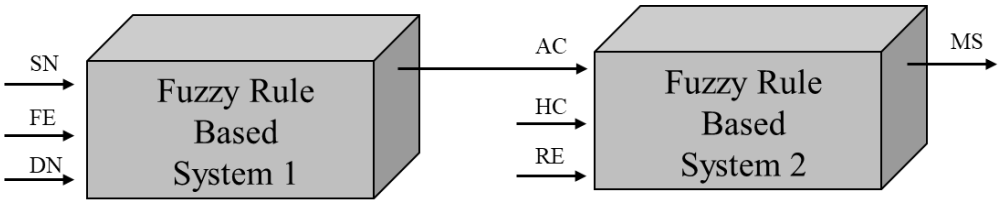

Figure 2:-Fuzzy Rule-Based System Overview

Fuzzy Rule-Based System 1
Input parameters
SN = {S (Slow), N (Normal), F (Fast)}
FE = {VS (Very Small), S (Small), A (Average), L (Large)}
DN = {L (Low), M (Medium), H (High)}
Output value
AC = {S (Short), A (Average), L (Long), VL (Very Long)}

Fuzzy Rule-Based System 2
Input parameters
AC = {S (Short), A (Average), L (Long), VL (Very Long)}
HC = {F (Few), A (Average), M (Many)}
RE = {S (Small), A (Average), L (Large), VL (Very Large)}
Output value
MS = {U (Unapplied), A (Apply)}

Since the mobile sensor node uses the RWP model, the SN input parameter of fuzzy logic system 1 changes randomly at each mobile sensor node. The faster the mobile sensor node speed, the faster the network path changes, and therefore the faster the fuzzy logic setting period should be. Another input parameter, FE, reflects the fact that if events occur frequently in a certain area, the number of packets passing through the path increases. When a packet is sent in one path, the energy of a sensor node included in the path is consumed more rapidly than the energy of other sensor nodes. The multipath sequentially transmits packets according to the set path. When multipath is used, load balancing of the sensor nodes is possible [12]. Therefore, the routing should be changed to multipath through the shortening of the fuzzy logic setting period. An area where sensor nodes are concentrated will have relatively low route discovery. Therefore, if the fuzzy logic set period of DN is fast, the multipath setting will be used unnecessarily in dense sensor node areas.

Next, AC (the output value of fuzzy logic system 1) is used as an input parameter of fuzzy logic system 2. As the fuzzy logic cycle becomes shorter, the sensor node needs to set the routing to multipath. However, due to the influence of the other input parameters of fuzzy logic system 2, the routing is not unconditionally set to multipath, even if the fuzzy set period is fast. HC, another input parameter of fuzzy logic system 2, does not need multipathing for sensor nodes that are close to the BS. If multiple paths are established, the sensor nodes placed around the BS consume energy unnecessarily for multipath routing. The input parameter RE is an important factor in the lifetime of the sensor network. A sensor node will not work when its energy is exhausted. Therefore, a coverage hole occurs when a large number of sensor nodes are depleted of energy. When the RE of the sensor node is small, the lifetime of the sensor network can be increased through the use of the multipath setting and the load balancing of the sensor node.

Fuzzy Rule Base and Membership Function:-

The proposed method converts input parameters and output values into membership functions through fuzzification with a double fuzzy logic system. After that, the fuzzy logic setting cycle and multipath usage are determined through defuzzification. Figures 3 and 4 are membership functions for fuzzy sets in fuzzy logic systems 1 and 2.

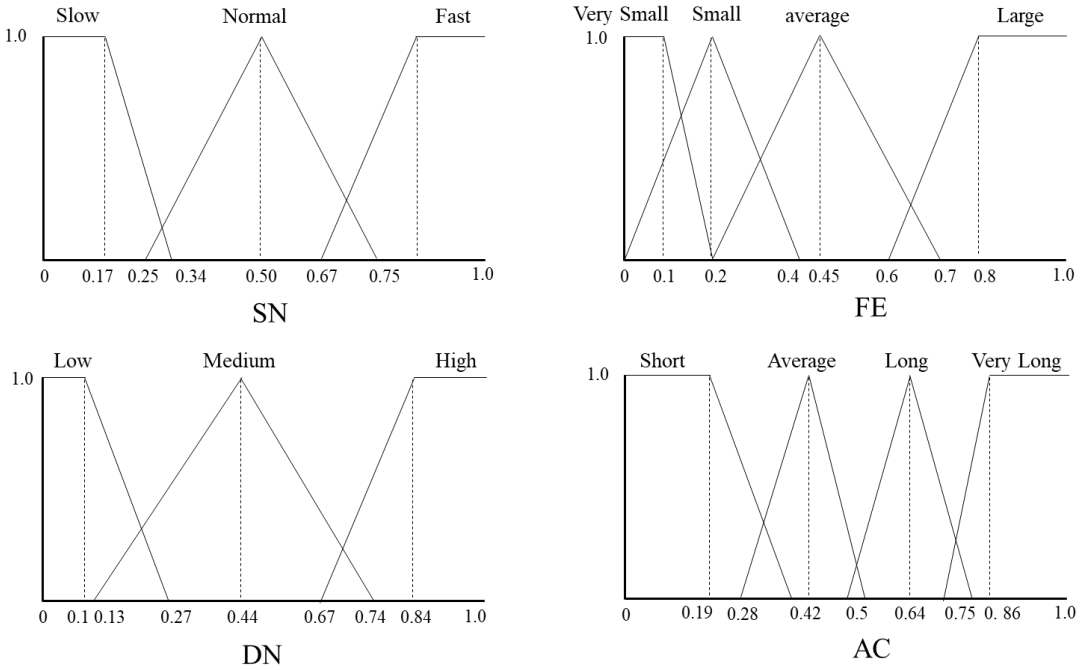

Figure 3:-Membership Function (Fuzzy Logic System 1)

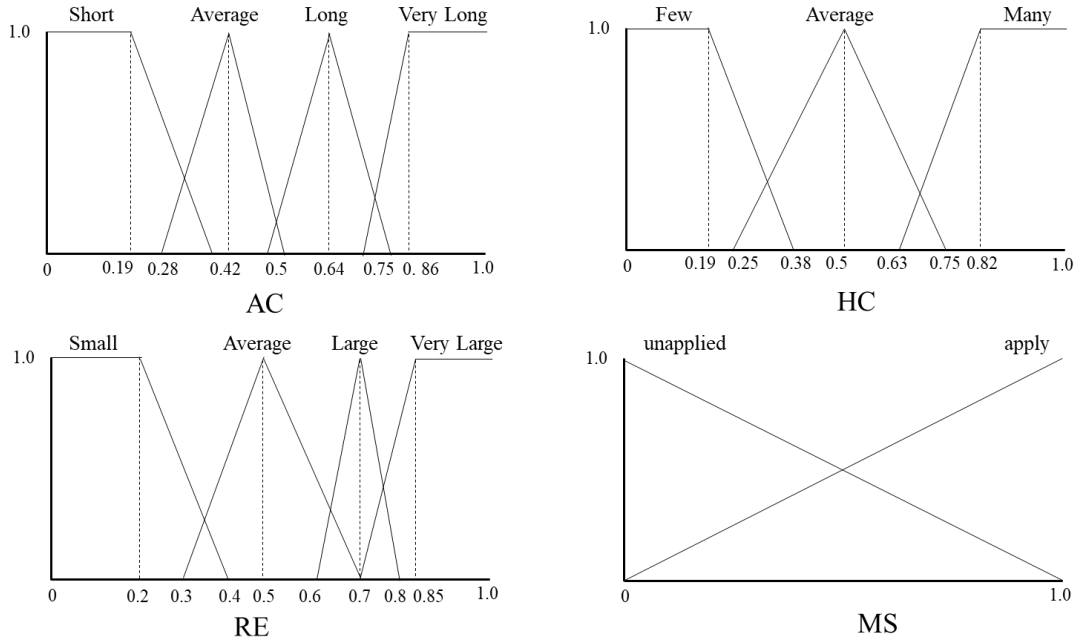

Figure 4:-Membership Function (Fuzzy Logic System 2)

Then, a fuzzy rule base is created from the input parameters and output values of fuzzy logic systems 1 and 2. Tables 1 and 2 display some of the fuzzy rule bases.

Table 1:-Rule Base (Fuzzy Logic System 1)

Rule	Input			Output (AC)
	SN	FE	DN	
0	S	VS	L	L
1	S	VS	M	VL
8	S	A	H	L
9	S	L	L	A
17	N	S	H	L
23	N	L	H	A
25	F	VS	M	A
27	F	S	L	L
34	F	L	M	S
35	F	L	H	S

Table 2:-Rule Base (Fuzzy Logic System 2)

Rule	Input			Output (MS)
	AC	HC	RE	
0	S	F	S	A
1	S	F	A	A
7	S	A	VL	U
10	S	M	L	A
11	S	M	VL	U
15	A	F	VL	U
16	A	A	S	A
23	A	M	VL	U
24	L	F	S	A
32	L	M	S	A
33	L	M	A	A
39	VL	F	VL	U
40	VL	A	S	A
46	VL	M	L	U
47	VL	M	VL	U

Experimental Results:-

The proposed method verifies the energy efficiency of the sensor network through a program written in C++, and Visual Studio is used for verification. The sensor field used in the proposed scheme is 300 x 300 (m2) in size, and the number of mobile sensor nodes is 200. The sensor node energy is set at random but does not exceed 1 Joule. The sensor nodes are moved according to the RWP model, and the moving speeds are set to [0, 40] km/h and [0, 60] km/h, respectively. The direction of the sensor node is set to [0,2π]. The threshold for detecting a selective forwarding attack is set to 15 in the fog computing-based system for selective forwarding detection. Eelec = 50 nanoJoules/bit are consumed to transmit the packet at the sensor node, and εelec = 100 picoJoules/bit/m2 are consumed for transmission amplification [13].

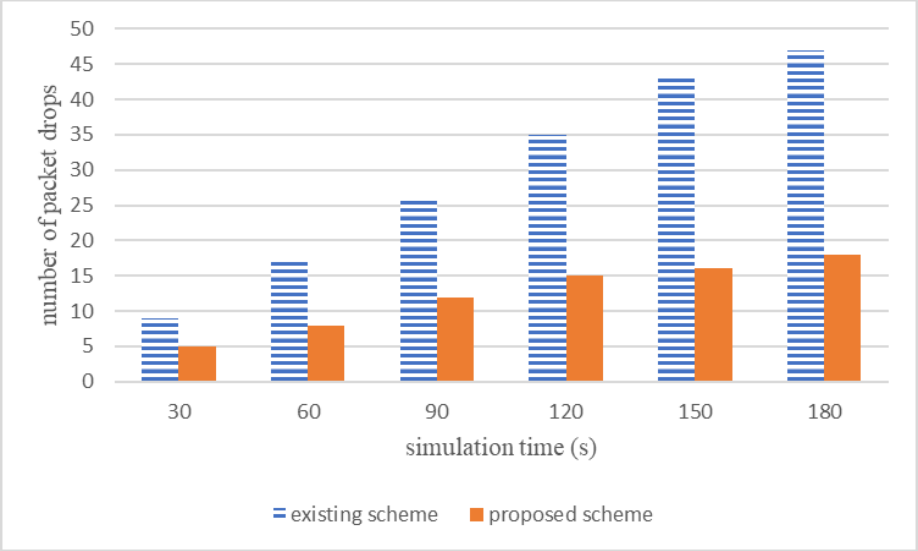

Figure 5:-Number of packet transmission failures to the BS([0,60] km/h)

Figure 5 depicts the packet drop rate of the proposed scheme in a sensor network when an optional forwarding attack occurs. It can be seen that the packet drop rate is small when the proposed scheme is used in a MWSN.

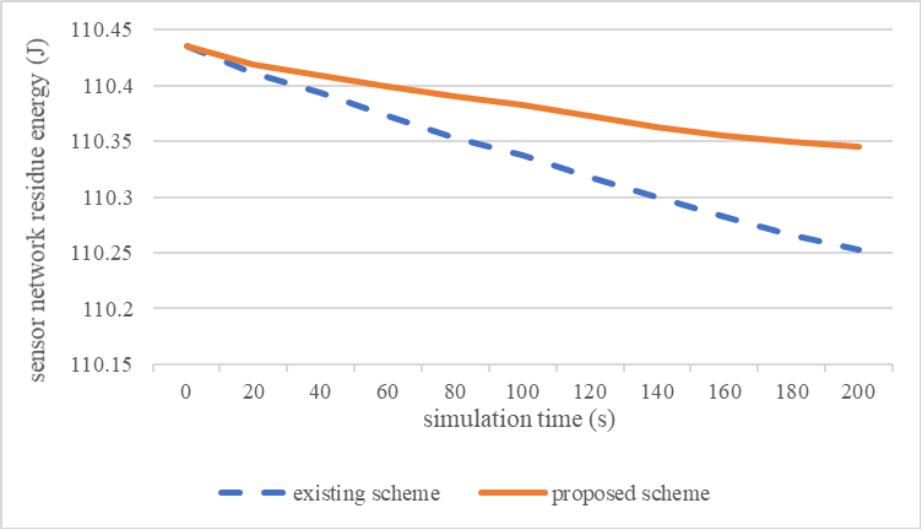

Figure 6:-Sensor network efficiency ([0,40] km/h)

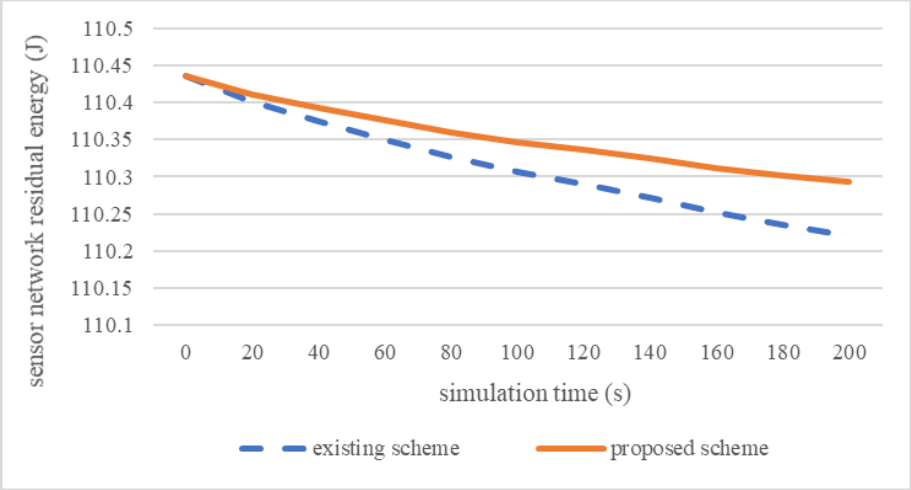

Figure 7:-Sensor network efficiency ([0,60] km/h)

Figures 6 and 7 compare the sensor network energy efficiencies of the existing scheme and the proposed scheme. When the simulation is run for 200 seconds, the proposed scheme improves the energy efficiency of the sensor network by about 8.3374% compared with the existing scheme.

Conclusion:-

Selective forwarding attacks that occur in MWSNs are difficult to detect because the compromised node moves and attacks occur in various regions. In consideration of this problem, a fog computing-based system for selective forwarding detection has been proposed. This detection scheme uses a Fog server and a watchdog to detect selective forwarding attacks. However, because a large number of sensor nodes move, path failure frequently occurs, and route discovery is executed every time a path problem occurs. Therefore, the energy of the sensor node is continuously consumed for path maintenance. The energy consumption of the sensor node can be reduced through a detection technique using the AOMDV routing protocol with multipath. When this routing protocol is used, route discovery is executed only when all the established paths fail. However, in areas where multipathing is not required, unnecessary energy consumption for multipathing occurs in the sensor nodes. To solve this problem, the proposed scheme improves the energy of the sensor network by determining whether to multipath through fuzzy logic. Future research will focus on a detection scheme to improve energy by controlling the routing for various network layer attacks in MWSNs.

Acknowledgements:-

This research was supported by the MIST(Ministry of Science and ICT), Korea, under the National Program for Excellence in SW 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. W.Chen, et al. "Wits: A wireless sensor network for intelligent transportation system," Computer and Computational Sciences, 2006. IMSCCS'06. First International Multi-Symposiums on, IEEE, Vol. 2, pp. 635-641, 2006.
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. G. S. Sara and D. Sridharan, "Routing in mobile wireless sensor network: A survey," Telecommunication Systems, Vol. 57, No. 1, pp. 51-79, 2014.
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. 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
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. Y. Hu, Y. Wu, and H. Wang, "Detection of insider selective forwarding attack based on monitor node and trust mechanism in wsn," Wireless Sensor Network, 2014.
11. J. Ho, M. Wright, and S. K. Das, "Distributed detection of mobile malicious node attacks in wireless sensor networks," Ad Hoc Networks, Vol. 10, No. 3, pp. 512–523, 2012.
12. 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
13. 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.