ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology
Volume 1, Issue 4, June 2012

Rule Based Technique detecting Security attack for Wireless Sensor network using fuzzy logic

Mohit Malik, Namarta kapoor, Esh naryan, Aman Preet Singh

Lovely Professional University, Jalandhar Punjab India

Abstract. This paper represents the rule based technique which helps to detect the security attack in the Wireless Sensor network .There are many type of security attack which effects on the wireless sensor network. To demonstrate the effectiveness of the wireless sensor network, We have find ten security attack type in this work these parameters are fuzzy rule based system has been developed for calculating the impact of security attack on the wireless sensor network. We use the mouse data set to test these performances in Matlab tools.

Keywords: Feature selection, detection techniques, mouse dataset, Matlab, fuzzy logic etc

1 INTRODUCTION

A wireless network allows the people access application and information without wires. This provides the facilities to access application different parts of the building, city, or any where in the world. Wireless network allows people to communicate with e-mail or browse from a location that they prefer [3]. A wireless sensor network is a wireless network consisting of distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions, such as sound, vibration, pressure, at different locations. The development of wireless sensor networks motivated by military such as battlefield surveillance, however, wireless sensor networks are now used in many civilian application areas, including environment and habitat monitoring, healthcare applications. A wireless sensor network is a collection of nodes organized into a cooperative network each node consists of processing capability may contain multiple types of memory have an RF transceiver, have a power source e.g., batteries. The wireless network consists of thousands of low-power, low-cost nodes deployed to monitor and affect the environment [7]. Wireless sensor network emerged as mean study to interact with physical world. The wireless sensor technology has made it possible to deploy small, low-power, low-bandwidth and multifunctional wireless sensor nodes to monitor and report the conditions and events in different challenging environment [11]. A wireless sensor becomes a very popular because wireless nodes monitor and report the different environments. Wireless sensor network rapidly used in military, wildlife monitoring, earthquake monitoring, building safety. Wireless sensor network have recently emerged an important means study and interact with physical world. The recently technological advances in wireless sensor technology has made it possible to deploy small, low-power, low bandwidth, and multifunctional wireless sensor nodes to monitor and report the conditions and events in different challenging environment. As wireless sensor network continue to grow there is need for effective security mechanisms. Because sensor network may interact with sensitive data or operate in

unattended environment it is necessary that these security concerns should be addressed from the beginning of the system design [9]. However, security in sensor network poses different challenges for network security. Thus design mechanism of security very critical of the better and wider adaptability of this network in commercial scenarios. This paper investigates various security attacks on wireless sensor network and their impact on WSN [7].

1.1. Types of Security attack on wireless Sensor network [8]

Figure-1 Shows security attack on WSN

1.2. Security attack on WSN

Denial of service attack – It is occured by the failure of node or malicious action.

Eavesdropping attack - Adversary listen message transmitted to nodes.

Collision attack – It creates Interruption in the working wireless sensor network.

Sink hole attack – In a sinkhole attack is a serious threat in it compromised node tries to all or much traffic possible from a particular area.

Traffic analysis attack- It is a type of security attack which create a traffic on a wireless sensor network.

De- synchronization attack – De- synchronization changes sequences number of packet.

Selective farwarding attack – In this attack compromised node drops packets which effect on network efficency.

Jamming attack- Jamming attacks launched at MAC layer.

Clone attack – In this attack the attacker replicate the nodes in the form of clone.

Route information manuplation attack - In this attack the attacker gives a false routing information.

2. LITERATURE SERVAY

To minimize the chances of software project failure need to proper study all the risk factors which can have direct or indirect effect on the success of software product. Much application development used to make the software in efficient manner and various steps each risk defined. Tools are available for management of various kinds of risks. Fuzzy logic approach used to identify threats for the risks [3] [10]. This logic is composed of fuzzy sets, provides the concept of degrees of membership, which increases the number of possibilities that can be subject to research. This logic is perfect deal with uncertain risk come in project management [6].

3. EXPERIMENTAL RESULTS

Rule based Technique is the type of tool that helps to detect the Security attack influence on WSN. It is used for the different decision making. Rule based system presents information graphically and may include an expert knowledge. It is a specific class of computerized system that supports business and organization and decision activates. A Rule based system is an software based system intended to help decision maker compile the useful information from raw data, documents personal knowledge and business model to solve the problem..

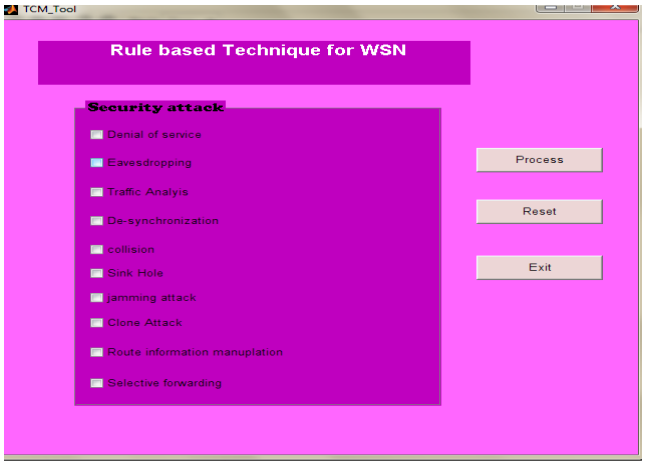

Figure 2: GUI Tool technique design Methodology

This rule based system help to analysis risks on WSN and provides ability to see the Security attack which provides highly influences on the WSN. We constructed 40 rule base

systems with different rules take guidance form including the WSN Organizations, Network, Manager, and Network companies. Using MATLAB, GUI Based tool is developed according to different added rule as shown in fig2

The impact of Security attack upon WSN, The impact levels of the risks are categorized into five levels. The impact Attack is categorized into five levels. The impact of risk can be "very low", "Low", "Medium", "High", very high". The inputs are represented by fuzzy system. Membership function is used to represent the fuzzy sets. Membership function of the system are as shown in fig 4.Membership function (MF) is a curve that defines how each point in the input is mapped to a membership value (or degree of membership) between 0 and 1.The membership functions are formed using straight lines of these, the simplest is the triangular membership function, and it has the function name trimf is a collection of three points forming a triangle. The trapezoidal membership function, trapmf, consists of truncated triangle curve. The membership function igbellmf (generalized bell membership function) and

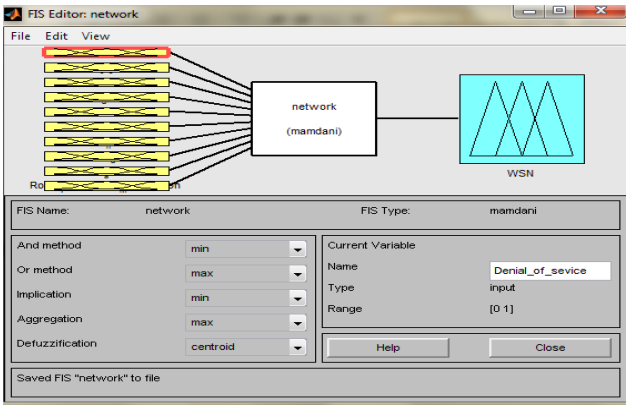

Figure 3: Input and output parameters

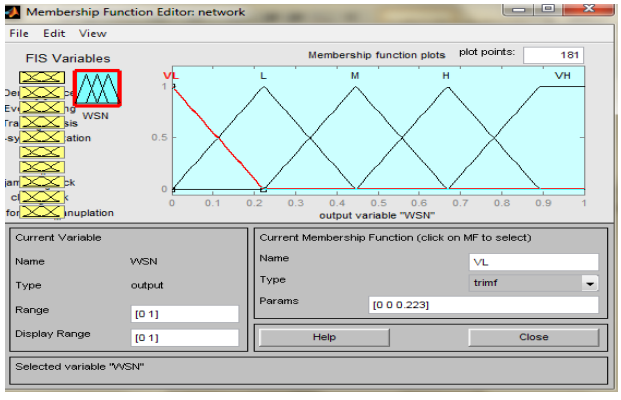

Figure 4: Membership function editor in Matlab

Gaussian membership function gaussmf define the fuzzy sets. Polynomial based curves account for several of the membership functions in the toolbox. Three related membership functions are the Z, S, and Pi curves, all named because of their shape. The function zmf is the asymmetrical polynomial curve open to the left, it defined Z- shape. Smf is the mirror-image function that opens to the right, and defines the S-shape. pimf is zero on both extremes with a rise in the middle. Fig 3 shows the input output parameters.

Rule editor given in figure 5 change and delete the rule. Also rule viewer and surface viewer are given in fig 6 and fig 7. Rule editor given in help to add and delete the rules. In the rule editor rule are formulated after representing input and output of fuzzy sets in membership functions. Some rules are-

1. If (Denial_ of_ service is Yes) and (Eavesdropping is No) and (Traffic_ analysis is Yes) and (De-synchronization is No) and (collision is Yes) and (Sink_ hole is No) and (jamming_ attack is Yes) and (clone_ attack is No) and (Route information_ manipulation is Yes) and (Selective_ forwarding is No) then (WSN is H) (1) .

2. If (Denial_ of_ service is Yes) and (Eavesdropping is Yes) and (Traffic_ analysis is No) and (De-synchronization is No) and (collision is Yes) and (Sink_ hole is Yes) and (jamming_ attack is No) and (clone_ attack is No) and (Route information_ manipulation is Yes) and (Selective_ forwarding is Yes) then (WSN is VH) (1).

3. If (Denial_ of_ service is Yes) and (Eavesdropping is Yes) and (Traffic_ analysis is Yes) and (De-synchronization is Yes) and (collision is Yes) and (Sink_ hole is No) and (jamming_ attack is No) and (clone_ attack is No) and (Route_ information_ manipulation is No) and (Selective_ forwarding is No) then (WSN is M) (1) .

4. 40 If (Denial_ of_ service is Yes) and (Eavesdropping is Yes) and (Traffic_ analysis is Yes) and (De- synchronization is Yes) and (collision is Yes) and (Sink_ hole is Yes) and (jamming_ attack is No) and (clone_ attack is Yes) and (Route_ information_ manipulation is Yes) and (Selective_ far warding is Yes) then (WSN is VH) (1).

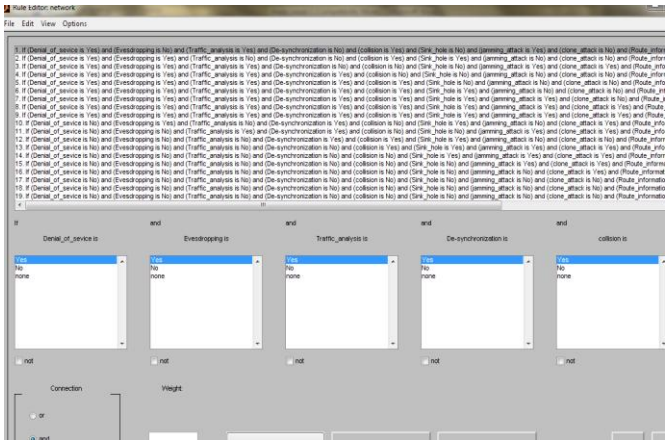

Figure 5: Rule Editor

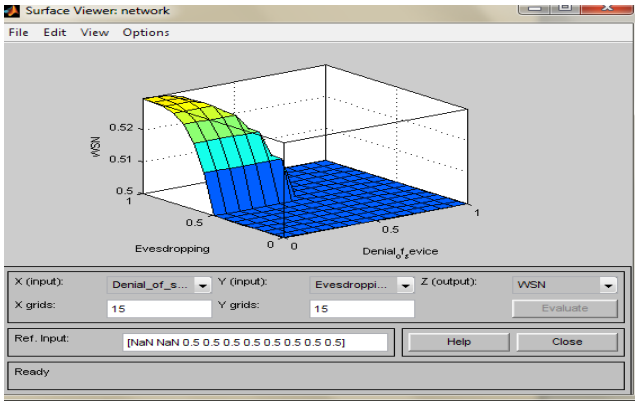

Figure 6: Surface viewer

Case- 1. In first case we see all security attack impact on WSN. In which tool calculating who how much chance of various Kinds of security attack on WSN and tell what impact on the WSN. Tool helps to predict the impact of Security attack on WSN. In figure 7a input is provided for the sample cases and tool gives the result possibility of attack occurrences will be 73.2388% on WSN in Figure 7b Show output of case.

Figure 7a: Snapshot of GUI with input for case 1

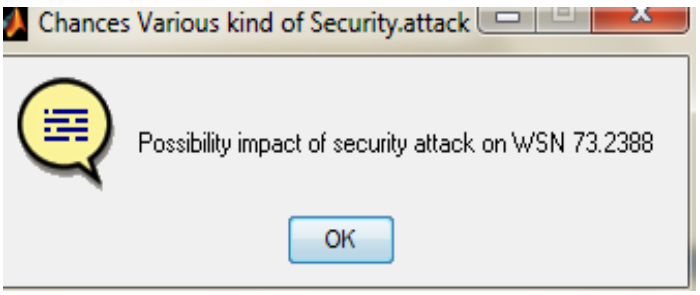

Figure 7a: Output for case 1

Case - 2 In Second cases we see some security attack impact on WSN. In which tool calculating who how much security attack impact on the WSN, Tool helps to predict the impact of Security attack on WSN. In figure 7b input is provided for the sample cases and tool gives the result possibility of attack occurrences will be 69.2195% on WSN in Figure 7b Show output of case 2 .if some security attack likes Denial of services, De-Synchronization, Jamming attack, clone attack , Route information manipulating ,Selective forwarding , collusion.

Figure 7b: Snapshot of GUI with input for case 2

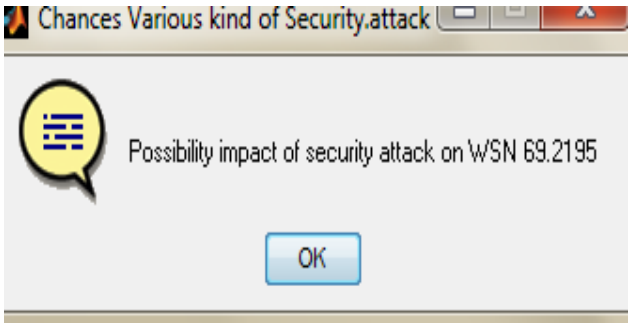

Figure 7b: Output for case 2

5. CONCLUSION AND FUTURE SCOPE

Many method of the fuzzy rule based system has been applied and different case study has been presented in this paper discussed various kinds of security attack and their impact on WSN. As the wireless sensor continue to grow and become more common there is strong requirement to secure these networks for better and wider adaptability in commercial scenario. A secure WSN design consists of proper attack detection and design mitigation techniques.

In future these techniques use to improve the secure data of network and fulfill the position of detection techniques in detection techniques methodology.

ACKNOWLEDGEMENTS

I wish to express my science profound gratitude to Mr. Gaurav Kumar Tak Asst. Professor, whose supervision & guidance in this investigation has been carried out, without whose guidance and constant supervision. It is not possible for me to complete this research paper successfully.

REFERENCES

[1]. Abdel-Azim, M.; Abdel-Fatah, A.I.; Awad, M.; "Performance analysis of artificial neural network intrusion detection systems," Electrical and Electronics Engineering, 2009. ELECO 2009. International Conference on , vol., no., pp.II-385-II-389, 5-8 Nov. 2009

[2]. Peng Shanguo; Wang Xiwu; Zhong Qigen; , "The study of EM algorithm based on forward sampling," Electronics, Communications and Control (ICECC), 2011 International Conference on , vol., no., pp.4597-4600, 9-11 Sept. 2011 doi: 10.1109/ICECC.2011.6067693

[3]. Fisher, D.; Ling Xu; Carnes, J.R.; Reich, Y.; Fenves, J.; Chen, J.; Shiavi, R.; Biswas, G.; Weinberg, J.; , "Applying AI clustering to engineering tasks," IEEE Expert , vol.8, no.6, pp.51-60, Dec. 1993 doi: 10.1109/64.248353

[4]. J.-S. R. Jang, C.-T. Sun, E.Mizutani, Neuro-Fuzzy and Soft Computing, p (426-427)Prentice Hall, 1997

[5]. Maria Colmenares & Olaf Wolken Hauer, "An Introduction into Fuzzy Clustering", http://www.csc.umist.ac.uk/computing/clustering.htm, July 1998, last update 03 July,2000

[6]. http://home.dei.polimi.it/matteucc/Clustering/tutorial_html/cmeans.html

[7]. www.ics.uci.edu/pub/ml-repos/machine-learning-database/, 2001

[8]. Von Altrock, Constantin (1995). Fuzzy logic and Nero Fuzzy applications explained. Upper Saddle River, NJ: Prentice Hall PTR. ISBN 0-13-368465-2

[9]. Arabacioglu, B. C. (2010). "Using fuzzy inference system for architectural space analysis" Applied Soft Computing 10 (3): 926–937. DOI:10.1016/j.asoc.2009.10.011.

[10]. Biacino, L.; Gerla, G. (2002). "Fuzzy logic, continuity and effectiveness" Archive for Mathematical Logic 41 (7): 643–667. DOI:10. 1007/s001530100128. ISSN 0933-5846

[11]. Cox, Earl (1994). The fuzzy systems handbook: a practitioner's guide to building, using, maintaining fuzzy systems. Boston: AP Professional. ISBN 0-12-194270-8

[12]. Ozyilmaz, L.; Yildirim, T.; "Diagnosis of thyroid disease using artificial neural network methods," Neural Information Processing, 2002. ICONIP '02. Proceedings of the 9th International Conference on , vol.4, no., pp. 2033- 2036 vol.4, 18-22 Nov. 2002 doi: 10.1109/ICONIP.2002.1199031