Performance of Various Attack Detection Algorithms in Internet of Things (IoT)

Vaishnavi.S[1], Dr.Sethukkarasi.T[2]
[1]*Assistant Professor, Department of Computer Science and Engineering, R.M.K. College of Engineering and Technology, Tamilnadu-601206, India*
[2]*Professor, Department of Computer Science and Engineering, R.M.K. College of Engineering and Technology, Tamilnadu-601206, India*

***Abstract*- IoT is a highly dynamic and radically distributed networked system, composed of a very large number of smart objects producing and consuming information. As the objects involved in IoT are heterogenic nature and these objects communicate through Internet they give rise to many challenging research areas. One such major research challenge in IoT is Security. Securing IoT from different types of attacks is a major challenge. Now IoT is widely applied to social life applications such as smart grid, intelligent transportation, Healthcare, smart security and smart home. IoT can make the usage of all these applications easier with its technology but if it does not ensure security it may lead to major problems like leakage of personal privacy information, etc. In this paper we present a survey of different types of attacks on IoT and discuss the algorithms used to detect these attacks. Specifically we present the most common attacks like DDos attack, Sybil attacks, SIP Flooding attack, man-in the Middle attack and Clone attacks. Finally, we discuss the challenging research issues and future directions for Securing IoT.**

***Index Terms*- WSN, Internet-of-Things, Security and attacks.**

I. INTRODUCTION

Within the past decade, the number of Internet of Things (IoT) devices introduced in the market has increased drastically. With totals approaching 15 billion, the staggering conclusion that there are roughly two connected devices per living human is reached [1]. This trend is expected to continue, with an estimate of 26 billion connected devices by the year 2020, the majority of which being IoT devices. IoT devices are armed with an array of sensors whilst also offering the means to establish a network connection, enabling the transmission of the collected information to a remote node.

The Internet of Things (IoT) stands the network of physical devices, vehicles, buildings and other items-embedded with sensors, actuators, electronics, software and network connectivity that allow these objects to gather and interchange data. The word internet means a distributed network and Things in the IoT sense, can refer to a wide variety of devices such as heart monitoring implants, biochip transponder on farm animals, electric clams in coastal waters, automobiles with built-in sensors. The IoT offers a wide variety of smart devices-all of which face the difficulty of securing complete privacy. As the devices are all so diverse their heterogenic nature is often used as an excuse by manufactures and owners alike to skip sufficient security controls. [5]While the IoT will make life easier, there are significant security challenges in its use. Sluggish development and limited commercialization have led some industry spectators to jump to call it as "Internet of NoThings". Then final the technological growths made it to overcome this name. Presently it's facing lot of security it's now called as "Internet of Insecure Things". Your data might be handled to an attack without security measures in place. Information is observed is called as passive attack. Information is damaged or replaced in the network is called as passive attack. Attackers can do three different tasks such as task control, steal information and disrupt services show in Fig-1.

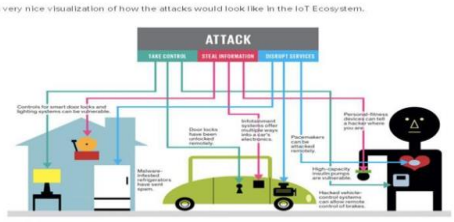


Fig-1 visualization of attacks in IoT

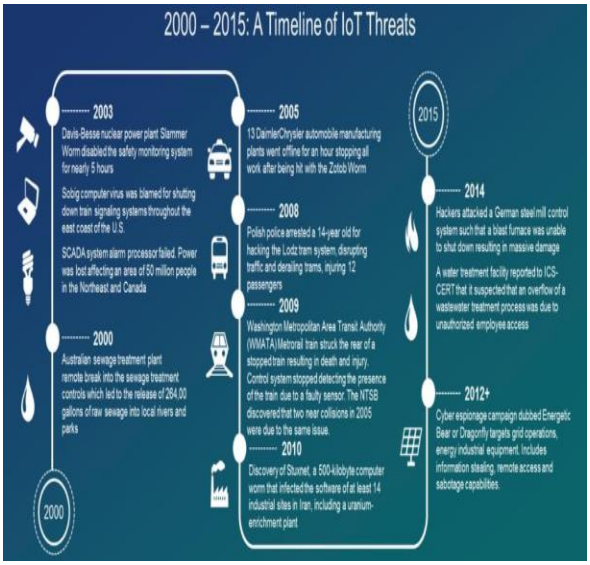
Take control is taking control of the smart devices in IoT. For example the attacker can take control over a smart lock at our home. Steal Information is nothing but stealing the information related to the smart devices in the IoT. For example information related to the car which location and how much is travelling; engine used for it can be steeled. Disrupt services means stopping the functionality of a smart device. For example a heart patient has a Smart Pacemaker (a device that support the heart in pumping of blood) installed in his body which the attackers can disrupt there by leading to the death of the patient. When we look all the roles performed by an attacker on IoT. We understand how much security is needed for IoT.

II. REVIEW OF ATTACKS AND ITS DETECTION ALGORITHM

In this section, we review various attacks in IoT, how they are secured using existing technologies is analyzed in this paper.

A. Distributed Denial of Service Attack(DDoS)

Denial of Service (DoS) attack tries to disrupt the services of the network or servers. Attack will be done from a single attacker machine (Ex: SYN-FLOOD). Distributed Denial of service attacks are like DoS Attack but these attacks will be originated from the different attacker's machines to target the victim. In fig-2, Masters and agents/zombies are compromised computers running attacker's code. All DoS attacks can be done like DDoS.



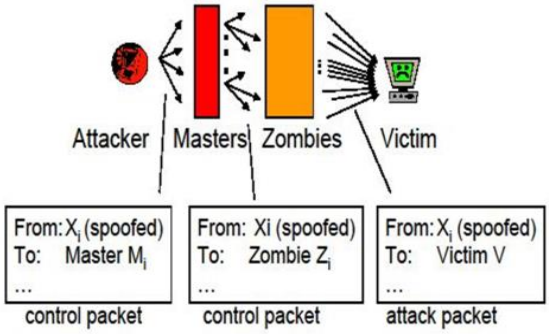


Fig-2 DDoS Attack

The detection of Dos attacks using (MCA) Multivariant Correlation Analysis [1], Multivariant means multiple parameters and correlation means relationship among these parameters. The algorithm used detect is Normal profile generation algorithm which is based on Triangle Area Map (TAM) and Mahalanobis distance (MD). TAM stores all the extracted correlations in KDD cup99.MD is adopted to measure the dissimilarity between traffic records. The detection system contains three major steps such as basic features are generated from networks traffic, MCA is done with TAM and detection by training and testing phases.

B. SIP Flooding Attack

Session Initiation Protocol (SIP) is used for monitoring multimedia communication sessions above the Internet Protocol (IP).SIP flooding attack is mid the most severe attacks because it's informal to promotion and accomplished of quickly draining the resources of both network and nodes. In fig-3, SIP can be configured to operate in authenticated mode. SIP is vulnerable to flooding attacks. A typical attack would be an INVITE flood. SIP with authentication is more vulnerable to flooding attacks.

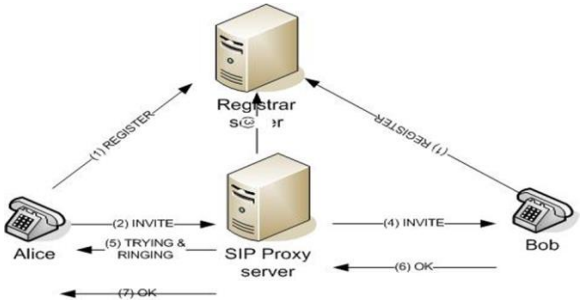


Fig-3 SIP Protocol

The detection SIP Attacks done by Sketch design technique based Hellinger Distance (HD).Sketch is capable of summarizing each of the incoming SIP

messages. [2]Sketch data distribution is used to establish a probability distribution for each SIP attribute independently.3-dimensional sketch contains of SIP attribute in hash table. When the HD obtained from certain element hash-row exceeds the threshold, attack detection is registered. This threshold will be polluted by the attacker so Estimated Freeze algorithm is used to freeze the threshold.

C. Blackhole Attack

Blackhole attack is a malicious node can attract total packets by misleadingly requesting a fresh route to the destination. Then engage them without promoting them to the destination. Supportive Black hole means the malicious nodes deed in a network. It occurs when intruder arrests and block the packet that they don't to destination node which re-program some nodes in the network.Fig-4, Packets are capture by node4 which is Blackhole attack doesn't send important information to destination and creates fake reply. It may also consume the complete traffic.

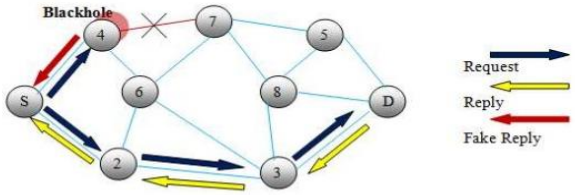


Fig-4 Blackhole Attack

D. Misdirection Attack

A attacker misdirect the packets route away from its neighbors to many other distant nodes in order reach the destination node in the network is known as misdirection attack. Thus packet reaches destination node leads to declines the throughput of the network and produces time-consuming in packet delivery. In Fig-5, a misdirection attack is node5 which misleads the packets to other distant nodes.

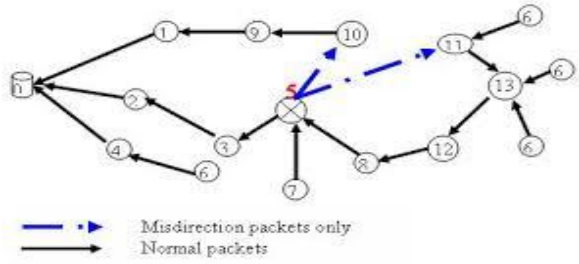


Fig-5 Misdirection Attack

E. *Wormhole Attack*

Wormhole can attract and avoid a huge amount of network traffic and achieve manipulation. An attacker creates tunnel between two distant nodes in the network by an in/out-of-band channel which is designed by a pair of attackers. This tunnel provides two distant locations a misinterpretation that they are near to each other. Source node S_9 sends the packets to a destination node S_2 in fig-6. At that time S_9 is attracts towards the path with less hop distance so wormhole tunnel is created between two nodes and sends the packets in the tunnel.

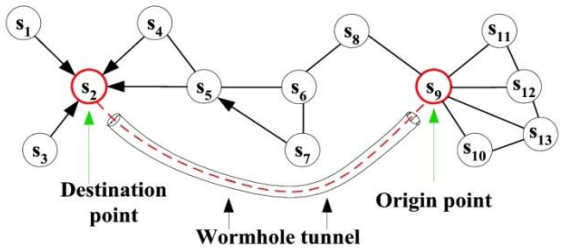


Fig-6 Wormhole attack

F. Sinkhole Attack

In order to use the more frequently route, attacker misdirects the route between base station and its neighbors. Sinkhole attack is a malicious node which reason severe threat to Wireless sensor network. Attacker captivates other nodes which are near to sinkhole than to the base station which a route with the less hope distance is presented to mislead its neighbors that forward all the traffic. Malicious node in fig-7 misguides packets which is depicts type of sinkhole attack.

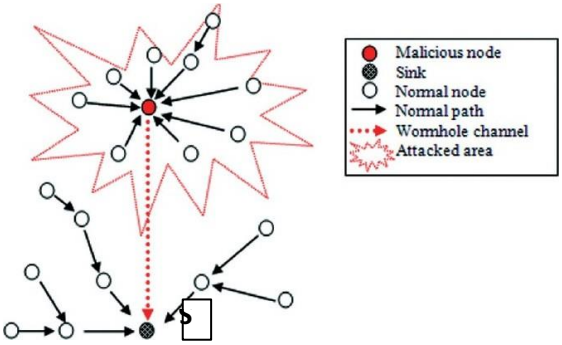


Fig-7 Sinkhole Attack

Blackhole, Misdirection, Wormhole and sinkhole attacks are detected using Hybrid Anomaly detection K-means clustering algorithm. [7] The proposed scheme contains two phases such as offline and online phases. Offline phases contains of trained data

after pre-processing which remove the outliers data points from traffic data using outliers detection and removal algorithm. Online phase will test dataset from network traffic after pre-processing. The testing dataset is fed into K-means clustering system which is used for clustering traffic parameters. Its output feds into Hybrid Anomaly Detection and post mining algorithm based on cluster nodes (CH). Each CH in a cluster detects whether a member in that cluster is a Blackhole node or Misdirection node or Collaboration of Misdirection node.

G. Clone Attack

In the attack an attackers detention a node and abstract its cryptographic secrets and create duplicates of this node in the complete networks due to this an attacker can simply misguide the packets. These clone node attacks very hazardous to the process of sensor networks. By capturing single node, the challenger can generate as many replicas nodes organized by the adversary. [11] These nodes look like certified participants in the network so it is very hard to detect a clone attack. In fig-8 node 'a' has be capture by attacker and created replicas node of it "a^I ". Then result of two paths passed to different locations.

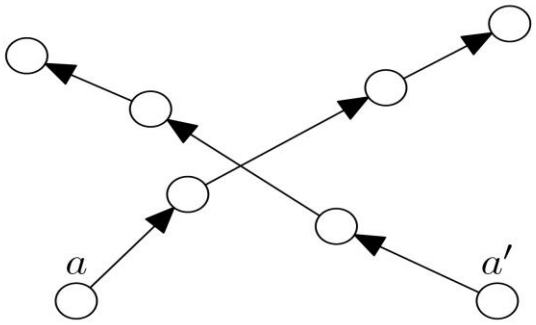


Fig-8 Clone Attack

RED (Randomized, Efficient, and Distributed) algorithm is used to detect the clone attack [12].Generates a unique ID to each node in a group of sensor nodes which makes that as original node. Cluster head is designated in each cluster. ID broadcasted to all neighbor nodes with a private key which is verified at the destination end. It is checked by cluster head in base station to detect clone attack.

H. Sybil Attack

In the Sybil attack, a malicious node performs as if it were a more number of nodes, for example by imitating other nodes or simply by demanding false identities. We express the Sybil attack as a malicious device criminally taking on multiple identities. We mention to a malicious device's further identities as Sybil nodes. Example: fake voters during elections. In fig-9, Sybil node is disrupt geographic and multi-path routing protocols to sensor node(ID_A, ID_B, ID_C).This transmission can be overhead and handled by the Sybil node.

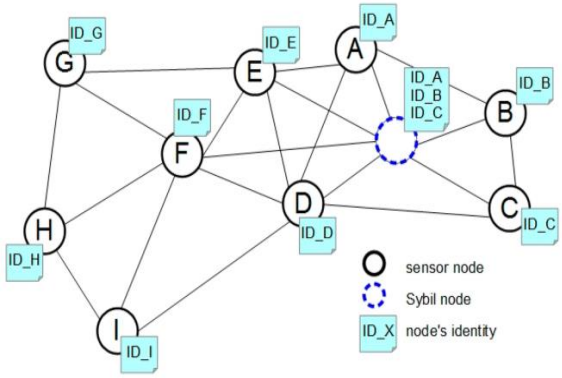


Fig-9 Sybil Attack

CAM-PVM algorithm (compare and match-position verification method) with MAP (message authentication and passing) is used for detecting Sybil attack [13]. When data are transmission in the network and each every node information is stored in table. The algorithm gathers the ID, timestamp, and current location information of the nodes after verification which is compared with original information when they are recorded. This outcome is sent to only trust nodes in the network for secured data transmission. If trusted node is unknown then data transmission is stopped and alternate path is chosen, which consuming more time and more costly. So detection of Sybil attack is done by MAP algorithm communicates by passing the authentication message.

I. Selective Forward Attack

In this attack an attacker encompass itself in a data stream lane and can selectively drop only distinct packets. In sensor networks it is supposed that nodes faithfully forward received messages but some neighbour node might decline to forward packets, over neighbours may start by another route. Fig10,in the network packets are passed in selective but one node which drops the packets and delay to forward it to neighbour node.

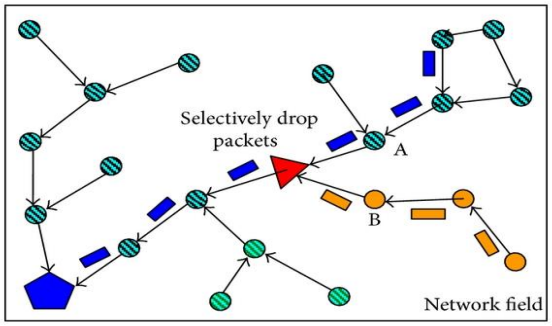


Fig-10 Selection Forward Attack

Selective Forwarding Detection (SFD) Algorithms [14] is used to detect Selection Forward Attack which consists of multi-layer detection framework of three layers by a different algorithm. In the first layer, MAC Pool of IDs Layer algorithm used to authenticates the entering traffic to define whether a node is legitimate or malicious. In the second layer, rule-based processing algorithm is used to checks the traffic by comparing with a list of rules. In the third layer, anomaly detection algorithm is used to classify unknown attacks, which look as false negatives, reject the traffic and send an alert.

J. Hello Flood Attack

In the network, each new node sends "Hello messages" to discovery its neighbor nodes. Also, it broadcast its route to the base station. Other nodes may choose to route data through this new node if the path is smaller. A laptop-class adversary that can retransmit a routing bring up-to-date with sufficient power to be received by the whole network leaves many nodes stranded. Target nodes try to reply, but the adversary node is out of radio range as sown in Fig-11. But, they have selected this node as their root. This attack puts the network in a state of misperception.

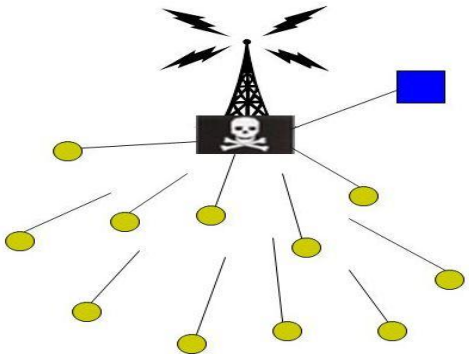


Fig-11 Hello Flood Attack

Adapting detection algorithm [15] is used to detect hello flood attack. This algorithm contains two phases such as Scalable Broadcast Algorithm (SBA) to reduce redundant forwarded packets and detection of hello flood attack which is founded on Received Signal Strength Indication (RSSI).The alpha-Beta filtering was offered for adapting algorithm with dynamic changes in network.

III. ISSUES

This is section discussed about various issues of detection algorithms in Table-1. Presently there is no complete framework to handle various attacks in IoT. All existing algorithm handles one or two type of attacks. The detection rate decreases as the traffic increases or number of attacks increases.

Table-1 Issues in Detection Algorithm

TYPES OF ATTACKS	DETECTION ALGORITHM	ISSUES
DoS Attack	Normal Profile Generation Algorithm based on Triangle Area Map and Mahalanobis Distance	i)Does not address the problems of other attacks ii)False-Position rate is high
SIP Flooding Attack	Sketch design based on Hellinger Distance using Estimation Freeze Algorithm	Attack detection rate is low against large scale DDoS Attack
Blackhole Attack	Hybrid Anomaly Detection K-Means Clustering Algorithm	High detection rate (98.6%) and low false positive rate (1.2%)
Misdirection Attack		
Wormhole Attack		
Sinkhole Attack		
Clone Attack	RED Algorithm	No pre-assumption in defining the clone node
Sybil Attack	CAM-PVM Algorithm	i) More time consumption and cost effectiveness. ii) The size of the network is not a constraint.
Selective Forward Attack	SFD Algorithms	i) Reliable, energy, efficient and scalable technique to prevent forwarding attacks. ii)98.3%accuracy detection rate
Hello Flood Attack	Adapting Detection Algorithm	Low false positive rate

IV. CONCLUSION

Internet of Things (IoT) is vulnerable due to many types of attacks and IoT cannot use in our day to day

life without security. This research work focuses on an idea to develop the framework to detect the different types of attacks in IoT networks. For developing the framework Hybrid Data Mining Technique can be used which is combination of two or more Data Mining Techniques or Algorithms. Through which the attacks can be detected. It can reduce the detection rate and false positive rate in future.

REFERENCES

[1] Zhiyuan Tan, Aruna Jamdagni, Xiangjian He, Priyadarsi Nanda, "A System for Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis", IEEE Transactions On Parallel And Distributed Systems, Vol. 25, No. 2, February 2014.

[2] Jin Tang, Yong Hao and Wei Song, "SIP Flooding Attack Detection with a Multi-Dimensional Sketch Design", IEEE Transactions on Dependable and Secure Computing, 2013.

[3] Wu, Zhigang Zhao, Feng Bao, and Robert H. Deng, "Software Puzzle: A Countermeasure to Resource-Inated Denial-of-Service Attacks", IEEE Transactions On Information Forensics And Security, Vol. 10, No. 1, January 2015.

[4] Nadav Schweitzer, Ariel Stulman, Asaf Shabtai, and Roy David Margalit, "Mitigating Denial of Service Attacks in OLSR Protocol Using Fictitious Nodes", IEEE Transactions On Mobile Computing, Vol. 15, No. 1, January 2016.

[5] Qi Jing,Athanasios V. Vasilakos,Jiafu Wan, Jingwei Lu,Dechao Qiu, "Security of the Internet of Things: perspectives and challenges", Springer 2014.

[6] Daniele Miorandi,Sabrina Sicari, Francesco De Pellegrini, Imrich Chlamtac, "Internet of things: Vision, applications and research challenges", Adhoc Networks, Elsevier 2012

[7] Mohammad Wazid, Ashok Kumar Das, "An Efficient Hybrid Anomaly Detection Using K-Means Clustering for Wireless Sensor Networks", Springer 2016

[8] Mikhail Zolotukhin, Timo H¨am¨al¨ainen, Tero Kokkonen,Antti Niemeland Jarmo Siltanen, "Data Mining Approach for Detection of DDoS Attacks Utilizing SSL/TLS Protocol", Springer 2015

[9] B. M. Aslahi-Shahri,R. Rahmani,M. Chizari,A. Maralani,M. Eslami, M. J. Golkar,A. Ebrahimi, "A hybrid method consisting of GA and SVM for intrusion detection system", Springer 2015

[10] Alampallam Ramaswamy Vasudevan, Subramanian Selvakumar, "Local outlier factor and stronger one class classifier based hierarchical model for detection of attacks in network intrusion detection dataset", Springer 2016.

[11] Jun-WonHo, Donggang Lin ,Matthew Wright, Sajai K.Das, "Distributed detection of replicas with deployment knowledge in wireless sensor networks", Preprint submitted to Elsevier,March,2009.

[12] Mauro Conti, Roberto Di Pietro, Luigi Vincenzo Mancini and Alessandro Mei, Distributed Detection of Clone Attacks in Wireless Sensor Networks, IEEE transactions on dependable and secure computing, vol. 8, no. 5, september/october 2011.

[13] Udaya Suriya Raj Kumar Dhamodharan and Rajamani Vayanaperumal, Detecting and Preventing Sybil Attacks in Wireless Sensor Networks Using Message Authentication and Passing Method, Scientific World Journal Volume 2015, Article ID 841267.

[14] Naser Alajmi and Khaled Elleithy, Multi-Layer Approach for the Detection of Selective Forwarding Attacks, sensors 2015, ISSN 1424-8220.

[15] H. Khosravi, R. Azmi, and M. Sharghi, Adaptive Detection of Hello Flood Attack in Wireless Sensor Networks, International Journal of Future Computer and Communication, Vol. 5, No. 2, April 2016.