International Journal of Engineering Research and Technology. ISSN 0974-3154, Volume 14, Number 6 (2021), pp. 588-592

Implementing Network Security in Wireless Sensor Network with Honeypot System

Dinesh Kumar Gupta[1] and Dr. Deepika Pathak[2]

[1]Research Scholar, School of Computer Science and Applications, Dr. APJ Abdul Kalam University, Indore (M.P.) India.

[2]Vice-Chancellor, Dr. APJ Abdul Kalam University, Indore (M.P.) India.

Abstract

Honeypot is a moving new technology with much prospective in the network security system. It is a resource which is proposed to be attacked and co-operated to gain more information about the attacker and his attack techniques. It is a very flexible tool that comes in many forms.The objectives is to provide security with energy efficiency in the wireless sensor networks (WSN) by using Honeypot system. The Honeypot system is a fake node plays dynamic role in the WSN that attract the attackers. It finds attackers ID, analysis types of attacks and energy consumption by the attacks. Then it alert base station without disturbing the network. The Base station can easily identify intruder or attacker using honeypot and alert all sensor nodes. So, every node is able to identify the attackers before the actual attack. When node becomes under attack, it gives problem in data collection. Honeypot avoids attacked node and achieve good level of energy efficiency, life time, success rate and throughput ratio. Also it reduces the vulnerability. Honeypot system makes prevention from the attackers. It is used for early warning to network as detect attacker and types of attacks. It improves the intrusion detection systems (IDS) and helps in designing better tools for network security.

Keywords: Wireless Sensor Networks (WSN), Security, Honeypot, Attack, Attacker, Intrusion Detection System (IDS).

I. INTRODUCTION

I.I. Honeypot

The Honeypot is a system developed for analyzing and detecting malicious attacks which attempting to get access to the network without permission. The Honeypot is a decoy machine which looks like a real server, real database and real operating system to the attackers. The Honeypot attracts the attackers. Attackers believe that there is some vulnerable weakness at your system. So they may be used to break and get access to your system. The main aim of honeypot system is to hide its existence from the attackers. Honeypot observes the activity of the attacker and create logs for their activity and try to get as more information as possible by asking some questions. It obtains the IP address through which attackers what to get access. Based on this information, Network Administrator know about the attackers with its location in the network and its purpose. [1]

I.II. Wireless Sensor Network (WSN)

The WSN is a collection of sensor nodes deployed in remote areas for various purposes like data aggregation, agriculture, automation, traffic management, environment monitoring, tragedy finding and military purpose. Each sensor node is capable of sensing, processing and communicating the required information. The components of the sensor nodes are microcontroller, transceiver, external memory and small battery power source. Data aggregation is defined as the method of collection of data from multiple sensors to remove unnecessary transmission and provide information to the Base Station (BS).

The attacked node injects false data and reduces energy efficiency of that node which gives abnormal situation to the BS. Our goal is to build a system that inform to administrator about attacks and achieve secure data aggregation with energy efficiency in sensor network. Honeypot is manipulated by BS and it is used to obtain information about the attackers. A honeypot stores a lot of data, whose data can be attacked and it is also expected to get explored and possibly broken. It does not fix anything and provide us with additional information about hackers or attackers. This system used for early warning, improves the intrusion detection systems (IDS) and in designing better tools for security.

BS sends the query and collects the sensed data from every sensor nodes in the network. Generally, every sensor node forwards its collected information to the intermediate node and finally BS processes the received data. The data aggregation aims to rise the network life time by reducing the resource utilization of sensor nodes. [2]

For creating Honeypot system the widely used tools are Honeyed, Nepenthes, KFsensor, Honeywell etc.

I.III. Attackers

Attackers are the unauthorized persons who want to misuse the information of any organization by braking network using hacking techniques. There are two types of attackers: outside attackers and inside attackers.

(1) Outside attackers are the persons who are unauthorized users means they are not authorized to access the network system

(2) Inside attackers are those persons who are authorized users and have access rights but they may use sensitive data to get profit either by leaking information to the others or using this information in wrong way which can loss the organization and to get profit for him.

I.IV. Intrusion detection systems (IDS)

Intrusion detection systems (IDS) are used to find attacks and attackers. IDS monitors wrong activities in the network and produce reports to the administrator. IDS are focused on identifying possible events, logging information about them and reporting to administrator. IDS distinguish between traffic coming from the client and the traffic coming from the attackers. IDS can be classified into three types.

(1) Anomaly Based Detection: It defines the network behavior; its predefined behavior is prepared or learned by the terms of the network administrators.

(2) Signature Based Detection: The signatures are determined by previously recognized attacks that are generated and referenced to detect attack in future.

(3) Specification Based Detection: A set of requirements and constraints that describes the correct operation of a program or protocol is defined.

The IDS requirements are:

- It should not degrade the network
- It should be reliable and minimum false positives and false negatives
- It should be transparent to the nodes and users
- It should be energy efficient

IDS challenges every node is independence from others and communications are controlled by Base Station (BS) managed by an administrator.

The IDS Challenges are:

- Sensor nodes are resource constrained
- Lead to increase network lifetime
- Sensor nodes have chances to fail or disappear from the network
- Requiring to monitor, detecting, responding to the intruders

Honeypot does not replace as standard IDS but it can be replace as IDS with more central point on information gathering of the attackers. [3]

II. INTRUSION DETECTION SYSTEM (IDS) WITH HONEYPOT

The term Honeypot was first presented by Lance Spitzner in 1999 in his paper “To Build a Honeypot” [4]. The honeypot works as an IDS and its fake access point implemented by an administrator that responds with fake data to the intruder. Honeypot allows different kinds of attacks and alert BS. Attackers easily attracted by this node. Who is visiting honeypot is known as an intruder. Honeypot is an IDS that appears an ordinary server, but all data and transactions are not genuine and find intruder techniques and determine vulnerabilities. Honeypot is accepted to get investigation on attacks. Honeypot do not fix anything. It provides the information to the administrator about attacks. Two popular reasons behind Honeypot are that

1. Study how attacker gain access to sensor nodes and maintain the records of attacker’s activities.We can gain awareness into attack methodologies to improve our real systems.
2. Collect information of attackers to alert all sensor nodes.

A honeypot in WSN waits for poor interaction. Interaction is needed to activate a honeypot. We have following advantages of Honeypots with IDS.

- Only transfer of information in Honeypot is attacker’s information
- Makes easier to analyze the attacker’s behavior
- Makes attackers to waste their time
- Disturbing the attackers
- Estimate energy taken by the attackers in the node also alerts the Base Station BS
- Provide security to actual server

III. ROLE OF HONEYPOTS IN NETWORK SECURITY

The Honeypots can be considered to be one of the latest technologies in the network security today. Honeypot is actively involved in deployment. Honeypots are used widely in research. [5]

Honeypots are used to know the attackers better. A classic web server may get millions of hits every day. So it gets quite difficulty to identify the attackers from the users. So we put honeypots in our same network system. Honeypots are just used to attract the attackers. If we get hits on our honeypots, we can distinguish the attacker from the users. As honeypots have no authentic uses, we trace back the attackers and improve our network security. [6]

IV. GOAL OF SETTING UP A HONEYPOT

We have used the concept of honeypots for providing security against attackers. A honeypot computer system is set up to act as an easily attacked. There are two goals for setting up a honeypot.

1. From the logged information learn, how the attackers investigate into the network
2. Collect appropriate proofs for attack of the attackers to submit to administrators for legal action.

To achieve these goals, the honeypot systems should satisfy certain conditions.

1. The honeypot system should be similar to other network systems.
2. Usage of interesting information in honeypots to attract hackers.

3. Restrict the traffic sent out to the Internet by an attacker or intruder.

V. WORKING OF HONEYPOT

Honeypot system works on the concept that all the traffic coming to the Honeypot system is suspicious or doubtful. Honeypot system looks like a real server. The only difference between honeypot system and real system is the location of the machine related to the real server. Honeypot is placed somewhere in WSN as shown in fig. 1. This means real server is hidden or invisible to the attackers. Generally, Honeypot system are planned to monitor the activity of an attacker, save log files and record events such as processes started, compiles, file adds, deletes and changes. By gathering such information, honeypot system improves the overall security system of the organization. If sufficient information is gathered, it may be used to legal proof in serious conditions. This data is used to measure the skill level of the attackers, their intension and even their identities. [1]

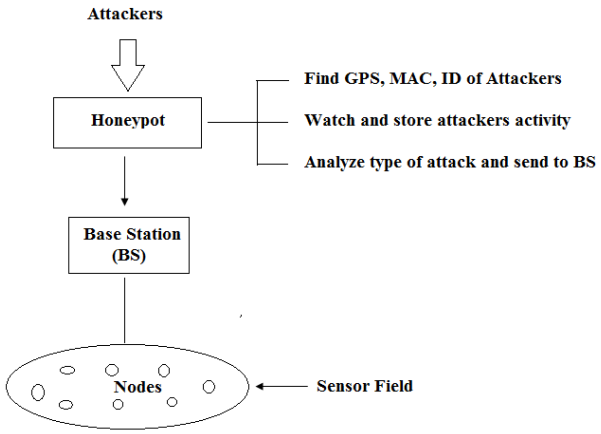

Fig. 1. Protect WSN with Honeypot System

VI. PROCEDURE OF HONEYPOT SYSTEM

1. Honeypot is a decoy system, it attracts the attackers.

2. Who enter into the Honeypot system are attackers.

3. To find attackers, Track

- GPS (Global Position System)
- MAC (Medium Access Control)
- Unique ID of attackers

4. Store Identification of attackers in the database.

5. Watch attacker's activity like

- Newly added information in Honeypot by attackers
- Modification done by attackers
- Theft by attackers
- Denial of Service (DOS)
- Denial of Sleep (DOSL)

6. Log all transactions done by attackers.

7. Honeypot system analyzes type of attack by using all logged transactions.

8. Estimate energy consumed by attackers.

9. Finally send details to Base Station (BS) include Attacker's ID, Types of attack, Energy Consumption.

10. Base Station receive attackers detail from Honeypot and add attackers in Blocked list.

11. Base Station alerts all sensor nodes about blocked list in database and avoid node become under attack.

12. Honeypot system sent follow-up request to the attackers.

VII. PROPOSED HONEYPOT SYSTEM WITH ALGORITHM

The Honeypot is a decoy system, it attracts the attackers. Honeypot system desires to watch unauthorized activities in the network. All authorized nodes know about fake node (Honeypot). When attackers interact with Honeypot system, it must do the following activities: (for abbreviation, follow Table 1 and Table 2)

Table 1. Possible type of attacks

Type of attack	Description
Warm Hole attack	There are two or more malicious nodes present in the network at different locations. When sender node sends information then one malicious node passed the information to another malicious node. Then the receiving malicious node sends the information to its neighbour nodes. In this way, attacker prove to the sender and receiver nodes that they are situated at a distance of one or two nodes but actual distance between these two are multiple nodes and usually both are out of range.
Hello Flood Attack	To discover the neighbours, the HELLO message is broadcasted by the nodes. The receiver node considers that the source node is in the range of data transmission and sends its data to the broadcaster. In a HELLO Flood Attack, HELLO message is broadcast with high transmission power by the attacker. The nodes which receive this HELLO message send the data packets to the attacker node. The attacker can change or modify the data packet or drop the packet. In this way, a lot of energy is wasted and also network over crowding occurs.

Selective Forwarding Attack	A malicious node in the network interrupts the communication process. There may be the case of multiple malicious nodes in the network that depends upon the attacker. This node selectively forwards some of the received packets. This malicious node can also be referred as a black hole as it may drop all the received packets. In such case, neighbouring nodes assumes that this has failed and starts searching for another route.
Sybil Attack	A single attacker makes and presents different identities to the other nodes. It can also be considered that "It can be in more than one place at a time". The malicious nodes are known as Sybil nodes. It makes confusion in routing.
Sink Hole Attack	A malicious node advertises fake routing information to attract the network traffic.
Black Hole Attack	Advertise short distance to all destinations and it drop all the received packets.
Denial of Service	Reduce the network bandwidth and unavailability of resources.
Denial of Sleep	Attackers interact continuously with the system and not allow taking rest, Waste Energy of node
Routing Table Attack	Attackers inject malicious routing information in routing table

Table 2. List of Abbreviations used in this system

Terms	**Description**
H	Honeypot
A	Attacker
ID1	GPS (Global Position System) of Attacker
ID2	MAC (Medium Access Control) of Attacker
ID3	Unique ID
DB	Data Base
D	Data
DOS	Denial of Service
DOSL	Denial of Sleep
TOA	Type of Attack
E1	Energy level before attacker entered
E2	Energy level after attacker attacked
EC	Energy Consumption
BL	Block List
FR	Follow up Request
RIB	Routing Information Base
BS	Base Station
SN	Sensor Node

(1) Identify attackers: To find the attackers, Track GPS, MAC, Unique ID of attackers. Store Identification of attackers in the database (Hidden Information)

[H] ← [A]

A[ID1] ← getGPS[A]

A[ID2] ← getMAC[A]

A[ID3] ← getID[A]

DB[ID1,ID2,ID3] ← A[ID1], A[ID2], A[ID3]

(2) Analyze type of attack: Honeypot system is expected to get attacked by attacker. It watches and store attackers activity in Hidden database. It analyze type of attacks and stored in database.

DB[A] ← [A([D])]

TOA ← Type of Attack

DB[TOA]←TOA

(2.1) Attack on Routing Table: Routing table or RIB is a table stored in the node that lists the routes to particular network destinations. Routing table holds information about the topology of the network immediately around it. Attackers may try to attack routing information of networks. In this type of attack, attacker node advertises routes to non-existent nodes, to the authorized nodes present in the network. Routing table attack causes an overflow of the routing table, prevent creation of entries to new routes to authorized node. Also modify genuine route updates and send data to unauthorized node. Create a fake routing table RIB, allowing attackers to access the FR.

DB[A] ← [A([D])];

TOA ← Attack on Routing Table

DB[TOA] ← TOA

Attacks on routing table mean, attackers try to create various attacks discussed in **Table-1**. If attacker accesses the routing table information, Honeypot alerts BS about possibilities of attack using routing table.

(3) Estimate energy consumed by attackers: Energy consumption can be calculated by energy before attackers entered and after attackers attacked.

E1 = Energy consumed before attack

E2 = Energy consumed after attack

EC = E1 – E2

DB[EC] ← EC

(4) Alert BS: After attackers attack the honeypot system, it analyze type of attack and energy consumption and send details of attackers ID, TOA, EC to the BS. The BS receives attacker's information and store in BL.

BS[BL] ← H(A[ID]) (attacker's ID)

BS[BL] ← H(A[TOA]) (Type of attack)

BS[BL] ← H(A[EC]) (Energy Consumption)

(5) Alert all SN by BS: BS alerts all sensor nodes SN to avoid this attacked node.

SN ←BS[BL]

(6) Send Follow-up Request: Finally BS alert by Honeypot system then its send follow-up request to the attackers to watch further attacks of attacker.

[A] ← H[FR]

Follow up request not create any burden to the sensor network as well as it can follow the attacker goal for further stimulate the attackers for further attack and try to waste their time.

VIII. HONEYPOT IMPLEMENTATION

When a System developer wants to develop a honey pot there is an important point to be remember. How to hide that it is honeypot system from the attackers. This point is used to implement the honeypot.

This is an application which allows setup of multiple virtual systems (honeypots) on a single machine or node, each with different services and behavior. It simulates a network stack of various operating systems to the attackers and makes him believe that they are interacting with the real system not with the honeypot system.

When the attacker sends a packet to the virtual honeypot, then the packet is forwarded to the host machine by router. After receiving the packet, router checks its routing table that the forwarded address of virtual honeypot exists in it or not. If it exists, then router send ARP request for the virtual honeypot to determine the MAC address of host. If it does not exist then the router dropped the ARP request. [1]

In this paper, we have implemented the honeypot system for capturing hacker information like IP address. In a honeypot computer, a fake website is made available. A login page is displayed which requires the Login ID as the identification number and a password to enter into the company network. Suppose a hacker tries to intrude into the company network by providing wrong information or use SQL injection techniques, and then a log is captured for the provided details. The honeypot system allows the hacker to enter into the login page as if his login details were validated and displays the page for doing something, which is ultimately a fake page and thereby no harm can be done to the company. By this way, a honeypot can be used to capture hacker information interfering into a network.

The proposed system can block particular IP address of hackers and also provide indications to network administrator for taking legal action. Network administrator should restrict these issues by using strong gateways. The Log size is also a major constraint to be looked after. Growing logs are always a weak performance and suitable steps should be taken for removal them in regular intervals.

IX. CONCLUSION

An attacked node in wireless sensor network is a challenging one to achieve secure data transfer and collection. Attacked node reduces energy efficiency of sensor nodes. The proposed system creates a fake server node called Honeypot, which attracts the attackers and agree to carry out all types of attacks with us. This system redirects the attacker to honeypot system also motivate them to attack and alert the BS. Subsequently BS alert all sensor nodes in the network before the actual attack, so that we can avoid node become attacked. It leads to secure data transfer and collection with energy efficiency. Honeypot do not replace with the security of standard IDS, but with IDS it can more focus on information gathering and dishonesty of the attackers. We have multiple mechanisms which successfully provide security against threats, but combination of honeypot system with other security system gives better results.

REFERENCES

[1] Narote S. and Khanna S., Advance Honeypot System for Analysing Network Security, International Journal of Current Research and Academic Review, 2014:2(4):65-70.
[2] Vidhya N. and Sengottuvelan P., Avert Compromised Node in Wireless Sensor Network with Honeypot System, Indian Journal of Science and Technology, 2016:9(41):1-7.
[3] Butun I, Salvatore D, Morgera M, Sankar R, A Survery of Intrusion Detection Systems in Wireless Sensor Networks, IEEE, 2013:16(1):266-282.
[4] Spitzner L., To built a honeypot, http://www.spitzner.net/honeypot.html, 1999.
[5] Jain Y. K., Singh S., Honeypot based Secure Network System, International Journal on Computer Science and Engineering (IJCSE), 2011:3(2):612-620.
[6] Shridhar K., Jain M., Honeypots : Approach and Implementation, International Journal of Science and Research (IJSR), 2014:3(12):1038-1043.