Indian Journal of Science and Technology, *Vol 9(41), DOI: 10.17485/ijst/2016/v9i41/98419, November 2016*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Avert Compromised Node in Wireless Sensor Network with Honeypot System

N. Vidhya[1*] and P. Sengottuvelan[2]

[1]Bharathiar University,Coimbatore - 641046, Tamil Nadu; India; nvidhya81@gmail.com
[2]Periyar University, PG Extn Centre, Dharmapuri, Salem - 636011, Tamil Nadu,India;sengottuvelanp@yahoo.com

Abstract

Objectives: To avoid node become compromised and achieve secure data aggregationwith energy efficiency in the Wireless Sensor Network(WSN)by using Honeypot system. **Methods/ Statistical Analysis:** Honeypot system is a fake node plays vital role in the sensor network that attract the attackers, find attackers ID, analysis type of attacks and energy consumption by the attacks subsequently alert Base Station without disturbing the sensor network. Base Station can easily identify intruder or attacker using Honeypot and alert all sensor nodes. So each node able to identify the attackers before the actual attack. **Findings:**When node become compromised, itleads problem in data aggregation.Honeypot avoids compromised node and achieves good level of energy efficiency, life span, throughput ratio and success rate. Also it degrades the vulnerablility of attacks. **Application/Improvement:**Honeypot system makes deception and deterrence to the attackers. Its used for early warning, to detect attackers and type of attacks, it enhances the intrusion detection systems and helps in designing better tools for security.

Keywords: Attackers, Compromised Node, Data Aggregation, Energy Efficiency,Honeypot, Type of Attack

1. Introduction

The components of sensor node are microcontroller, transceiver, external memory andtiny battery power source. WSN is a collection of sensor nodes deployed in remote areas for various purposes like examination, agriculture, smart homes, automation, traffic management, environment monitoring, disaster finding and military purpose. Each sensor node is capable of sensing, processing, and communicating the required information.Data aggregation is defined as the method of aggregation of data from multiple sensors to remove unnecessary transmission and provide combined information to the Base Station (BS). The compromisednode injectsfalse data and reduces energy efficiency of that node whichleads unbearable situation to the BS. Our goal is to build a system that avoid compromised node 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 lot of data, whose data can be attacked or compromised and it is also expected to get probed and potentially exploited. It does not fix anything and provide us with additional information about hackers or attackers. This system used for early warning, enhances the intrusion detection systems 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 risethe network life time by reducing the resource utilization of sensor nodes. Designing a well-organized data aggregation protocol is a difficult task because the protocol must ensure efficiency in energy level, data accuracy, fault tolerance, latency and communication overhead. To achieve successful data aggregation it should avoid node become compromised otherwise compromised node should launch much false data leads to many complications for secure data aggregation.

**Author for correspondence*

Intrusion Detection systems are used to find attackers and attacks. Intrusion detection system monitorswicked activities in the network and produce reports to the administrator. Intrusion Detection systems are focused on identifying possible incidents, logging information about them and reporting attempts. Intrusion Detection System is classified into three categories[1]. a) Anomaly Based detection – define the network behaviour, its predefined behaviour is prepared or learned by the specifications of the network administrators. b) Signature Based detection – The signatures are determined by previously recognized attacks that are generated and referenced to detect future attack. c) Specification Based detection – A set of requirement and constraints that describes the correct operation of a program or protocol is defined.

Intrusion Detection System requirements are:

- Should not degrade the network
- Should be reliable and minimum false positives and false negatives.
- Should be transparent to the nodes and users.
- Should be energy efficiency.

Intrusion Detection System challenges in WSN - every node is independent from others and communications are controlled by BS managed by an administrator.

- Sensor nodes are resource constrained (battery, size, memory, etc).
- Lead to increase network lifetime
- Sensor nodes have chances to fail or disappear from the network.
- Requiring to monitoring, detecting, responding to the intruders.
- Difficult to time synchronizing nodes into the WSN.

Honeypot does not replace other traditional security of standard Intruder Detection System but with more focal point on information gathering and cheating of the attackers.

In[2], Brute force SSH attacks carried out on six different universities campus networks with Honeypot Techniques. Brute force password guessing attacks against SSH, FTP and Telnet servers are attacks to compromise servers in the internet. An important aspect to avoid interruption of these networks is to protect it against Brute force attacks. They mainly focused on effort to gain remote access to our SSH Honeypots plus tools and techniques employed. SSH is Secure Shell defined as "a protocol to get secure remote login and other network services in the insecure network".

In[3], ComSen uses a hybrid approach, consists of two components: a distributed system and centralized system. Distributed system running on each node in a WSN, a copy of this component runs on all sensor nodes also the sensor application routing protocols etc.Centralized system running on the base station, it is a higher order machine, so ComSen uses it to perform compromises are accurate or mistakes.

In[4], HoneyPharm is an algorithm to find all actions of hacker to attain secured Wireless Mesh Network. The whole network is divided into clusters,each cluster consists one Honeypot. Low interaction Honeypot finds the attacker and traps all the activity of attacker, then sends the attackers information to the high interaction Honeypot that are performing as a Remote Gateway which is a vital place for collecting all malwares. When the low interaction honeypot receives an attack, it can activate a trigger on high interaction Honeypot. The high interaction Honeypot investigates all the activities of attacker and stores it in a log files.

In[5], Roaming Honeypot technique renders the location of Honeypot to be unknown to the attacker in MANETs. Roaming Honeypot is unpredictable to the attacker, continuously changing and disguised. The whole network is divided in smaller grid like zones for convenience and one Honeypot is deployed in each zone. Mobile Honeypot should be aware of their own positions through a positioning system.

In[6], employedHoneypot for small scale industry for intrusion detection and noticing the activities of attacker. An attack on the virtual machine canbe capturedby Honeypot and monitor all activities and behaviour of the attacker.

In[7], Honeypot used in computer system to find attackers activity for illegal communication in the network like IDS, IPS, firewall etc. These systems are collection of Honeypots and IDS/IPS which have advanced performance especially for finding susceptibility.

In[8], proposedalgorithm is interaction between the game theory and Honeypot, applies the production of Honeypot along with the new game theory approach to analyze the past behaviours and performs iterative learning from the log. Game theory contains a game which have group of players, a set of policy for each player, and a set of functions for every game.

In[9], Genetic algorithm was applied with Honeypot using network tap, span port, hub or firewall to collect information about traffic that traverse in the network. The

collected traffic data is used by the GA for formationof set of rules for an Intrusion Prevention Rule based system.

In[10], the term HoneySpot isfrom mixing of two words Honeypot and Hotspot, Honeypot is system whose information can be easily compromised and Hotspot is a place that offers Wi-Fi access whose value also compromised. Purposeof Honeyspot is to collect information about the attacks in the wireless network, attacks that exploit the wireless technology weakness and subvert the security mechanism in place, which mainly focused on radio frequency and 802.11 based vulnerabilities.

In[11], proposed algorithmused to improve energy efficiencyof the wireless sensor nodes based on hybrid data collection and smart sleep mechanism in the sensor network. This hybrid technique increase the network lifetime and collect large amount of data then routed to sink. Proposed technique used for maximization of network life time mainly in war field or natural disasters

In[12], an efficient Position-based Key Sharing(PKS) scheme was used to get higher connectivity and ideal flexibility with lessutilization of resources in Wireless Sensor Networks and develop the network lifetime with three steps: Initially, Random based Key Pre-distribution, Multivariate Optimization-based Collective Key Detection and Key Path organization.

In[13], Base Station is based on an interval table prepared by the base station at the early stage of each period. The base station decides routes based on rule also send data to cluster heads. It was determined to collect data movement route toward itself.

2. Intrusion Detection System with Honeypot

Honeypot is Intrusion Detection system and its fake access point implemented by an administrator that responds with fake data to the intruder. Honeypot allows different kind of attacks and alert BS. Attackers easily attracted by this node. Who is visiting Honeypot is an intruder. Honeypot is an intrusion detection system that appears an ordinary server, but all data and transactions are phony and find intruder techniques and determine vulnerabilities. Honeypot is accepted to get investigated, attacked and potentially demoralized. Honeypot do not fix anything. Its provide information to the administrator about attacks. Two popular reason behind Honeypot. 1. Learn how intruder gain access to sensor nodes and maintain the record of intruder's activities. We can gain

Figure 1. Protect sensor network with honeypot system

insight into attack methodologies to improve our real production systems. 2. Gather informationof intruders to alert all sensor nodes. In[14], a honeypot in WSN waits for unprivileged interaction. Interaction is needed to trigger a honeypot.

Advantage of Honeypot:

- The only transfer of information in Honeypot isattacker's information.
- It makes easier to analyze the attacker's behaviour
- Deception – makesattackers to waste their time
- Deterrence – threatening the attackers
- Can estimate energy taken by the attackers in the node also alert the BaseStation.

3. Proposed Model

Honeypot is a decoy system, it attracts the attackers. Honeypot system desires to watchunauthorized activities in the network. All authorized nodesknow about fake node (Honeypot). When attackers interact with Honeypot system, it must do the following activity:

a) Identify attackers - To find the attackers, track GPS, MAC, Unique ID of attackers.Store Identification of attackers in the Database (Hidden information)

$$[H] \leftarrow [A]$$

$$A[ID_1] \leftarrow \text{getGPS}[A].$$

$$A[ID_2] \leftarrow \text{getMAC}[A].$$

$$A[ID_3] \leftarrow \text{getID}[A].$$

$$DB_1[ID_1, ID_2, ID_3] \leftarrow A[ID_1], A[ID_2], A[ID_3].$$

b) Analyse type of attack – Honeypot system is expected to get probed, attacked and compromised. Its watch and store attackers activity in Hidden database. Its analyse type of attacks broadly classified into,

a. Interruption – asset is destroyed or becomes unavailable or cannot be used.

[A (del[D])]→ DB;

TOA – Interruption

b. Interception – gain access to an asset, there is no privacy it is an attack on confidentiality of the system.

[A (copy[D])]→ DB;

TOA – Interception

c. Modification – access to a system and make some changes to it like modification it is attack on integrity of the system.

A [(Mod[D])]→ DB;

TOA – Modification

d. Fabrication – gain access to the system and inserts false objects into the system it is attack on authenticity of the system.

[A (add[D])]→ DB;

TOA – Fabrication

Routing table or RIB is a data 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, adversary node advertises routes to nonexistent nodes, to the authorized nodes present in the network. Routing table attacks cause 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, allow attackers to access the FR.

[A (access [D])] → RIB;

TOA – attack on routing table.

Attacks on routing table mean, attackers try to create various attacks discussedTable 1. If attackers access the routing table information, Honeypot alerts BS about possibilities of attack using routing table.

Also, attackers interact continuously with the system and not allow taking rest leads Denial of sleep attack.

A (CI [D]) → DB;TOA – DOSL.

c) Estimate energy consumed by attackers – Energy consumption can be calculated by energy before attackers entered and after attackers attacked.

Table 1. Possible attack types and their issues.

Type of attack	Belongings
Routing loop	Attackers inject malicious routing information
Denial of services	Alter legitimate routing setup.
Black hole attack	Advertise short distance to all destination
Warm hole attack	Make confusion in routing mechanism.
Selective forwarding	Refuse to forward certain message and drop them
Hello Flood	Announce false neighbour

$$EC = (E_1 - E_2)$$

$$DB_1 [EC] \leftarrow EC$$

d) Alert BS from Honeypot – after attackers attack the Honeypot system, it analyse type of attack and energy consumption and send details of attackers lD, TOA, EC to the BS. BS receives attacker information and store in BL and alerts all sensor nodes to avoid node become compromised.

H (A [ID]) →BS [BL] (attackers ID)

H (A [TOA]) →BS[BL] (Type of attack)

H (A [EC]) →BS [BL](energy consumption)

e) Finally BS alerted by Honeypot system then its send follow-up request to the attackers to watch further attacks of attacker.

H[f] → [A]

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

Procedure 1: Honeypot System

1. Honeypot is decoy system, it attracts the attackers.
2. Who enter into the Honeypot system is attackers.
3. To find attackers, track
   - GPS,
   - 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.

Table 2. List of Abbreviations

Terms	Expansion
H	Honeypot
A	Attackers
ID1	GPS(Global positions system) of attackers
ID2	MAC(Medium Access control) of attackers
ID3	Unique ID
DB	Database
D	Data
DOS	Denial of Service
DOSL	Denial of Sleep
TOA	Type of attack
E_1	Energy level before attackers entered
E_2	Energy level after attackers attacked
EC	Energy Consumption
BL	Block List
F	Follow up request
RIB	Routing Information Base
CI	Continuous Interaction

Theft by attackers.
Denial of Service.
Denial of Sleep

6. Log all transactions done by attackers.
7. Honeypot system analyse Type of attack by using all logged transactions.
8. Estimate energy consumed by attackers
9. Finally send detail to BS include, Attackers ID, Type of attack, Energy Consumption.
10. Base station receive attackers detail from Honeypot, add attackers in Blocked list.
11. Base station alert all sensor nodes about blocked list in database. And avoid node become compromised.
12. Honeypot system sent follow-up request to the attackers

4. Simulation Analysis

The result analysis of Honeypot is compared with various types of intrusion detection systems. In[15], ITIDS (Isolation Table based IDS) to detect intrusion by hierarchical wireless sensor network and calculate approximately the effect of intrusion. Its effectively prevents attacks in live nodes, but when the number of nodes increased then the intruders can penetrate into the network. In[16], DIDS (Dynamic IDS) the detection rate of DIDS is higher when smaller number of nodes isused; when the number of nodes gets increased the DIDS effectiveness goes down. In[17], IMIDS (Insomnia Mitigating IDS) for heterogeneous wireless sensor network to find insomnia of stationary sensor nodes. It uses cluster based mechanism in an energy efficient manner to build a five layer hierarchical model for IDS, shows more effective with energy efficiency and throughput, but our system is more efficient in aspects when compared to IMIDS.

Objective of the proposed model is identifying attackers, understand the attacker's goal and alert BS to prevent node become compromised. Honeypot system finds attackers using Signature based attack detection also Anomaly based attack detection. Anomaly based detection is possible when DOSL is done by attackers. Honeypot can detect numerous traffic surge due to sending many packets in an aggressive manner without waiting usual time interval. Many IDS proposed in WSN to find known and unknown attack. Our proposed model will not replace all IDS and its additional security mechanism to avoid node compromised and watch attacker's activity, make attackers waste his time and try to trouble the attackers.

Figure 2 shows that the throughput ratio of the system that is implemented using honeypot which is more efficient than the other Intrusion Detection System. Proposed model can analyse attackers behaviour by allowing them without difficulty enter into the node and access node freely. Honeypot system cleanly observes attacker's activity without any interruption.This create attackers accomplish their effort without any uncertainty. This is advantage of proposed model compare with other intrusion detection system.

Figure 3 shows that the life Span is more for Honeypot system compared to other IDS. Other IDS play role in the

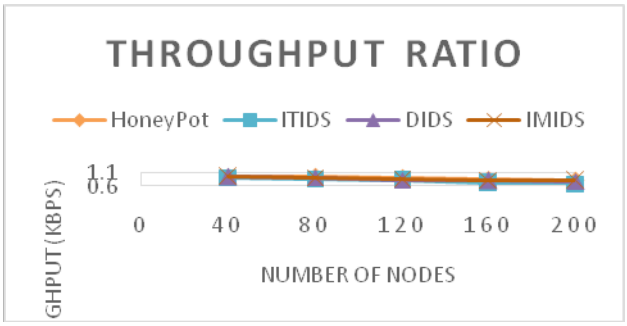

Figure 2. Throughput ratio.

sensor nodes that available in the network. Honeypot is different from other IDS, as it is interact with attackers without disturbing the sensor nodes that are available in the network.

Figure 4 shows that the defect rate decreases as the number of nodes increases in the simulation for Honeypot system when compared to IDS.Existing IDS are suffer from lack of resources like high processing power, huge storage capabilities, unlimited battery backup etc. Two major advantage of Honeypot system are: not influences existing network model and resources of sensor nodes. Honeypot is additional security system in WSN to achieve prevention of compromised node. Using Honeypot system, BS can alert sensor nodes and avoid node become compromised. For secure data aggregation, compromised node is big challenge. The important tasks of Honeypot system are: a) avoiding compromised node, it leads BS acquire Secure data aggregation with good energy efficiency. b) Honeypot system sends follow up request to the attackers for further attack and alert the BS. It used to trace the goal of attackers or motivate the attackers for further attack. This is major difference of Honeypot system from other IDS.

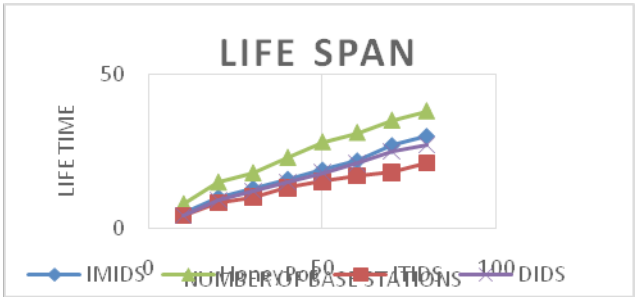

Figure 3. Life span.

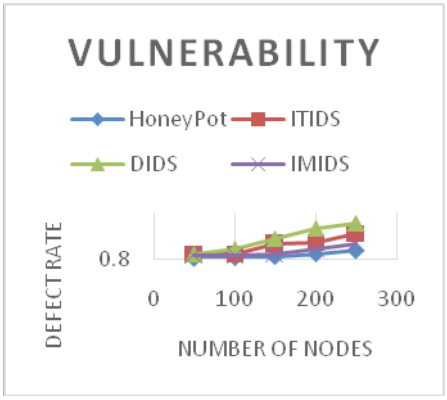

Figure 4. Vulnerability.

Success rate analysis of the captured attackers by the Honeypot and other Intrusion Detection Systemis shows in Figure 5. It clearly shows Honeypot is ahead of all other IDS.

Figure 6 shows that the energy efficiency by the sensor nodes. Honeypot uses only 20 percentage of the energy in one hour, whereas other IDS uses about 40-45 percentage of the energy.

Honeypot is a light weight system not imposing burden to the sensor node in the network that learn about attack patterns, locate attackers and observe attacker's activity and alert BS. Traffic in Honeypot is the reason for attackers in Honeypot. Opportunity of compromised node is more in WSN without a Honeypot Intrusion Detection system. Attackers directly try to attack any node that try to compromise them and disrupt sensor network. Theproposed model redirects the attacker to Honeypot system also motivate them to attack and alert the BS; it reduces the percentage of compromised node in the network.

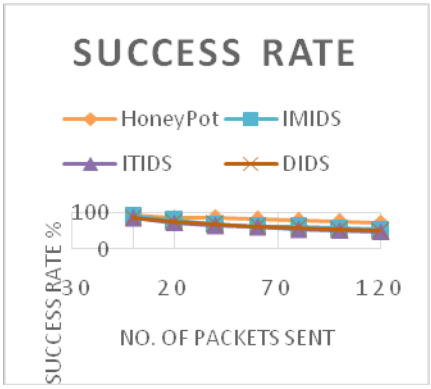

Figure 5. Success rate.

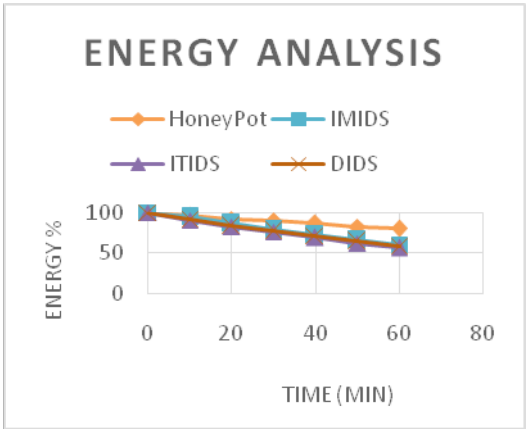

Figure 6. Energy analysis.

5. Conclusion

A compromised node in sensor network is a challenging one to achieve secure data aggregation and compromised node reduces energy efficiency of sensor nodes.The proposed model creates a fake server node called Honeypot, which attracts the attackers and agree to carry out all types of attackswith autonomy. This model redirects the attacker to Honeypot system also motivate them to attack and alert the BS. Subsequently BS alert all sensornodes in the network before the actual attack so that we can avoid node become compromised; it leads to secure data aggregation with energy efficiency. Honeypot do not replace other traditional security of standard intruder detection system but with more focus on information gathering and deception of the attackers.

6. References

1. ButunI, Salvatore D, Morgera M,Sankar R.A survey of intrusion detection systems in wireless sensor networks. IEEE. 2013;16(1):266–82.
2. Kheirkhah E, Amin SMP, Sistani HAJ, Acharya H. An experimental study of SSH attacks by using honeypot decoys. Indian Journal of Science and Technology. 2013 Dec; 6(12):1–12.
3. Wang YT, Bagrodia R.Comsen: A detection system for identifying compromised node in wireless sensor networks. The Sixth International Conference on Emerging Security Information, System and Technologies; 2012.
4. Rawatp, Goel S, Agarwal M, Singh R. Securing WMN using hybrid honeypot system. International Journal of Distributed Parallel Systems. 2012; 3(3):1–6.
5. ShamshS, VandanaD.Roaming honeypots along with IDS in mobile ad-hoc networks. International Journal of Computer Application.2013; 69(23):1–8.
6. Singh G, Sharma S, Singh P. Design and develop a honeypot for small scale organization. International Journal of Innovative Technology and Exploring Engineering. 2013; 2(3):1–5.
7. Baykara M, Das R.A survey on potential applications of honeypot technology in intrusion detection systems.International Journal of Computer Networks and Applications. 2015; 2(5):1–9.
8. SaranyaJ,Lekha J.A review on trap- tracking and preventing intruders in WSN using honeypot driven game theory. International Journal of Infinite Innovations in Engineering and Technology. 2015; 2(4):1–8.
9. DivyaD,Chugh A. GHIDS: A hybrid honeypot system using genetic algorithm. International Journal of Computer Technology and Applications. 2012; 3(1):187–91.
10. Siles R. Honeypot: The wireless honeypot- monitoring the attackers activities in wireless networks. The Spanish Honeynet Project;2007Dec.
11. Shankar T, Karthikeyan A, Sivasankar P, Neha RR. Implementation of smart sleep mechanism and hybrid data collection technique for maximizing network lifetime in WSN's. Indian Journal of Science and Technology. 2015 May; 8(S9):1–8.
12. Jayamurugan G, Kamalakkannan P. Position-based key sharing with higher connectivity and multivariate optimized resource consumption in WSN.Indian Journal of Science and Technology. 2015 Dec; 8(35):1–9.
13. Fanian F, Rafsanjani MK. A novel routing efficient algorithm based onclustering in WSNs. Indian Journal of Science and Technology. 2013 Dec; 6(12):1–4.
14. Markert J,MAssoth M. Honeypot effectiveness in different categories of attacks on wireless sensor networks. 25thInternational Workshop on Database and Expert Systems Applications, IEEE UK; 2014.
15. Chen R-C, Hsieh C-F, Huang Y-F. An isolation intrusion detection system for hierarchical wireless sensor networks. Journal of Networks. 2010Mar,5(3):1–8.
16. Huo G, Wang X. DIDS: A dynamic model of intrusion detection system in wireless sensor networks. Information and Automation Conference; 2008.
17. Bhattasali T, Chaki T. A survey of recent intrusion detection systems for wireless sensor networks. Advances in Network Security and Applications, 4th international Conference CNSA 2011, Chennai, India; 2011 Jul.