7th International Conference on Communication, Computing and Virtualization 2016

DoS attack prevention technique in Wireless Sensor Networks

Shital Patil[a], Sangita Chaudhari[b],*

[a]A. C.Patil College of Engineering, Mumbai University, Kharghar, Navi Mumbai, 410210, India
[b]A. C.Patil College of Engineering, Mumbai University, Kharghar, Navi Mumbai, 410210, India

Abstract

Wireless Sensor Networks (WSN) has wide applications in data gathering and data transmission via wireless networks. Due to the weaknesses in the WSN, the sensor nodes are vulnerable to most of the security threats. Denial-of-Service (DoS) attack is most popular attack on these sensor nodes. Some attack prevention techniques must be used against DoS attacks. There are different techniques to prevent DoS attack in wireless sensor network. In this paper, an immune system is proposed for the DoS attack on WSN which will improve the accuracy rate of attack prevention, reduce the false alarm rate and able to recognize different Dos attack.

Keywords: Dos attack, attack prevention, prevention in WSN;

1. Introduction

The WSN are flexible, easy to implement and straight forward. They are growing because of low cost and effective. It has wide applications in military, health care to gather data and data transmission. Due to security issues and limited resource energy, they are vulnerable to security attack. So there is a need to provide effective security mechanisms. The DoS attack is considered as one of the major attack on WSN. The main aim of DoS is the disruption of services by attempting to limit the access to a machine or service instead of subverting the service itself. This kind of attack aims at rendering a network incapable of providing normal service by targeting either the network's bandwidth or its connectivity. These attacks achieve their goal by sending at a victim a stream of packets that swamps his network or processing capacity denying access to his regular clients[1]. Most of the attack prevention

* Corresponding author. Tel.: +91-932-420-4088;
  E-mail address: sschaudhari@acpce.ac.in

techniques are based on soft computing, game theory, artificial intelligence and multi-agent approaches. Soft computing based approaches uses the fuzzy Q-learning algorithm, Decision tree. In game theory, a strategy is de fined for all possible situations and Nash equilibrium is the solution. Artificial intelligence uses the danger theory, dendritic cells. In multi-agent immune system, each agent has defined duties and goals[2].

The game theory framework based on Utility based Dynamic Source Routing (UDSR) is used as secure routing protocol which is derived from Dynamic Source Routing (DSR) and Watch-list is used to identify malicious node. Utility value is used to choose secure route. Cooperation and reputation are used to calculate node misbehavior. UDSR loses fewer fractions of packets due to malicious nodes, whereas regular DSR faces loss of more packets. UDSR is facing less loss comparing to DSR because DSR doesn't react to the bad behavior of nodes but UDSR and Watch-list isolate the node by labeling that node as malicious node. So that node in the network can be ignored and it won't be able to harm the network. The major problems are how to avoid the false labeling and how to set threshold values[3].

Auction theory is used to detect non-cooperative nodes. This approach uses UDSR protocol. Instead of utility value bid price is used to choose secure route. This protocol is named as Secure Auction-based Routing (SAR). To recognize malicious node timeout timer is used by destination. If the timer expires and before reaching packet to the destination, then bad route message to base station and all nodes will be placed into watch-list. If nodes comes more than a predefined number of times then base station will put that node into ignore list and it will broadcast that list. In SAR the average number of dropped packets stays steady, because nodes with bad reputation will be ignored by the majority. SAR loses fewer fractions of packets due to malicious nodes because it reacts to the bad behavior. It has same problems as UDSR, false labeling and threshold values[4].

The repeated game theory approach is based on game theory which recognizes the presence of nodes that agree to forward packets but fail to do so. It categorizes different nodes based upon their dynamically measured behavior. This framework enforces cooperation among nodes and provides punishment for non-cooperative behavior. Sensor nodes trust each other based on the reputation. To increase the reputation in the network, each node will participate fairly in packet transfer. Otherwise IDS will recognize the malicious nodes and isolates them from participating in network functions which will have less reputation. The benefit of this framework is that, the base station has a history of the previous games and when a node is malicious it gets a negative reputation when the total reputation accumulates, a path consisting of less number malicious nodes is chosen to be the winning path. This results in isolation of malicious nodes. To lower the rate of false positives and false negatives detection, it misses more malicious nodes[5].

A LEACH protocol is secured by using a Bayesian game which is called as S-LEACH. S-LEACH has different rounds, each starts with setup phase, and continues with a steady state phase. In setup phase cluster heads (CHs) are selected. For second phase, the cluster heads assign the time on which the sensor nodes belong to their cluster, can send data to them, based on a TDMA (Time Division Multiple Access) approach. The local intrusion detection system (IDS) would notify central IDS about malicious nodes. Then central IDS informs about malicious nodes to whole network. So local IDSs would be alerted to not assign any time for selfish nodes, and prevent wastage of system resources. The number of packets dropped is less than non-secured network. Throughput is high because CHs can check their member nodes more in their all located transmission times and recognize the type of them[6].

The AODV-HFDP (Ad-hoc On demand Distance Routing with Hello flood Detection cum Prevention) routing protocol is used to detect node that generates hello flood attack. Hello flood attack is an attack on the network layer. A hello message is used to indicate presence of node. On receiving a hello message, each node updates its neighbor table, to indicate route towards the base station node. To distinguish between a friend and a stranger a technique based on simple test packet is applied. The Hello message receiving node sends simple test packet to hello sending node, if the reply comes in allotted time threshold then hello sending node is considered as a friend, if not then it is classified as a stranger. After declaring the node as malicious, the information of hello sending node is deleted from the routing table and this information is broadcast throughout the network. All nodes in the network delete malicious node information from routing table. As compared to AODV, AODV-HFDP gives higher packet delivery ratio. But it works for homogeneous sensors, fixed signal strength[7].

An ant-based framework exploits the significance of stateless and stateful signatures and hence preserving the legitimate packets only, thereby discarding the contaminated packets. The Ant-Based Routing Algorithm is used. The attack is detected by DDA (DDOS Detecting Ants), if reliability changes or buffer size exceeds the threshold

value. DDA detects unusual rise in network traffic. This rise can be flooding so to find the reason the sample packet is sent to adjunct node that is DPA (DDOS Preventing Ants). DPA notices the difference between the current numbers of arriving packets on the node with sample packets. The legitimate packets remain unaffected by attack avoids false labeling. Fewer resources are consumed. Also helps in detecting the source of traffic[8].

Message observation mechanism (MoM) is based on the spatiotemporal correlation. MoM utilizes the similarity function to identify the content attack as well as the frequency attack. And then the MoM adopts rekey and reroute countermeasures to isolate the malicious node. The MoM is deployed in CH due to sink function of CH. The MoM consists of three components: normal message list (NML), abnormal message list (AML) and observation mechanism (OM). To detect DoS attack, two aspects are considered the number of messages and the content of messages. If new message belongs to AML then it is declared as bogus message. If the message is received by CH more than threshold number then it is declared as replayed message. After detecting the malicious node, CH announces the ID of malicious node and refuse to forward its messages. The cluster key session key and the pair wise key are changed. Filters are used to send the key to cluster members which will filter the malicious node. New routes are built to CH. This mechanism reduces the loss of packets as the number of malicious nodes increases. MoM not only detects and defenses the DoS attack but also can reduce the energy consumption because it does not forward packets from malicious node further[9].

Hybrid Energy-Efficient Distributed clustering (HEED) protocol is used for clustering of sensor nodes. The CHs is selected by using two clustering parameters, residual energy of each node and intra cluster communication cost which is a function of node degree or cluster density. HEED prolongs the network lifetime than LEACH. If any node failed to do mutual authentication then that node is declared as malicious node. When a CH detects a malicious or compromised node, it requests the KDS to disrupt the operations of a compromised or malicious node. The KDS simply deletes the secret key of that node from KDS records which results in keyless node. Then all the services are cancelled and blocked for detected node for future requests. CHs send an encrypted message to all other cluster heads about the detected malicious node to block it for inter cluster communication. The remaining clusters do not be disrupted from its operations. It not only defends the wireless sensor network against DOS attacks but also maintains integrity, authenticity and confidentiality between sensor nodes. If the attacker knows our mechanism then cluster can be malicious. This technique is efficient and accurate[10].

The cooperative Game-based Fuzzy Q-learning(G-FQL) is a combination of both the game theoretic approach and the fuzzy Q-learning algorithm in WSNs. Regardless of whether the attacks are carried out on a regular or irregular basis, the IDPS can adjust its learning parameters through fuzzy Q-learning to identify future attacks. It is a three-player strategy game consisting of sink nodes, a base station, and an attacker. The sink node monitors message attacks through the game-based FQL operation. Upon completing the first stage, the sink node transmits an alarm to the base station when the attacker assaults the sensor node. Upon receiving an abnormal signal from the sink node, detection fitness test is used in conjunction with the knowledge database to assess attack patterns and severity. It also informs the affected sink node that it needs to protect itself against the offending attack pattern. If the sink node still detects an irregularity, then the sink node advises to revise its detection strategy. The process continues till attack condition is resolved and returns to the correct state of defense strategy. The sink node notifies IDS2 that the attack at the sensor node has been successfully counteracted and the attack has ceased. The IDS2 thus concludes defending the sensor node. By integrating the game theory with the Fuzzy Q-training method, performance surpasses that of any other individual defense approach. The Game-FQL preserves a greater number of sensor nodes during simulation. The cooperative game-based FQL method enhances energy efficiency via optimization[11].

Cooperative fuzzy artificial immune system (Co-FAIS) continuously sniffs data from the network and inspects the sensor's behaviour. It consists of six modules: Sniffer Module, Fuzzy Misuse Detector Module, Danger Detector Module, Fuzzy Q-learning Vaccination Module, Cooperative Decision Making Module and Response Module. The sniffer module seizes packets from the network traffic online and to examine transmit it to the detection module. The sniffed data is fed to the offline system in case of high traffic volumes, and the outcome is saved in a log file. To pre-process packet features, a fuzzy rule-based packet analyser serves as a detection module. The Fuzzy Misuse Detector Module computes the match between packets and self-packets and then reports the highest matching value. The FMDM consists of the following components: capturing traffic, feature extractor, fuzzification, the fuzzy inference engine, knowledge base, and the expert analyser. Feature extractor captures the network traffic and creates the threat profile. The threat profile is based on CPU usage (Eu), memory load(Bs), bandwidth saturation(Tr), connection

numbers(Co). In fuzzification, input/output linguistic variables are defined. And also membership functions are defined. The knowledge base stores the fuzzy rules used by the fuzzy inference engine to obtain a new fact. The expert analyser decides the influence result from defuzzification, as to whether inspected packets are attacked or not. The Danger Detector Module compares the usage profile of the current system against that of the normal system saved in the profile database, and checks for possible deviations and measure their degree. It is used to recognize new attacks. Fuzzy Q-learning Vaccination Module updates information regarding the system in terms of thresholds, profiled resources, etc., by examining the behaviour of a real attack in a monitored environment and checking the system's ability to react and defend itself. Cooperative Decision Making Module combines the outcome from the FMDM and FQVM detector. A consolidated result is obtained, along with analysis of attack source that portrays what the real cause of the attack may be and the name of the attack if it is known by the system. Response Module updates databases or modifies hosts in the network. The response module produces an attack signature and eliminates it from the safe list, so response will be faster to the same attack in a repeat case. The response module functions as a prevention system by taking online action to break the attack instantaneously. The cooperative-based FAIS give higher accuracy score. It gives higher detection rate. It also preserves a greater number of sensor nodes. The energy consumption rate is lower. But training time is large[2].

The table 1 shows the comparison of various Dos attack Prevention techniques.

Table 1. Comparison table for DoS attack prevention techniques

Name of the technique	Malicious behaviour	Good Behaviour Pay-off	Parameter	Protocol	Evaluation Parameter
Game Theoretic Approach	Black holes and falsify route error message	Reputation	Reputation, Cooperation, Utility, Density, Reliability, Distance, Weight Parameters	Utility based Dynamic Source Routing (UDSR)	Mean no of packets dropped
Enforcing Security Using Economical Modeling	Non cooperative nodes.	Reputation.	-	SAR (Secure Auction-based Routing)	Mean no of packets dropped, Reputation,
Repeated Game Theory Approach	Agree to forward packets but fail to do so	Reputation	Cost of forwarding packet, History, Rating, Reputation, Utility, Weight	Repeated Game Theory based on DSR	Number of hops for received packets, Throughput
A Bayesian Game Approach	Non cooperative nodes.	Reputation	-	S-LEACH	Number of packets dropped, Throughput
Strength based Detection and Prevention	Reply of Hello message	Signal Strength	Signal Strength	AODV routing protocol	Total packet received Total packet dropped Packet delivery ratio
An Ant Based Framework	Flooding	Reliability, buffer size	-	Ant-Based Routing Algorithm	-
Protection using KDS	Node replication, Capture nodes.	Mutual Authentication	-	Hybrid Energy-Efficient Distributed clustering (HEED) protocol	Network Lifetime, energy Used
Message Observation Mechanism (MoM)	Content attack, Frequency attack	NML AML	The number of messages and the content of messages.	message observation mechanism (MoM)	Loss Rate of packets, Number of packets
Cooperative game theoretic approach	-	Reputation	cost for attack detection, ratio of correct attack detection to no detection and total detection	Fuzzy Q-learning algorithm	accuracy of defence rate, number of live nodes, energy consumption

Cooperative fuzzy artificial immune system(Co-FAIS)	-	Reputation	energy usage, time response, buffer size, count	Co-FAIS	accuracy of defence rate, number of live nodes, energy consumption

The techniques are compared based on routing algorithm, evaluation parameter, parameter considered for attack detection, malicious behaviour of node and good behaviour. Each technique finds the malicious node and tries to isolate it from the network to avoid the DoS attack. Co-FAIS identify the attack behaviour and alert the attack pattern to its member node to improve the security of network. But it has certain drawbacks such as lacks in learning capabilities and is based on a normal model generated online which does not change over the time during detection.

In this paper, an immune system is proposed for DoS attack on WSN. There are some major issues to consider. As the wireless sensor is growing fast, providing security to sensor node is difficult tasks. While preventing a DoS attack, it should not degrade the performance of the system. It should maintain the accuracy. False alarm rate should be low. The prevention system should survive in repetitive attack on same node. In our proposed system we are considering new learning parameters which will improve system accuracy as well as detect different attacks. The rest of paper is organized as follows: section 2 represents the framework of proposed system, section 3 represents the conclusion.

2. Proposed System

Co-FAIS is an immune system for DoS attack on WSN. It is the first real time intrusion detection model. It compares current system with normal system to recognize the attack by using fuzzy logic. But it has some disadvantages such as lacks in learning capabilities and based on single normal model which does not change over the time during detection. So there is need to update the normal model which is compared with current system. To improve the learning capabilities more learning parameters can be added in the system. The proposed immune system will improve the current Co-FAIS by adding two learning parameters in fuzzy system. It will improve the accuracy rate of detection and improves learning capabilities.
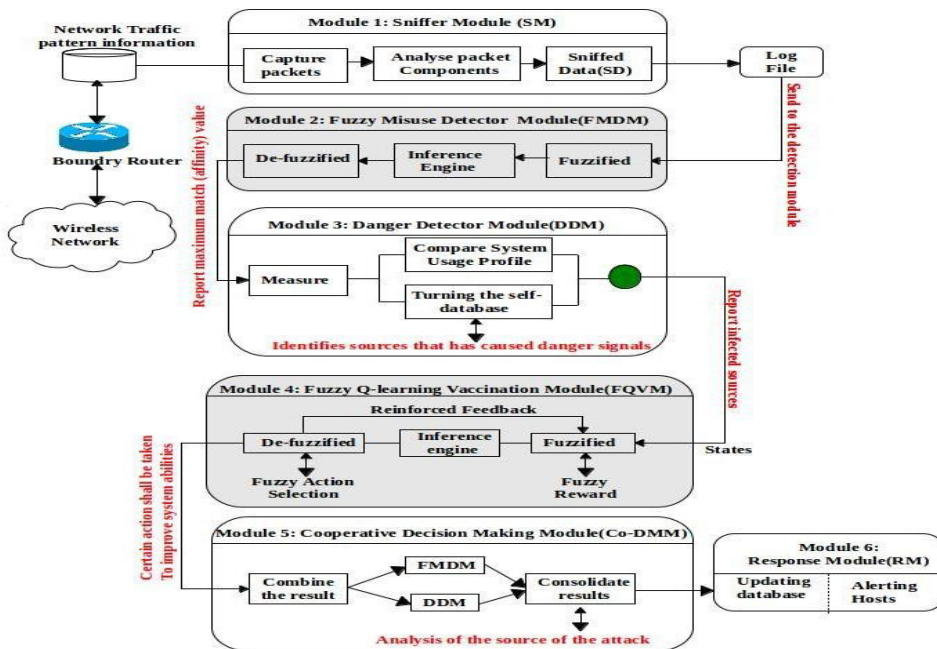

Fig. 1 Proposed Immune System

There are six modules in the proposed immune system: Sniffer Module (SM), Fuzzy Misuse Detector Module (FMDM), Danger Detector Module (DDM), Fuzzy Q-learning Vaccination Module (FQVM), Cooperative Decision Making Module (Co-DMM) and Response Module (RM). The Fig. 1 shows proposed immune system for DoS attack on WSN. In shaded region shows the two fuzzy modules. In proposed system we changed the number of learning parameters. We added two more learning parameter with existing Co-FAIS i. e. Throughput and Sleep Interval.

2.1. Sniffer module

It grabs the packets from networks online and for pre-processing it sends to the Fuzzy misuse detection module. It creates the log file of packets.

2.2. Fuzzy Misuse Detector Module

It is a fuzzy based module which identifies the malicious packet. It compares the current packet with normal packet reports the values which are crossing the threshold value. It consists of capturing traffic, feature extractor, fuzzification, the fuzzy inference engine, knowledge base, and the expert analyzer. Feature extractor captures the network traffic and creates the threat profile. In existing system the threat profile is based on CPU usage (Eu), memory load (Bs), bandwidth saturation (Tr), connection numbers (Co). In existing system the threat profile is based on CPU usage (Eu), memory load (Bs), bandwidth saturation (Tr), connection numbers (Co). In the proposed system number of parameters is increased. With the existing parameters two new parameters are added in the proposed system throughput (Th) and sleep interval (Si) which will improve the system accuracy. Now, threat profile (TP) is defined by six parameters TP = {Eu, Bs, Tr, Co, Th, Si}, where Eu denotes the sensor node's energy consumption; Tr is the variance of time difference between two connections during a specific time window; Bs denotes the length of the packet from source to destination; Co is the number of connections to the same host as the current connection in the last two seconds. Tt is throughput is the number of successfully received packets in a unit time. Si is the sleep interval of the node. In fuzzification, input/output linguistic variables are defined. Table 2 shows these variables. And also membership functions are defined. The knowledge base stores the fuzzy rules used by the fuzzy inference engine to obtain a new fact. The expert analyzer decides the influence result from defuzzification, as to whether inspected packets are attacked or not.

Table 2. Fuzzy linguistics and abbreviations of variables for each parameter.

Parameters	Inputs linguistic variables	Range
Energy usage (Eu): Joule	Low (L), Medium (M),	0-100 (J)
Buffer size (Bs): kb	High (H)	4-7068 (Kb)
Time response (Tr): ms		0-120 (ms)
Count (Co): ms		1-3 (%)
Throughput (Tt): bps		75-100(%)
Sleep Interval: ms		5-100(ms)

2.3. Danger Detector Module

If attack is detected then this module calculates the difference between parameters of malicious packet and normal packet. And it is saved into database to find new attacks.

2.4. Fuzzy Q-learning Vaccination Module

The real attacks are observed in this module. It checks the system abilities to detect and defend the attack. The Fuzzy Q-learning algorithm is used to detect the attack. In this algorithm the fuzzy min-max action selection and reward function with conventional Q-learning is used. It consists of fuzzy controller which converts the continuous

inputs into fuzzy sets. Six fuzzy sets have been defined for the fuzzy Q-learning input to represent six different situations as a Q-learning state space. The fuzzy Q-learning inputs, given by Energy usage (Eu), Time response (Tr), Buffer size (Bs), and Count (Co), Throughput (Th), Sleep Interval (Si) correspond to the network's fuzzy state. Abnormality is the output of the FQL which represents the action of agent A(t). Fuzzy rules are defined based on the fuzzy inputs. Fuzzy states(s) are considered in modeling the detected attack behavior. The FQL agent assigns a weight to all possible next states based on fuzzy logic controller (FLC). Through association to the threshold value, optimal cost may be achieved.

2.5. Cooperative Decision Making Module

This module combines the outcome from the FMDM and FQVM detector. It gives consolidate results and analysis of attack source.

2.6. Response Module

This module updates databases or modifies hosts in the network. To make prevention faster it produces an attack signature and eliminates it from the safe list.

3. Conclusion

Dos attack reduces the performance of the system. The privacy and security of data are the major issues concerning about the wireless sensor networks. Special prevention techniques are required to deal with the DoS attacks in WSNs. There are some approaches and techniques to prevent DoS attacks on the system. Our proposed cooperative immune system is an enhancement to the existing immune system, Co-FAIS. It improves the accuracy of the system. It reduces the false alarm rate. Two different parameters are used to analyse the attack.

References

1. Christos Douligeris and Aikaterini Mitrokotsa. Ddos attacks and defense mechanisms: classification and state-of-the-art. Computer Networks, 44(5):643–666, 2004
2. Shahaboddin Shamshirband, Nor Badrul Anuar, Miss Laiha Mat Kiah, Vala Ali Rohani, Dalibor Petković, Sanjay Misra, and Abdul Nasir Khan. Co-fais: cooperative fuzzy artificial immune system for detecting intrusion in wireless sensor networks. Journal of Network and Computer Applications, 42:102–117, 2014
3. Afrand Agah, Kalyan Basu, and Sajal K Das. Preventing dos attack in sensor networks: a game theoretic approach. In Communications, 2005. ICC 2005. 2005 IEEE International Conference on, volume 5, pages 3218–3222. IEEE, 2005.
4. Afrand Agah, Kalyan Basu, and Sajal K Das. Enforcing security for prevention of dos attack in wireless sensor networks using economical modeling. In Mobile Adhoc and Sensor Systems Conference, 2005. IEEE International Conference on, pages 8–pp. IEEE, 2005.
5. Afrand Agah and Sajal K Das. Preventing dos attacks in wireless sensor networks: A repeated game theory approach. International Journal of Network Security, Vol.5, No.2, PP.145–153, Sept. 2007
6. Maryam Mohi, Ali Movaghar, and Pooya Moradian Zadeh. A bayesian game approach for preventing dos attacks in wireless sensor networks. In Communications and Mobile Computing, 2009. CMC'09. WRI International Conference on, volume 3, pages 507–511. IEEE, 2009.
7. Virendra Pal Singh, Aishwarya S Anand Ukey, and Sweta Jain. Signal strength based hello flood attack detection and prevention in wireless sensor networks. International Journal of Computer Applications (0975–8887) Volume, 2013.
8. Dimple Juneja and Neha Arora. An ant based framework for preventing ddos attack in wireless sensor networks. arXiv preprint arXiv:1007.0413, 2010.
9. Yi-ying Zhang, Xiang-zhen Li, and Yuan-an Liu. The detection and defence of dos attack for wireless sensor network. The journal of china universities of posts and telecommunications, 19:52–56, 2012.
10. Dines Kumar.V.S and Navaneethan.C. Protection against denial of service (dos) attacks in wireless sensor networks. International Journal of Advanced Research in Computer Science & Technology, 2:439–443, March 2014.
11. Shahaboddin Shamshirband, Ahmed Patel, Nor Badrul Anuar, Miss Laiha Mat Kiah, and Ajith Abraham. Cooperative game theoretic approach using fuzzy q-learning for detecting and preventing intrusions in wireless sensor networks. Engineering Applications of Artificial Intelligence, 32:228-241, 2014.