IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

A Review on Prevention of Attack using SVM as well as Fuzzy Logic

Lokeshwar Singh[1], Ashish Sharma[2]

M.Tech. Student, Department of Computer Engineering, BIMT Shimla, India [1]

Assistant Professor, Department of Computer Engineering, BIMT Shimla, India [2]

Abstract: Wireless Sensor Networks are modernizing the way; the people interact with the physical world. They comprise of small sensor nodes which have many capabilities such as sensing, monitoring, computation and wireless communications. They are deployed in large amounts to collect data from the environment, perform local processing and communicate their results. In this work, we investigate the Gray Hole Attack and its variants, which is very simple to implement but difficult to detect. In Gray Hole attack the malicious node works as a normal node but refuses to forward certain selected packets and simply drop them .Due to this nature, the Gray Hole attack is very harmful for mission critical applications and can damage the whole network communication, making the network useless .So, in proposed work utilization of two AI methods will be done i.e. SVM and fuzzy logic, in which comparison of both methods will be done in mitigation of gray hole attack in WSN network in MATLAB 2010a environment within required area.

Keywords: WSN, SVM, OLSR, Gray hole, Fuzzy sets.

I. INTRODUCTION

Wireless Sensor Network (WSN) technology enables design and implementation of novel; intriguing applications that can be used to address numerous industrial, environmental, societal and economical challenges and thus, the importance and potential of WSNs are constantly growing.

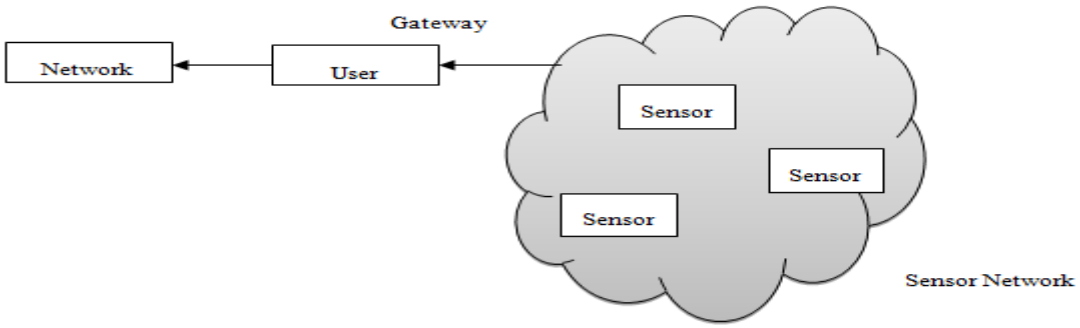

Fig. 1 Sensor Networks

A sensor node (as shown in the Fig. 1) is generally defined as a cheap and small piece of hardware, which consists of four main units:

• One or more sensors that detect physical phenomena. Common sensors monitor scalar values of temperature, pressure, humidity, light intensity, etc.

• The sensor is coupled with a data processing unit. The latter controls sensing, application logic and network transfer. It receives data from the sensors as well as it can filter (e.g. thresholding) compress or correlate data from a series of measurement. The network structure, the communication process and the power management of the node are also organized by the processing unit.

• The data's wireless transmission is provided by a communication interface.

• For every operational electronic system an energy source is needed.

Nodes in Wireless Sensor Networks (WSNs) sense data, find routes, and forward sensing data to a sink or BS that is usually far away from the data source. Since sensors usually have a small size, low-battery capacity, non-renewable power supply, limited processing ability, small buffer capacity, and a low-powered radio, WSNs pose new challenges to both industrial and academic communities [13]. A general approach employed in data gathering and data aggregation

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

is to construct a spanning tree which is rooted at the sink and connects all sensor nodes in the network [7]. If one node fails, the topology will be reorganized into a new topology. Tree maintenance is usually an energy-demanding operation [13]. A centralized system would mean that some of the sensors would need to communicate over long distances that lead to even more energy depletion. Hence, it would be a good idea to process locally as much information as possible in order to minimize the total number of bits transmitted.

II. GRAY HOLE ATTACK

It is a type of black hole attack. The packets use to fall in this with some probability. The gray hole attack exhibits varied number of malicious nodes. It has its own distinguishing behaviour [5]. A gray-hole attack exhibit a variety of malicious phenomenon. It fall packet impending on or after to definite exact node in a system as forwarding all packet from and to other nodes. There are two types of concepts lying in gray hole attack:
To detect this phenomenon attack is extremely hard except a system with wide detection algorithm exists, that is responsible for all the nodes performance in the network. Occasionally nodes are able to relate with each other and preserve recommended the malicious nodes survival to previous friendly nodes. The technology is same as Black-Hole attack where sequence number response may notice some Gray Hole attack. If multiple paths survive among sender and destination then buffer packets by suitable acknowledgement may notice lively Gray Hole attack in development although dormant or triggered attack is hard to notice with this approach.

Fig. 2 Gray Hole Attack

Node dependent attack: This type of attack drops **those** packets that moved toward the node that would be coming through definite node. For other nodes, it acts usually routing DATA packets towards the destination nodes accurately.

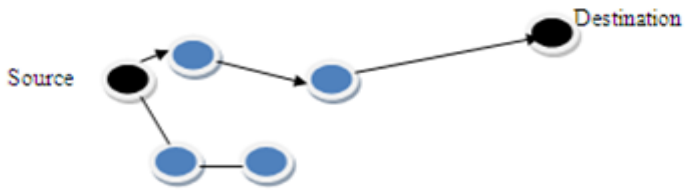

Fig. 3 Gray hole (Node Dependent Attack) (At time T1)

Time Dependent attack: It would drop DATA packets depends on numeral of pre-determined whereas behave usually throughout the other instance.

Fig. 4 Gray hole (Time Dependent) (At time T2)

III. FUZZY LOGIC

Fuzzy Model is the generalized model of previous classic models. As the output is not limited to only 0 and 1, so the theory of fuzzy logic is introduced. It is also known as diffuse logic. Difference between fuzzy logic and classical model is introduced using membership functions. Consider a finite set:

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

C= {c1, c2, c3….cn}
It is the universal set. Now according to graphical representation, suppose fuzzy sets have only two elements c1 and c2. So the degree of fuzzification can be called as entropy. Therefore entropy can be shown as [6]:

$E=\frac{f1}{f2}$; Where f1 and f2 are the distances

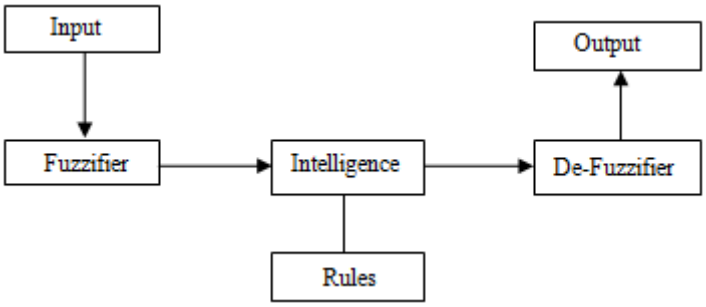

Fig. 5 Fuzzy Logic Model

IV. SUPPORT VECTOR MACHINES

Support vector machines (SVMs) are a binary classification algorithm developed by Vapnik. The main features of SVM are shown below, due to which its applications are quite important:

- Robust to large number of variables.
- It can be applied to learn complex and simple learning models.
- It avoid over fitting.

The advantages of support vector machines are:

- Efficient in high dimensional spaces.
- Still useful in cases where amount of dimensions is better than the number of samples.
- Uses a division of training points in the decision function (called support vectors), thus it is also memory efficient.
- Versatile: Dissimilar Kernel functions can be precise for the decision function. General kernels are provided, but it is also likely to identify custom kernels.

Using SVMs efficiently requires an accepting of how they work. When guiding an SVM the practitioner needs to make a number of decisions: how to pre-process the data, what kernel to use, and lastly, setting the parameters of the SVM and the kernel. Uninformed choices may result in strictly reduced performance.

V. OBJECTIVES

Aims and objectives of the work are summarized as follow:

a) To design a WSN network over MATLAB 2010a with various parameters like no. of nodes, length and width of network.
b) To design and implement Intrusion Detection system based on Computational method like fuzzy logic with rule sets and SVM method to detect gray-hole attack in network.
c) To validate gray-hole attack using proposed scheme and then evaluate QOS parameters.

VI. LITERATURE SURVEY

- Marigowald et.al has provided comprehensive information on types of attacks WSN is exposed to and possible methods of countering such attacks effectively. The motto here is to help novice researchers with objective to work on security challenges in Wireless Sensor Network environment [7].
- V.Kumar et.al has proposed some of the security goal for Wireless Sensor Network. Further, as security being vital to the acceptance and use of sensor networks for many applications; author have made an in depth threat analysis of Wireless Sensor Network. Lastly it proposes some security mechanisms against these threats in Wireless Sensor Network [8].
- Raja Wassem et.al has presented that security is a fundamental requirement for these networks. In this research, the center of attention is on physical attacks and issues in wireless sensor networks. Through this review, easily identify

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

the purpose and capabilities of the attackers. Further, well-known approaches of security detection against physical attacks have been discussed [9].

- Deepali et.al has proposed that the security of a wireless sensor network is compromised because of the random deployment of sensor nodes in open environment, memory limitations, power limitations and unattended nature. This paper focuses on various attacks that manifest in the network and provides a tabular representation of the attacks, their effects and severity. The paper depicts a comparison of attacks basis packet loss and packet corruption. Also, the paper discusses the known defence mechanisms and countermeasures against the attacks [10].
- K.Venkatraman et.al has presented multiple users that can use technique simultaneously over a single channel, therefore, security has become a huge concern. Even though there are numerous ways to secure a wireless network and protect the network from numerous attacks, providing 100% security and maintaining confidentiality is a huge challenge in recent trends. This journal will present you a survey about the various threats to wireless networks, the various advancements in securing a network and the various challenges in implementing the same [11].
- Mohammed Wazid et.al has presented the Wireless Sensor Networks (WSNs) that are inclined to different attacks in which Blackhole is a sort of Denial of Service (DOS) attack which is extremely hard to recognize and guard. In blackhole attack, the intruder catches and re-programs an arrangement of hubs in the system to obstruct the data they get as opposed to sending them towards the base station. Accordingly any data that enters the blackhole locale is caught and not ready to achieve destination bringing on top of the line to-end postpone and low throughput. Beforehand little measure of work is done only for identification and counteractive action of the Blackhole attack in the WSN making its discovery and avoidance extremely essential according to network execution is concerned. In this paper at first the influence of Blackhole attack was measured on the system parameters took after by the proposition of a novel method for the recognition and counteractive action of Black hole attack in WSN [14].

VII. PROBLEM STATEMENT

In proposed work, gray hole attack on the widely used OLSR routing protocol. Routing protocols are necessary to communicate with each other, so this work will utilise OLSR protocol. It has noticed from literature survey that computational methods are good for provision of accuracy, so usage of fuzzy logic will be done in this work. Then comparison will also be done by implementing with SVM method. The measurement of work will be evaluated using number of network parameters as shown below;

Throughput: it is the rate of invention or the rate on which a bit can be processed. When used in the framework of communication networks.

Packet Delivery ratio: it is defined as the ratio of data packets expected by destinations to those generated through sources. It can be taken as:

$$\mathrm{PDR} = \mathrm{S1} \div \mathrm{S2}$$

Where, S1 is the sum of data packets received by the each destination and S2 is the sum of data packets generated by the each source

End to end delay: The average time taken by data packet to reach the destination and includes all delays caused by buffering during route discovery latency, queuing at the interface queue. Mathematically, it can be defined as:

$$\mathrm{Avg.\,EED} = \mathrm{S/N}$$

S is the amount of the time spends to bring packet for each destination, and N is the number of packets received by the all destination nodes.

VIII. METHODOLOGY USED

Step 1 : Start
Step 2 : Initialize the network with various no. of nodes.
Step 3 : Enter width and length of network to implement network.
Step 4 : Calculation of X and Y location of nodes
Step 5 : Deployment of sensor nodes in network
Step 6 : Plotting of source and destination
Step 7 : Find source and destination
Step 8 : Find coverage set, and then find distance and then request HELLO message.
Step 9 : Optimize using fuzzy logic and SVM to find attack. Each layer represents a path which consists of sequences of positive integers that represent the IDs of nodes through which a routing path passes with the source node followed by intermediate nodes (via nodes), and the last node indicating the destination, which is the goal. Evaluate optimal route selection.
Step 10 : End

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 4, April 2017

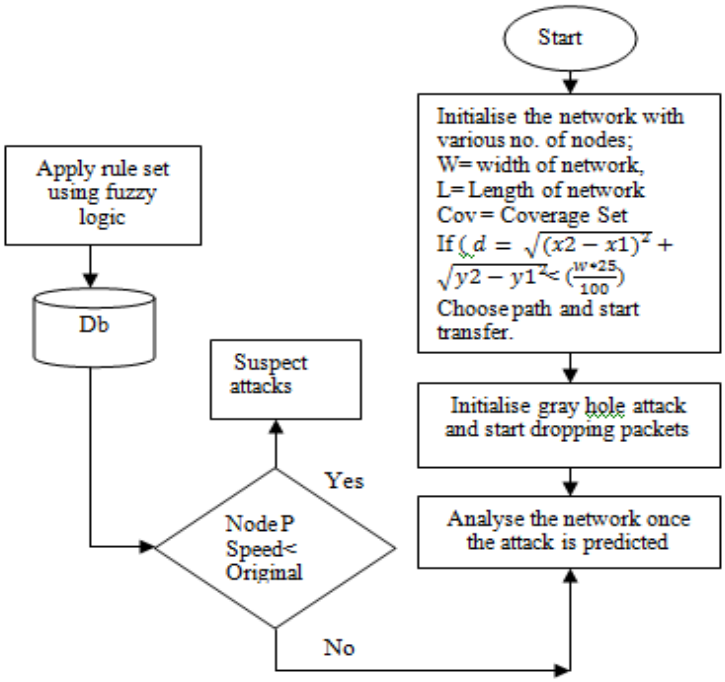

Fig.6 Proposed Flowchart

IX. CONCLUSION

Step 11: In wireless sensor network in MATLAB 2010 environment by considering length, width and number of nodes as the parameters for mitigation of gray hole attack. In this research, an Intrusion Detection system will be designed and implemented on the basis of computational method namely fuzzy logic consists of number of rule sets for the initialization of network with number of nodes (considering coverage set, length and width of the network) and for choosing the path for transferring the data and SVM (Support Vector Machine) for detecting the gray hole attack in the network.

REFERENCES

[1] Gursewak Singh and Rajni Bedi, "A Survey of Various Attacks and Their Security Mechanisms in Wireless Sensor Network", International Journal of Emerging Science and Engineering (IJESE), Vol. 2, Issue-8, 2014.
[2] Shio Kumar Singh, M P Singh and D K Singh, "A Survey on Network Security and Attack Defense Mechanism For Wireless Sensor Networks", International Journal of Computer Trends and Technology, 2011.
[3] Dr. Banta Singh Jangra and Vijeta Kumawat, "A Survey on Security Mechanisms and Attacks in Wireless Sensor Networks", International Journal of Engineering and Innovative Technology (IJEIT), Vol. 2, Issue 3, 2012.
[4] Huijuan Deng, Xingming Sun, Baowei Wang and Yuanfu Cao, "Selective Forwarding Attack Detection using Watermark in WSNs", International Colloquium on Computing, Communication, Control, and Management (2009 ISECS), pp.109-113, 2009.
[5] J. Brown and X. Du, "Detection of selective forwarding attacks in heterogeneous sensor networks", International Conf. on Communications, pp. 1583-1587, 2008.
[6] Guanrong, C, "Introduction to Fuzzy Sets, Fuzzy Logic and Fuzzy Control Systems", 2nd ed.; CRC Press: Houston, 2001.
[7] K Marigowda1 and Manjunath Shingadi, "Security Vulnerability Issues In Wireless Sensor Networks: A Short Survey", International Journal of Advanced Research in Computer and Communication Engineering, Vol.2, Issue 7, July2013.
[8] Vikash Kumar, Anshu Jain and P N Barwal, "Wireless Sensor Networks: Security Issues, Challenges and Solutions", International Journal of Information & Computation Technology, Vol. 4, pp. 859-868, 2014.
[9] Raja Anwar, Majid Bakhtiari, Anazida Zainal, Abdul Hanan Abdullah and Kashif Naseer Qureshi, "Security Issues and Attacks in Wireless Sensor Network", World Applied Sciences Journal, Vol. 30, pp.1224- 1227, 2014.
[10] Deepali Virmani, Ankita Soni, Shringarica Chandel and Manas Hemrajani, "Routing Attacks in Wireless Sensor Networks: A Survey, International Journal of Computer Science and Information Technologies, Vol. 5 , 2014.
[11] K.Venkatraman, J.Vijay Daniel and G.Murugaboopathi, "Various Attacks in Wireless Sensor Network Survey", International Journal of Soft Computing and Engineering, Vol.3, March 2013.
[12] Priya Maidamwar, and Nekita Chavhan, "A Survey on Security Issues to Detect Wormhole Attack In Wireless Sensor Network", International Journal on AdHoc Networking Systems (IJANS), Vol. 2, 2012.
[13] Md Abdul Azeem, Dr.Khaleel-ur-Rahman khan and A.V.Pramod, "Security Architecture Framework and Secure Routing Protocols in Wireless Sensor Networks -Survey", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.2, No.4, 2011.
[14] Mohammad Wazid and Avita Katal, "Detection and Prevention Mechanism for Blackhole Attack in Wireless Sensor Network", International conference on Communication and Signal Processing, IEEE, pp. 576- 581, 2013.
[15] Meenakshi Tripathi,M.S.Gaur and V.Laxmi, "Comparing the Impact of Black Hole and Gray Hole Attack on LEACH in WSN", The 8th International Symposium on Intelligent Systems Techniq, Procedia Computer Science, pp.1101 – 1107, 2013.