ISSN: 0975-766X
CODEN: IJPTFI
Available Online through *Research Article*
www.ijptonline.com

DETECTING ATTACKS IN WIRELESS SENSOR NETWORKS USING FUZZY Q-LEARNING

Radhika Baskar, P.C.Kishore Raja, Suraparaju Nikhil
Department of ECE, Department of ECE, Saveetha University, Chennai.

Received on: 25.09.2016 *Accepted on: 15.10.2016*

Abstract:

The attacks in Wireless Sensor Networks are increasing step-by-step by generating flooding packets that exhaust crucial computing and communication resources of a device being attacked within a very short intervals. This must be secured. For this, the attack detection technique requires an adaptive learning classifier, with less computational complexity and an accurate decision making to stunt these attacks. Here, Fuzzy Q-Learning algorithm is used to detect the attack patterns. The FQL algorithm protects the wireless nodes within the network and target nodes from the attacks. The accuracy of detection using fuzzy logic controller or Q-Learning alone is less when compared to the Fuzzy Q-Learning Intrusion Detection System.

Keywords: Attacks detection, Q-learning, Attacks in WSN, Fuzzy Logic, Intrusion, Detection System.

I. Introduction:

As a product of the development and combination of the sensor technology, embedded computer technology, wireless communication technology and distributed information processing technology, Wireless Sensor Networks (WSNs) provide a kind of brand-new information possession and processing method, and have broad application prospects in military, environmental protection, agriculture and health and other fields [1,2]. A Wireless Sensor Network is composed of many number of sensor nodes and each performs actions like sensing, computing and communicating.

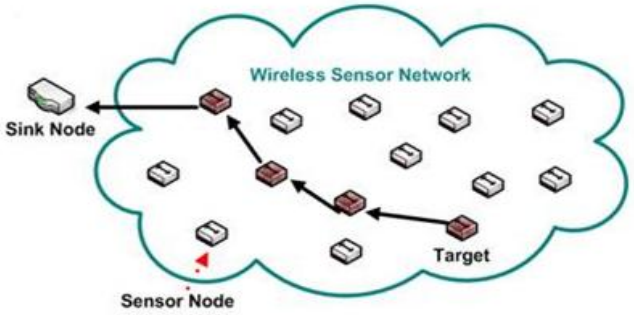

Fig. 1.A Wireless Sensor Network.

Recent advances in wireless communication and digital electronic have enabled the development of low-cost, low-power, multifunctional nodes which are small in size and which communicate with each other using radio frequencies [3]. Thus, to get the complete information of the sensor network, the data must be gathered collectively by the group of sensor nodes. But the sensor nodes present in the wireless sensor networks are limited-resourcedevices i.e., power and processing units (security and privacy). For this reason, exposure to numerous security threats is notably high. Thus, security became a major issue in case of designing wireless sensor networks.

The attacks in wireless sensor networks can be broadly classified into two,one is the attack against the security activities and another is against the basic activities (like routing mechanisms). Among these, the major attacks seen in Wireless sensor networks are Denial of Service (DoS) attacks. Denial of Service (DoS) [4], [5] is produced by the accidental failure of nodes or evil action. The simplest DoS attack tries to exhaust the resources on the market of the victim node, by sending further unessential packets and thereforestopslegitimate network users from accessing services or resources to that they're entitled.

In 2012, a report by Gartner reveals that a sophisticated class of Distributed Denial of Service (DDoS) attack sent an attack command to hundreds or even thousands of mobile agents, which then launched flooding attacks to access multiple websites [6]. Different types of DDoS attacks have been developed, which can be classified as TCP flood, UDP flood, ICMP flood, smurf, and distributed reflector attack [7]. During the distributed SYN flood attack, the adjusted systems are led to send SYN packets with an invalid source IP address, to create an sample of a half-open connection data structure on the target server. It can be concluded that the memory stack on the victim's system is filled up and no new demands can be handled [8]. Here, in section II, the objective is explained. In section III, methodology is described. In section IV, the simulation results are shown and in section V, the conclusion is given.

II. Objective:

The main aim of this discussion is, to design an attack detection system called a Fuzzy Q-Learning (FQL) algorithm to reinforce the learning ability of attack detection. This detection system helps in identifying the attack and thus the attacked node can be easily located and it can be repaired or replaced by taking necessary actions. Indirectly, this system helps in improving the security and privacy of the Wireless sensor network.

III. Methodology:

In this paper, we used Fuzzy Logic and Q-Learning algorithm to detect the attacks in Wireless sensor network. The entire detection process is carried out in two phases. In phase 1, the fuzzy logic controller used fuzzy min-max

strategy to provide the action choice policy. In phase 2, the Q-learning process adjusts their parameters (i.e., state, action) supported by fuzzy functions to cut back the complexness of states and action and also speed up the choice method. The following figure depicts the proposed architecture of Fuzzy Q-Learning algorithm for attack detection.

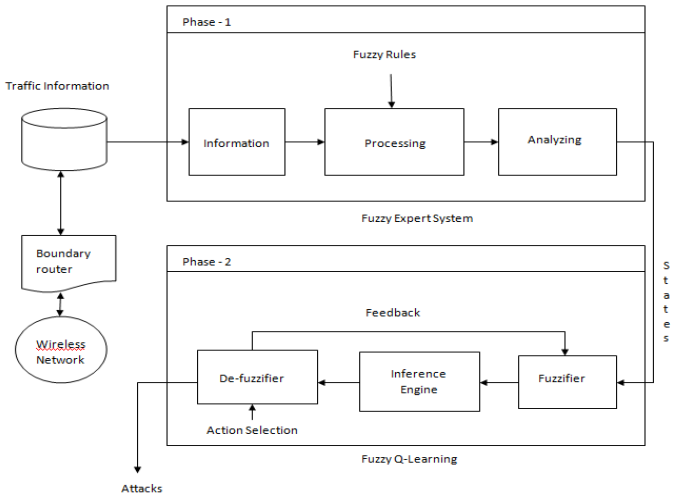

Fig. 2. Architecture of Fuzzy Q-Learning based attack Detection System.

A. Phase 1:

The fuzzy module mainly consists of three elements namely, fuzzifier, fuzzy logic controller and de-fuzzifier. The main element of the FLC is the Fuzzy Inference System invoked with set of well defined rules.

In first phase, to fully exploit the suspicious level, the fuzzy logic controller uses the knowledgeable System (or Expert system) that which utilizes Fuzzy Rules to identify the attacked conditions obtained from the traffic. Here, the Fuzzy Expert System (FES) is used to decrease the content of attacked data using fuzzy logic controller. TheFES consists of the respective components: the traffic capture, the feature extractor, the fuzzification, the fuzzy inference engine, the knowledge domain, the de-fuzzification, and the skilledanalyzer.

1).Traffic Capture:- The main function of the traffic capture is to collect the traffic information and prepare that information for the traffic analysis.

2).Feature Extractor:- The main function of feature extractor is toextract the captured features on the "network traffic" by the traffic capture elements.

3).Fuzzy System:- It carries the inspection process with the help of given set of rules in the inference engine.

B. Phase 2:

In the second phase, the FLC is elevated by Q-learning technique to sight the security threats captured by FES. The growth of FLC by Q-learning algorithm discovers six attributes namely, Protocol type (ES chooses only TCP),

Source and destination IP, Source and destination port, Time response (duration of response between sensor nodes), Buffer size, Count (no. Of connections).

Three fuzzy sets are outlined for the input of FQL to show three different situations of Q-learning: These inputs are named as TBC (Time response, Buffer size, Count). The FLC output, given by the increment within the states, represents the action of the sink node, A(t). The reward signal, R (t), made from the FLC, is measured in each modes of the nearnessso as to check if the sensors are encountering attacks. The acceptable variables of Time response, Buffer size, and Count acts as inputs and also the Detect Confidence acts as output.In order to find the optimal action, the reinforcement signal r (t) uses the equation,

$S(t) = [Tr, Bs, Co]$. FQL agent assigns a weight to all possible next states based on FLC. Associated to the threshold value, the optimal cost may be achieved.

IV. Simulation Result:

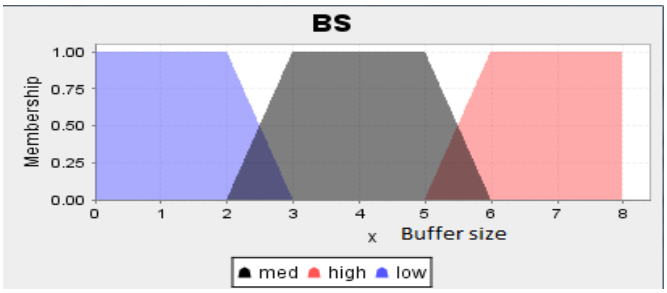

Fig. 3. Input Membership function.

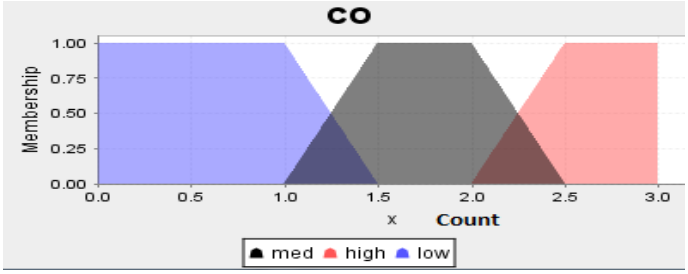

Fig. 4. Input Membership function.

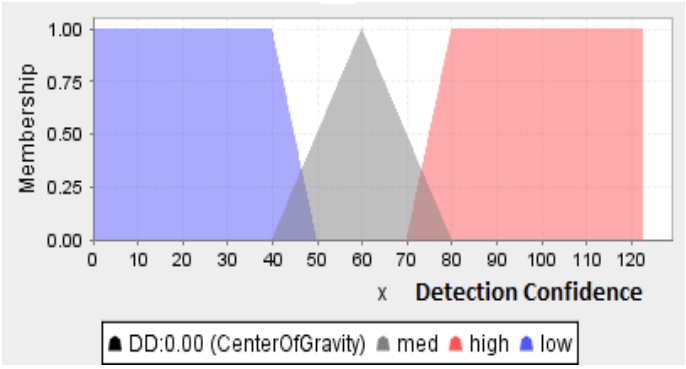

Fig. 5. Output Membership function.

V. Conclusion:

In this paper, we proposed the fuzzy Q-learning based algorithm for detecting attacks in wireless sensor network, which is far more accurate than the fuzzy logic controller or the Q-learning technique when used alone. Also the complexity of the process is certainly reduced as the complete algorithm is divided into two phases and is carried out one after another. A huge types of DDoS attacks can be detected in given short period using FQL algorithm as the time consumed for suspecting and identifying the attacked nodes is comparably less. Thus, accuracy in detection, reduced complexity and reduced time consumption are the achievements of using the proposed algorithm in this paper.

VI. References:

1. I.F. Akyildiz, W.Su, Y.Sankarasubramaniam, et al, "A survey on sensor networks," IEEE Communications Magazine, vol. 40, no. 8, pp. 102-114, 2002.
2. K. Akkaya, M. Younis, "A Survey of Routing Protocols in Wireless Sensor Networks," in the Elsevier Ad Hoc network Journal, Vol.3/3,pp. 325-349, 2005.
3. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, Wireless Sensor Networks: a Survey, J. Comput. Netw, 38 (2002) 393-422.
4. Blackert, W.J., Gregg, D.M., Castner, A.K., Kyle, E.M., Hom, R.L., and Jokerst, R.M., "Analyzing interaction between distributed denial of service attacks and mitigation technologies", Proc. DARPA Information Survivability Conference and Exposition, Volume 1, 22-24 April, 2003, pp. 26 – 36.
5. Wang, B-T. and Schulzrinne, H., "An IP traceback mechanism for reflective DoS attacks", Canadian Conference on Electrical and Computer Engineering, Volume 2, 2-5 May 2004, pp. 901 – 904.
6. DDOS Attacks against U.S. Banks Continue – LINKAGES Explored, Available from [www.gartner.com/], (2012).
7. A. D. Wood, J. A. Stankovic, Denial of Service in Sensor Networks, Computer, 35 (2002) 54-62.
8. C. V. Zhou, C. Leckie, S. Karunasekera, A Survey of Coordinated Attacks and Collaborative Intrusion Detection, Computers & Security, 29 (2010) 124-140.