Fuzzy -based TTL (Time To Live) Determination for Improving The Energy Efficiency of The WODEM for Wormhole Attack In WSN

Sun-Ho Lee[†] **and Tae-Ho Cho**[††],

Sungkyunkwan University, Suwon, 440-746, Republic of Korea

Summary

One of the typical attacks in Wireless Sensor Networks (WSN), is setting up the wrong route with using a wormhole. The wormhole attack, which is accomplished by selectively relaying packets between adversaries, can ruin the routing and communication of the network without compromising any legitimate nodes. To overcome this threat, there are a few countermeasures against the wormhole attack in WSN. The WODEM (WOrmhole attack DEfense Mechanism) can detect and counter any wormhole attacks. In this scheme, the WODEM can detect and counter wormhole attacks by comparing hop count with the pre-determined initial TTL (Time To Live). The selection of the initial TTL is important since it can provide a tradeoff between the detection ability ratio and the energy consumption. In this paper, we propose a fuzzy rule-based system that can conserve energy for determining the TTL, while it provides a sufficient detection ratio for a wormhole attack.

Key words:
Wormhole, Wireless Sensor Network, Fuzzy Logic, Security.

1. Introduction

The recent advances made for sensor nodes such as: low cost, low power, detecting, and computing, in addition to, the advances made in the field of wireless communication abilities, have made it possible for WSN to be used in more various fields [1]. A sensor network is composed of a large number of sensor nodes and a few base stations. The sensor nodes are densely deployed and they observe the surrounding environment. The sensor nodes have limited processing power, small storage capacity, limited energy, and the ability to communicate either among neighbors or directly to the base station (BS), which collects the sensor readings through narrow-bandwidth channels [2]. The limited energy is closely connected with the whole network lifetime, the efficient use of available energy bas been one of the most important challenges. In addition to the power management challenge, security is another great challenge the sensor network shares with other wireless networks. There are many applications such as military applications and confidential business operations that require secure communication and routing in sensor networks. In order to make the communications secure in sensor networks, many security protocols have been proposed to provide authenticity and confidentiality [3-4].

One of the typical attacks in a Wireless Sensor Network (WSN) is setting up the wrong route by using a wormhole. The wormhole attack is accomplished by two adversaries that simply relay incoming packets from one adversary to the other without decrypting or differentiating any packets. The two adversaries communicate with each other through a direct and dedicated channel by using a wired link or additional RF transceivers with a longer transmission range. The route via the wormhole looks like an attractive path to the legitimate sensor nodes because it generally provides a smaller number of hops and a shorter latency than the normal routing paths. During the relay of data, the communication suffers from severe performance degradation because the adversaries can arbitrarily drop the packets [4-7].

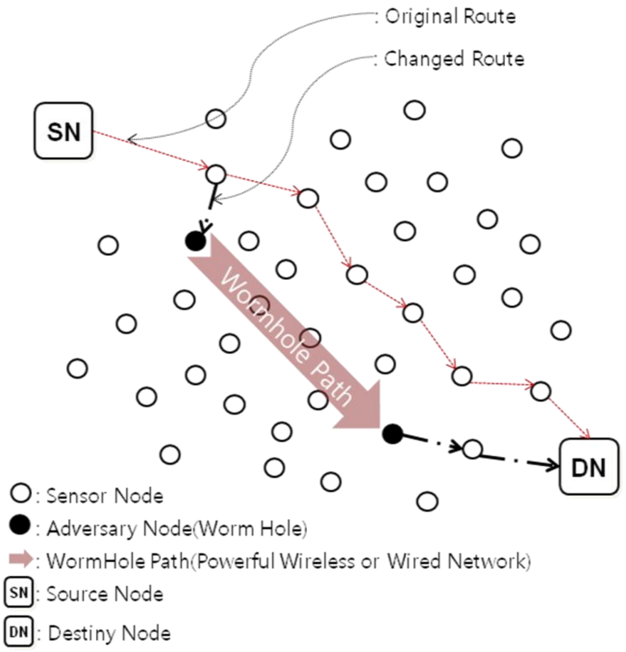

Fig. 1 Wormhole Attack in WSN

Manuscript received July 5, 2009
Manuscript revised July 20, 2009

The WODEM (WOrmhole attack DEfense Mechanism) can detect and counter a wormhole. In this scheme, it can detect and counter attacks by the wormhole by comparing the hop count and the initially pre-determined TTL (Time To Live). The selection of the initial TTL is important since it can provide a tradeoff between the detection ability ratio and the energy consumption [7].

In this paper, we propose a fuzzy rule-based system for determining TTL that can conserve energy, while it provides a sufficient detection ratio in the WODEM. The verification probability is adaptively determined by a fuzzy rule-based system. The density of nodes in a network, the average remaining energy for every node, and the distance to the destiny node form the source node are used in the determination.

The remainder of the paper is organized as follows: Section 2 briefly describes the WODEM. Section 3 describes the proposed method in detail. Section 4 reports the simulation results. Finally, the conclusion is discussed in Section 5.

2. The WODEM

The WODEM (WOrmhole attack DEfense Mechanism) [7] is proposed by Ji-Hoon Yun et al. The WODEM consists of three phases: the detector scanning, the wormhole detection, and the neighbor-list repair. In the first phase, the scanning phase, the detectors scan their counterpart detectors to measure the path loss exponent of the wireless channel and to prepare for the detection phase. In the next detection phase, a pair of detectors detects the wormhole attack between them. If a wormhole is detected, then the detectors start the repair phase where the invalid neighbors in the neighbor lists will be removed. The detectors repeat the detection and the repair phases until they no longer detect a wormhole. We explain the operation of each phase in the following subsections.

2.1 The Detector Scanning

In the scanning phase, each detector scans its counterpart detector and measures the channel's characteristics. To keep the scanning discrete, the scanning phase uses a separate channel that is different from the normal communication channel of the network so that the control packets of the scanning phase do not traverse a wormhole. Therefore, all the detectors in the scanning phase are tuned to the normal communication channel. We define the detector that triggers the scanning phase as the source node (SN). The source node starts its scanning phase by broadcasting a scanning packet with TTL 1. The scanning packet contains the location L_s and the transmission power level P_t of the SN. The SN repeats the sending of the scanning packet while it increases its transmission power by Δp in each transmission until it receives more than two replies from the other detector nodes. The reply packet contains P_t in the scanning packet and it contains the location L_r of the replying detector node. From the reply packets, the SN computes two characteristic parameters of its channel, i.e., the path loss exponent *n* and the constant *k* in the equation shown below:

$$P^t = k \times |L_s - L_r|^n$$

After the computation, the SN chooses its counterpart detector node, known as the Destiny node (DN), among the detectors that have replied to the scanning packets. Any detector can be either SN or DN.

2.2 The Wormhole Detection

In the detection phase, the SN and DN check whether there is a wormhole between them. Let L_r be the location of the DN and let H_{SR} be the hop count of the route from the SN to the DN. Consequently, the inequality below should always be true without any wormhole between two detector nodes:

$$H_{SR} \geq min\{H_{SR}\} = \left\lceil \frac{|L_s - L_R|}{r} \right\rceil$$

The right side of the above inequality is the minimum achievable number of hops between the S-R pair. To achieve this, the SN sends a detecting packet with a normal transmission range *r*. The detecting packet contains L_s and H_{SR}. Here, the TTL value of the detecting packet is set to be large enough for the DN to receive the packet. When the DN receives the detecting packet, it checks the above inequality and knows whether there is a wormhole between the S-R pair. If a wormhole is detected, then it enters the repair phase.

On the other hand, the detecting packet may traverse the wormhole and thus it can be dropped by the wormhole. Therefore, the DN needs to acknowledge the reception of the detecting packet regardless of the detection of the wormhole. If the SN does not receive an acknowledgement packet in a timeout time, it retransmits the detecting packet. This process is applied to all the exchanges of the control packets between the S-R pair. The acknowledgement delay increases as the drop rate of the wormhole increases.

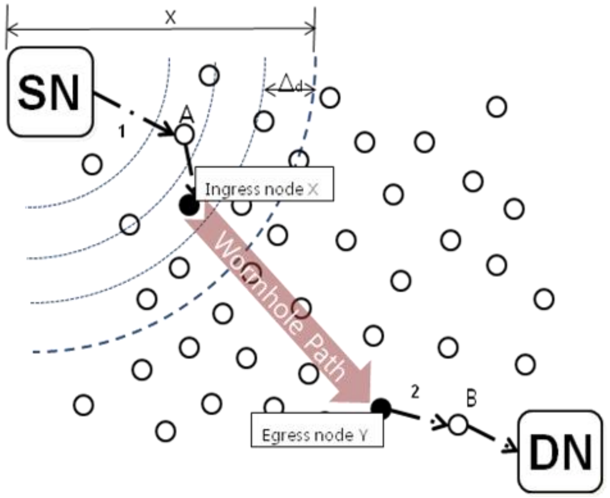

Fig. 2 The Wormhole Detection

2.3 The Neighbor-list Repair

In the repair phase, the detectors find two sensor nodes in the route, between which the detected wormhole resides, and they let them remove each other in their neighbor lists.

The SN starts the repair phase by sending a probing packet to the DN with an initial transmission range *r* and TTL 1. The probing packet contains L_S, the transmission range of the corresponding transmission and the initial TTL value. The SN repeats the sending of the probing packets by increasing its transmission range by Δd in a stepwise manner until it receives a probing reply packet from the DN or until the transmission range reaches the DN directly. If the SN still does not receive a probing reply packet from the DN after the above procedure, then the SN resets the transmission range to *r*, increases the initial TTL value by 1 and repeats the above procedure.

For every probing packet received, the DN examines whether the packet is probed via the wormhole using the inequality below:

$$(Initial\ TTL) \geq min\{H_{SR}\}$$

If the inequality is false, then it means the packet traversed shorter hops than the minimum valid number of hops, that is possible only by traversing the wormhole. Here, $min\{H_{SR}\}$ is obtained by:

$$min\{H_{SR}\} = \left\lceil \frac{|L_S - L_R| - R}{r} \right\rceil + 1$$

where *R* is the transmission range of the S-detector when it transmitted the corresponding probing packet.

The S-R pair repeats the process from the detection phase until they cannot detect a wormhole anymore.

3. TTL Determination Method on WODEM

3.1 The Motivation

WODEM has many processes to find the wormhole, that are similar to finding the detect nodes and so on. If the wormhole is detected, then the SN sends a probing packet with TTL 1, which then receives an acknowledgement and it increases the TTL.

Because the sensor node does not have enough energy, this repetitive process causes pretty high energy consumption. For reducing energy consumption, we apply the fuzzy rule-based system that considers the density of the nodes, the average remaining energy for every node, and the distance to form SN to DN.

3.2 The Assumptions

We assume that the network is composed of a number of sensor nodes, a few detector nodes, and a high capability BS. We also assume that BS has all the nodes information such as location, remaining energy and so on. We also assume that the detector nodes have a Global Positioning System (GPS) for recognizing each other [8]. We further assume that the BS and the detector nodes have much more energy and computing capability than a normal sensor node.

3.3 The Overview

Fig. 3 depicts the proposed method. In the proposed method, we apply an Aggressive TTL in the wormhole detection phase that results in fuzzy logic. The initial TTL is changed to an Aggressive TTL, so that it does not need the repetitive process until the Aggressive TTL value is reached. Then it moves through the original process at WODEM.

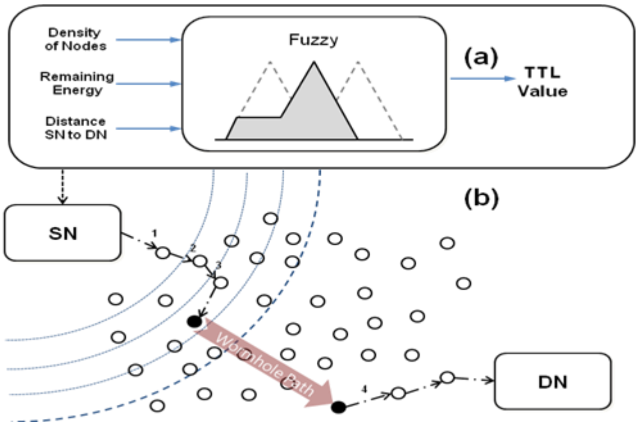

Fig. 3 Proposed Method

3.4 The Determination of the Aggressive TTL

BS determines the Aggressive TTL by using the nodes' information around the SN and the DN. When nodes are distributed, the BS computes the density of the nodes while considering the arrangement of the network and the number of nodes. The BS computes the remaining energy by using nodes' energy information between the SN and the DN. It then computes the distance to the DN form the SN after completing the detector scanning phase. Then it determinates the Aggressive TTL which inputs these three values into the fuzzy logic.

3.5 The Input and Output Parameters

○ The Input Parameter

In our proposed method, the density of the nodes in network is one of the important considerations. If the density is low, then this means there are few nodes within the distance from the SN to the DN area, and consequently, the TTL is determined to be low.

The remaining energy is also important. If the remaining energy is small, then the TTL is determined to be low. It means they do not have enough energy to detect the wormhole using the initial TTL. So we determine the TTL to be Large.

The distance from the SN to the DN is similar that of the density nodes. It can show the number of nodes between the SN and the DN. It can be combined with the density nodes for improving value of the TTL.

The density_of_nodes = {Very_Low, Low, Middle, High, Very_High}

The remaining_energy = {Small, Medium, Much}
The distance_from_S_to_D = {Very_Short, Short, Middle, Long, Very_Long}

○ The Output Parameter

We consider the density of the nodes, the average remaining energy for every node, and the distance to the DN form the SN. If the TTL value is large, then the Wormhole Detection phase starts process having a large initial TTL value. Consequently, the energy consumption is decreased..

Aggressive_TTL = {Very_Small, Small, Medium, Large, Very_Large}

3.6 The Membership Function

○ The Input Parameter

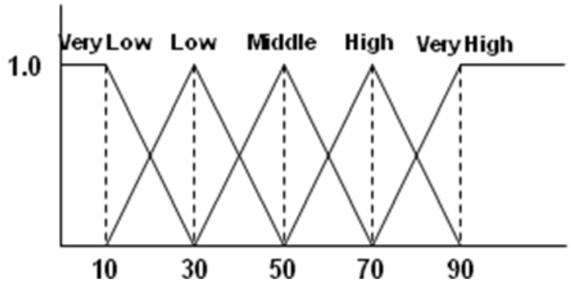

Fig. 4 The Input Membership Function
(a) density of nodes

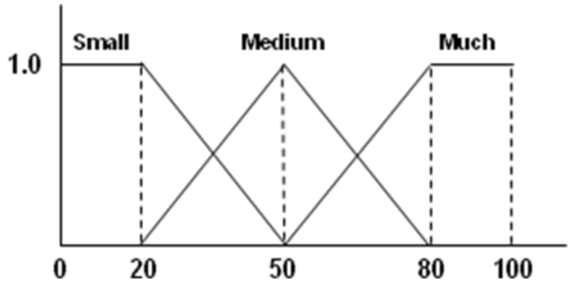

Fig. 5 The Input Membership Function
(b) remaining energy

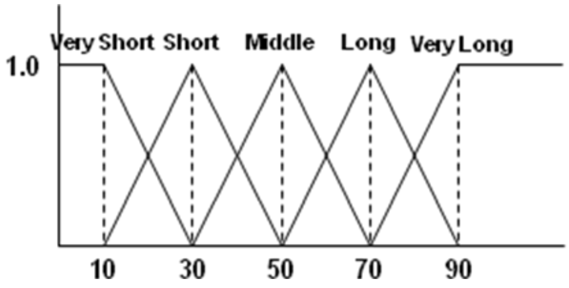

Fig. 6 The Input Membership Function
(c) the distance from S to D

○ The Output Membership Function

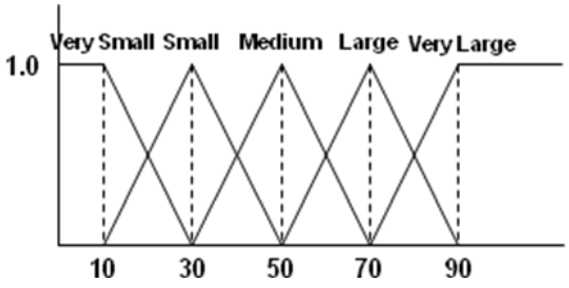

Fig. 7 The Output Membership Function
(d) Aggressive TTL

3.6 The Fuzzy Logic

RULE 5: IF Very_High AND Medium AND Very_Long THEN Very_Large;

RULE 7: IF Very_High AND Medium AND Middle THEN Large;

RULE 18: IF High AND Much AND Short THEN Medium;

RULE 33: IF Middle AND Much AND Short THEN Small;

RULE 64: IF Very_Low AND Much AND Very_Short THEN Very_Small;

4. Simulation Results

We compare our proposed method with WODEM by using simulation to show the effectiveness of our proposed method. Our simulation is conducted over a 1000m×400m rectangular flat space with 100 randomly distributed sensor nodes. Each node consumes 16.25 and 12.5 µJ to transmit / receive a byte, respectively [9].

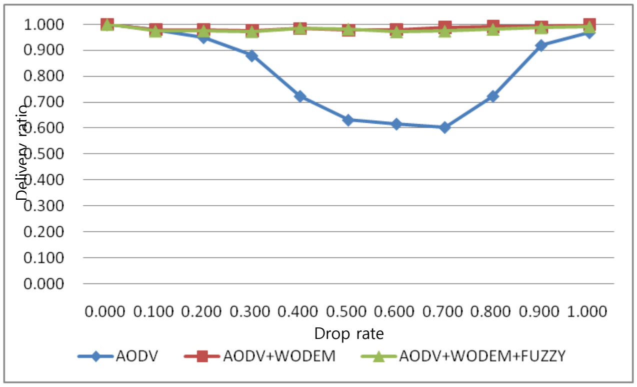

Fig. 8 The Effect of the Wormhole Attack as The Drop Rate Varies

Fig. 8 shows the packet delivery ratios of the network with and without the WODEM and the proposed method in a simulation network. Here, the packet delivery ratio is defined as the ratio of the number of packets that are received by the sink to the number of packets that are generated by the sensor nodes. In this simulation, we also consider AODV [8] for the routing protocol in order to investigate the effect of the routing protocol in the wormhole attack. As shown in figure 8 where, AODV is used, the delivery ratio recovers as the drop rate is higher than 0.7 due to its local repair algorithm. With WODEM, the wormhole cannot cause any damage to the network for both routing protocols regardless of the drop rate. In our proposed method the wormhole cannot damage the network, and this is similar to the results shown in the WODEM.

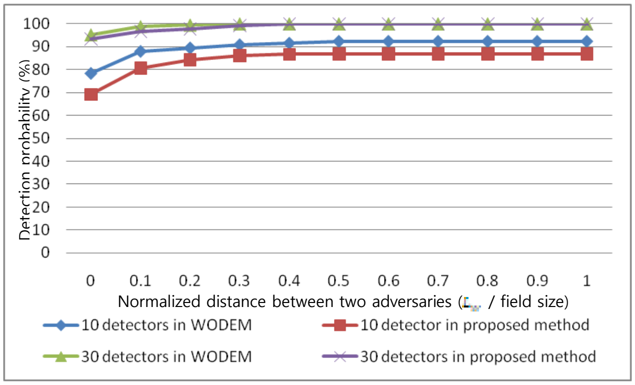

Fig. 9 The Detection Probability Vs. The Wormhole Length

(field size = 1000m)

Fig. 9 shows the simulation result of the relation between the detection probability and the distance L_W between two adversaries of a wormhole with 100 sensor nodes. From the figure, the longer L_W is, the higher the detection probability is. That is because it is more probable that the number of hops of the illegal route is smaller than the ideal minimum hop count.

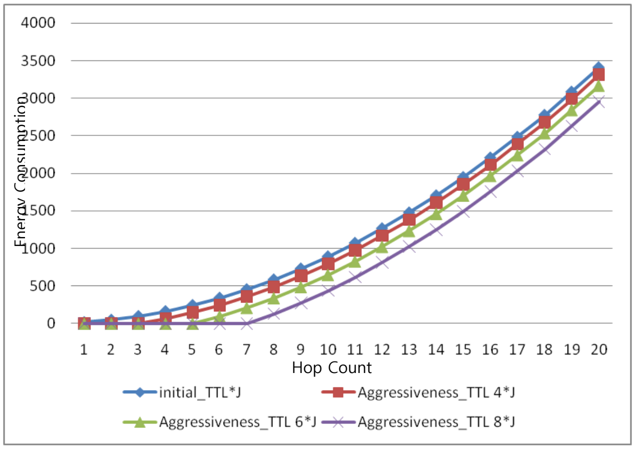

Fig. 10 The Energy Consumption As The Aggressive TTL Increased

Fig. 10 shows the average energy consumption during the wormhole detection phase. As shown in the figure, the determined TTL saves more energy than the initial TTL. As the value of the Aggressive TTL is increased, the amount of energy consumption is decreased.

5. Conclusion

In this paper, we propose a fuzzy-based for determining method the Aggressive TTL in the WODEM. In our proposed method, the Aggressive TTL is adaptive according to the fuzzy rule-based system with considering the density of the nodes, the average remaining energy for every node, and the distance to DN form SN. The simulation results show that the proposed method can simultaneously conserve energy, and provide a sufficient detection ratio.

Acknowledgments

This work was supported by the Korea Research Foundation Grant funded by the Korean Government (KRF-2008-313-D00827).

References

[1] I.F. Akyldiz, W. Su, Y. Sankarasubramaniam, E. Cayirci., "A Survey on Sensor Networks," IEEE Wireless Communication Magazine, Vol. 40, no. 8, pp. 102-116, 2002.

[2] J.N. Al-Karaki, A.E. Kamal, "Routing techniques in wireless sensor networks: a survey," IEEE Wireless Communication Magazine, Vol. 11, no. 6, pp. 6-28, 2004.

[3] Przydatdek, B. Song, D. and Perrig, A. (2003), "SIA: Secure Information Aggregation in Sensor Networks", ACM, in Proc. of SenSys, pp. 255-265.

[4] C. Karlof and D. Wagner, “"Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures,”" Proc. 1st IEEE Int''l., Wksp. Sensor Network Protocols and Applications, May 2003.

[5] Y.-C. Hu, A. Perrig, and D.B. Johnson, “"Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks,”" Proc. 22nd Ann. Joint Conf. IEEE Computer and Communications Societies (INFOCOM 2003), IEEE Press, 2003, pp. 1976–-1986.

[6] J. Eriksson, S. Krishnamurthy, and M. Faloutsos, “"Truelink: A practical countermeasure to the wormhole attack,”" in ICNP, 2006.

[7] J.-H. Yun, I.-H. Kim, J.-H. Lim, and S.-W. Seo. WODEM: Wormhole Attack Defense Mechanism in Wireless Sensor Networks. In Ubiquitous Convergence Technology (ICUCT 2006), pages 200–-209. LNCS 4412, 2007.

[8] Charles E. Perkins: Ad hoc On-Demand Distance Vector (AODV) Routing, RFC 3561, IETF, July 2003.

[9] Ye F, Luo H, Lu S. Statistical En-Route Filtering of Injection False Data in Sensor Networks. *IEEE.Sel.ArreaComm.*, 2005, 23(4):839-850.

Sun-Ho Lee received his B.S. degrees in Internet Media from Kyungwon University, Republic of Korea, in February 2009. He is currently a graduate student in the School of Information and Communication Engineering at Sungkyunkwan University. His research interests include wireless sensor networks, modeling & simulation, artificial intelligence, and information security.

Tae Ho Cho received his Ph.D. degree in Electrical and Computer Engineering from the University of Arizona, USA, in 1993, and his B.S. and M.S. degrees in Electrical Engineering from Sungkyunkwan University, Republic of Korea, and the University of Alabama, USA, respectively. He is currently a Professor in the School of Information and Communication Engineering, Sungkyunkwan University, Korea. His research interests are in the areas of wireless sensor networks, intelligent systems, modeling & simulation, and enterprise resource planning.