Assorted Attack Detection for IoT

Mareeswari Govindaraj*
2nd year M.E. Student, Department of Computer Science and Engineering, Sri Vidya College of Engineering and Technology, Virudhunagar, India
*Corresponding author: mareeswarig29997@gmail.com

***Abstract*: While IoT has huge social impact, it comes with a number of key security Challenges. Smart devices are vulnerable to variety of attacks. In this project, we propose the solution to detect all types of attacks in an IoT environment. For this, we initially create the wireless network and then implement mobility and energy in every node of the network. Later we intentionally create some malicious in the network for detecting the attacks. Then, we Perform data transmission between the nodes as a regular manner. For data transmission we used AODV protocol. Finally, we identified the malicious behavior and perform analysis on that collected data and then detected the attacks. It also detected the types of attack occurred.**

***Keywords*: Attack, Internet of Things, Intrusion detection system, Malicious behavior.**

1. Introduction

Anything that has sensor attached to it and it can transmit data from one object to another or to people with the help of internet is known as Internet of things. Internet of things extend internet connectivity beyond some of the standard devices like computer, laptops, tablets and smartphones, to any range of non-internet enabled physical devices and everyday objects like fridge, washing machine, television. IoT devices include all the wireless sensors, software, actuators, and computer devices. They are attached to a specific object that operates by the internet and then enable the transfer of data among objects automatically without any human intervention.

Internet of things evolved from multiple technologies like machine learning, real time analytics, embedded systems and commodity sensors. Traditional technology fields of wireless sensor networks, embedded systems, automation, controlling systems and others are contributing to enable the Internet of Things.

Smart devices are not only within the domestic environment, but it is also used in smart homes, smart cities, intelligent transport, wearable devices, agriculture, manufacturing, Environmental monitoring, smart grids, and health care systems.

While IoT has huge social impact, it comes with a number of key security Challenges. Smart devices are one of the major weakest link for breaking into a secure infrastructure. Smart device vulnerable to variety of attacks such as data leakage, spoofing, disruption of service (DoS/DDoS), energy bleeding, insecure gateways, etc. These can lead to dangerous effects, causing damage to hardware, disturb the system availability, cause for system blackouts, and even physically harm individuals.

Researchers developed many Intrusion Detection Systems that have capability to detect several attacks in several available environments. An intrusion detection system (IDS) is a system that monitors network traffic for malicious activity and give alert when such activity is discovered.

An intrusion detection system may be implemented as software application that is running on customer hardware, or any network security appliance. It monitor the operation of firewall, router, files and servers that are needed by other security controls. It provide a user-friendly interface that’s why non-expert staff members can assist with managing system security. It include a major attack signature database against which have information from the system can be matched. It recognizing and reporting when the IDS detects that data files have been altered.

Traditional anomaly detection systems are also ineffective within IoT ecosystems, since the range of possible normal behaviors of devices is significantly larger and more dynamic than traditional IT environments. Popular Intrusion Detection Systems like SNORT and Bro which are only work on traditional IP-only networks as they are static and use signature-based techniques. Finally, the Intrusion Detection Systems is developed for WSN would also be ineffective to Internet of things ecosystem because of their inability to adapt their applicability only for single platform and the protocol, and their small and particular range of detection techniques. As these technologies have a direct impact on our lives, privacy considerations and security. It must become a higher priority. There is a need for an IDS to monitor malicious behavior or policy violations within a heterogeneous IoT devices network and subsequently understand their impact.

2. Literature Survey

Eirini Anthi et al. [1] proposed three-layer Intrusion Detection System (IDS) to detect a range of popular network based cyber- attacks on IoT networks. But It only detect known and simple attacks. If any unknown attacks found, it can’t be detected. Pete Burnap et al. [2] developed an IDS to monitor IoT ecosystems, which adapt to heterogeneous environment and detect malicious activity on the network. Shahid Raza et al.

[3] proposed an intrusion detection system for the Internet of Things to detect Wormhole attack and who is the attacker. Stephen et al. [4] proposed a technique to identify whether the router node is a malicious node or not using the IR (Intrusion Ratio) value. Chen Jun et al. [5] proposed an Event-processing IDS architecture in IoT environments on the basis of security requirement analysis for IDS. Philokypros Ioulianou et al. [6] proposed a design to adopt a signature-based intrusion detection approach and involves both centralized and distributed IDS modules. Arunan Sivanathan et al. [7] developed a classification method to distinguish IoT from non-IoT traffic and it also identify specific devices. Michael et al. [8] presented a service oriented infrastructure which provide elastic provisioning for any application components on resource constrained devices and heterogeneous devices. Olivier et al. [9] analyzed what are all the network attacks that can be launched in IoT gateways and then identify which are relevant metrics to detect that type of attacks. Liang Xiao et al. [10] investigated the attack model for IoT systems and review the IoT security solutions for these type of attacks such as authentication, access control. YairMeidan et al. [11] monitor the behavior of the network traffic and by using deep auto encoders technique it detects all anomalous network traffic from the compromised Internet of Things devices. Mahmudul Hasan et al. [12] analyzed the performances of multiple machine learning models and then concluded which machine learning technique detects the attacks and anomalies on the IoT Systems accurately and prove Random Forest(RF) performs comparatively better. Martin Roesch et al. [13] provided a layer of defense which monitors network traffic for predefined suspicious activity and detect the attack or any malicious activity. If any attack or any malicious operation found it alert system administrators. Prabhakaran et al. [14] presented a denial-of-service (DoS) detection architecture for 6LoWPAN which is protocol for low-power lossy networks. Tariqahmad et al. [15] proposed a Lightweight Intrusion Detection System to detect Sybil attack and Hello flood attack in IoT network. Rohan Doshi et al. [16] proposed packet-level machine learning DoS detection can accurately distinguish normal traffic and DoS attack traffic from consumer IoT devices. Christopher et al. [17] presented a solution to the detection of botnet activity within consumer IoT devices and networks. Prachi Shukla. [18] presented 3 new Intrusion Detection Systems (IDSs) for IoT: 1) Kmeans clustering based unsupervised IDS; 2) decision tree based supervised IDS; and 3) a hybrid 2 stage IDS which combines both. Douglas et al. [19] developed an ultra-lightweight deep packet anomaly detection approach. It uses the feature of bit-pattern matching. Nanda Kumar et al. [20] proposed a technique that isolate anomalous node and its packets are discarded at the data link layer. So it avoids the unnecessary packet processing overhead.

3. Methodology

A. *Network creation*

For detecting the attack, first create the network which contain 17 nodes. That 17 nodes are connected by using the wireless network. That wireless node can have the properties like mobility that is the node can move from one location to another location at any time.

That wireless node can have another property that is energy. Because each node in this wireless network indicate the smart device, system, sensor or any home appliance. Each of these device contain limited amount of power supply that is energy. So the node should include this energy property as well.

This intrusion detection process is performed for IoT devices. So we want to include these two important properties. In a normal network contain only the system, so we need not consider that but in IoT environment we must consider this energy and mobility properties.

Each node can have the ability to transfer the data packets and the routing information. This node can be viewed by using the NAM (Network Animator) software and the movement also can view in this NAM software.

B. *Create malicious behavior*

To detect the malicious property first, we want to insert that malicious behavior. Then only we analyze that traffic and can detect the attack.

After creating the malicious behavior, the data traffic gets changed. Based on this data traffic behavior we detect the attacks.

For creating the malicious behavior, it creates a tunnel between the two nodes, dropping the packet, flooding the request packet, create multiple identities like this. These are the malicious behavior caused for the attack.

C. *Data transmission*

In this module perform data transferring between the nodes that are connected by wireless channel. This transmission includes data packets, routing information, request packet for data transmission, acknowledgement packet.

In this attacking case, this data transmission contains the malicious behavior. So this system wants to analyze this malicious behavior.

The packets transmission can be view in the NAM software by using different color of arrows. The arrows are continuously move indicate the packet forwarding between the nodes.

D. *Analyze the transmission and detect attacks*

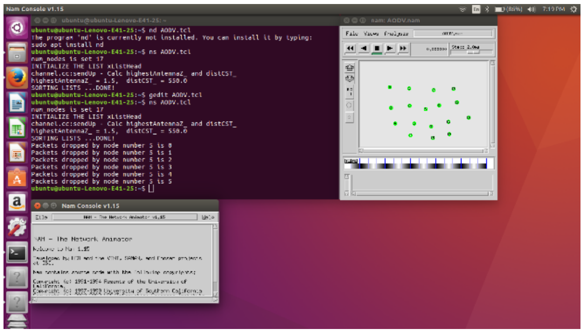
The packet transmission is analyzed by using the software like Xgraph or trace graph. Trace graph can view the analyzed information.

Using trace graph we can view the traffic behavior before malicious gets added and after inserting malicious behavior. Based on this two information, detect the malicious behavior. Based on this malicious behavior. Detect which type of attack is being occurred.

Using trace graph, we can view the networking information such as delay, number of generated packets, number of dropping packets, throughput etc. This information used for analyzing the traffic and detect the attacks.

4. Results and Discussion

A. *Black hole attack*



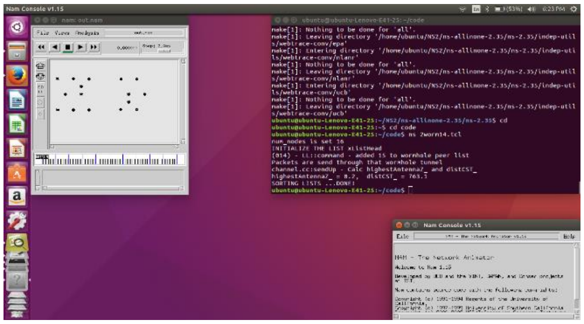
```
ubuntu@ubuntu-Lenovo-E41-25:~$ nd AODV.tcl
The program 'nd' is currently not installed. You can install it by typing:
sudo apt install nd
ubuntu@ubuntu-Lenovo-E41-25:~$ ns AODV.tcl
num_nodes is set 17
INITIALIZE THE LIST xListHead
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 550.0
SORTING LISTS ...DONE!
ubuntu@ubuntu-Lenovo-E41-25:~$ gedit AODV.tcl
ubuntu@ubuntu-Lenovo-E41-25:~$ ns AODV.tcl
num_nodes is set 17
INITIALIZE THE LIST xListHead
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 550.0
SORTING LISTS ...DONE!
Packets dropped by node number 5 is 0
Packets dropped by node number 5 is 1
Packets dropped by node number 5 is 2
Packets dropped by node number 5 is 3
Packets dropped by node number 5 is 4
Packets dropped by node number 5 is 5
ubuntu@ubuntu-Lenovo-E41-25:~$
```

Fig. 1. Black hole attack

Form this figure, we knew that first created all the nodes are good node and run the program it does not show any msg.

After that create node 5 as a black hole node and then run the program, it shows the packet dropping message.

B. *Wormhole attack*

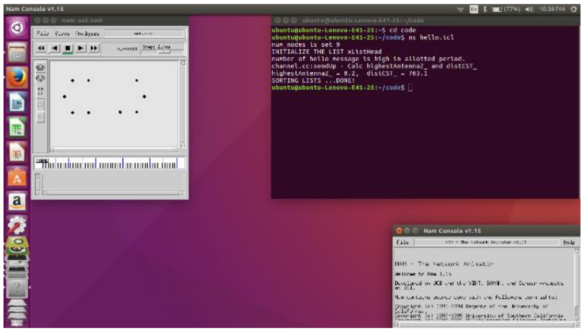


```
make[1]: Nothing to be done for 'all'.
make[1]: Leaving directory '/home/ubuntu/NS2/ns-allinone-2.35/ns-2.35/indep-util
s/webtrace-conv/epa'
make[1]: Entering directory '/home/ubuntu/NS2/ns-allinone-2.35/ns-2.35/indep-uti
ls/webtrace-conv/nlanr'
make[1]: Nothing to be done for 'all'.
make[1]: Leaving directory '/home/ubuntu/NS2/ns-allinone-2.35/ns-2.35/indep-util
s/webtrace-conv/nlanr'
make[1]: Entering directory '/home/ubuntu/NS2/ns-allinone-2.35/ns-2.35/indep-uti
ls/webtrace-conv/ucb'
make[1]: Nothing to be done for 'all'.
make[1]: Leaving directory '/home/ubuntu/NS2/ns-allinone-2.35/ns-2.35/indep-util
s/webtrace-conv/ucb'
ubuntu@ubuntu-Lenovo-E41-25:~/NS2/ns-allinone-2.35/ns-2.35$ cd
ubuntu@ubuntu-Lenovo-E41-25:~$ cd code
ubuntu@ubuntu-Lenovo-E41-25:~/code$ ns 2worm14.tcl
num_nodes is set 16
INITIALIZE THE LIST xListHead
(014) - LL::command - added 15 to wormhole peer list
Packets are send through that wormhole tunnel
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 8.2,  distCST_ = 763.1
SORTING LISTS ...DONE!
ubuntu@ubuntu-Lenovo-E41-25:~/code$
```

Fig. 2. Wormhole attack

Create 14 and 15 nodes as wormhole node and run the program. It shows error message as packets are send through wormhole tunnel.

C. *Hello flood attack*

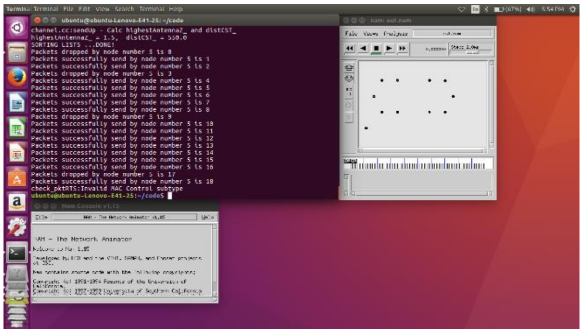


```
ubuntu@ubuntu-Lenovo-E41-25:~$ cd code
ubuntu@ubuntu-Lenovo-E41-25:~/code$ ns hello.tcl
num_nodes is set 9
INITIALIZE THE LIST xListHead
number of hello message is high in allotted period.
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 8.2,  distCST_ = 763.1
SORTING LISTS ...DONE!
ubuntu@ubuntu-Lenovo-E41-25:~/code$
```

Fig. 3. Hello flood attack

Each node has counter value of hello packets. If it exceeds it display error message as number of hello message is high in allotted period.

D. *Greyhole attack*

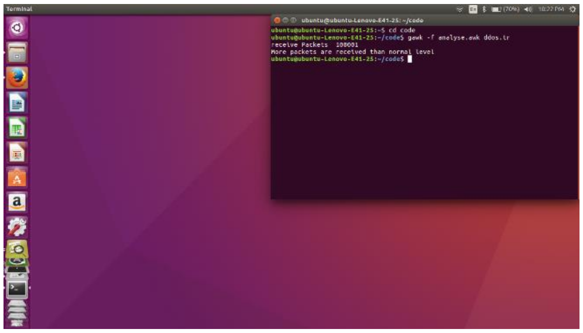


```
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 550.0
SORTING LISTS ...DONE!
Packets dropped by node number 5 is 0
Packets successfully send by node number 5 is 1
Packets successfully send by node number 5 is 2
Packets dropped by node number 5 is 3
Packets successfully send by node number 5 is 4
Packets successfully send by node number 5 is 5
Packets successfully send by node number 5 is 6
Packets successfully send by node number 5 is 7
Packets successfully send by node number 5 is 8
Packets dropped by node number 5 is 9
Packets successfully send by node number 5 is 10
Packets successfully send by node number 5 is 11
Packets successfully send by node number 5 is 12
Packets successfully send by node number 5 is 13
Packets successfully send by node number 5 is 14
Packets successfully send by node number 5 is 15
Packets successfully send by node number 5 is 16
Packets dropped by node number 5 is 17
Packets successfully send by node number 5 is 18
check_pktRTS:Invalid MAC Control subtype
ubuntu@ubuntu-Lenovo-E41-25:~/code$
```

Fig. 4. Greyhole attack

When run the program, it displays some of the packets are successfully sent but some packets are dropped.

E. *Denial of service attack*

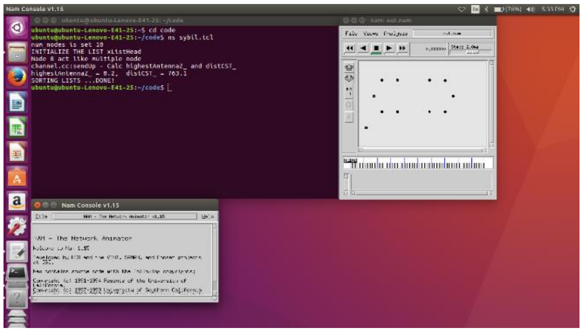


```
ubuntu@ubuntu-Lenovo-E41-25:~$ cd code
ubuntu@ubuntu-Lenovo-E41-25:~/code$ gawk -f analyse.awk ddos.tr
receive Packets  100001
More packets are received than normal level
ubuntu@ubuntu-Lenovo-E41-25:~/code$
```

Fig. 5. Denial of service attack

When run the program, it displays more packets are received than normal level.

F. *Sybil attack*



```
ubuntu@ubuntu-Lenovo-E41-25:~$ cd code
ubuntu@ubuntu-Lenovo-E41-25:~/code$ ns sybil.tcl
num_nodes is set 10
INITIALIZE THE LIST xListHead
Node 8 act like multiple node
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 8.2,  distCST_ = 763.1
SORTING LISTS ...DONE!
ubuntu@ubuntu-Lenovo-E41-25:~/code$
```

Fig. 6. Sybil attack

When run the program, it displays node 8 act like multiple nodes.

5. Conclusion

While IoT has huge social impact, it comes with a number of key security challenge. Hence, there is a need for an Intrusion Detection Systems (IDS) to monitor malicious activity or policy violations within a network of heterogeneous IoT devices and subsequently understand their impact. In this project, we propose the solution to detect all types of attacks in an IoT environment and also detect which types of attack occurred.

References

[1] Arunan Sivanathan, Daniel Sherratt, Hassan Habibi Gharakheili, Adam Radford, Chamith Wijenayake, Arun Vishwanath, and Vijay Sivaraman, (2017) "Characterizing and classifying iot traffic in smart cities and campuses", In Proc. IEEE INFOCOM Workshop SmartCity, Smart Cities Urban Comput., pp. 1–6.

[2] Chen Jun and Chen Chi. (2014), "Design of complex event processing ids in internet of things", in Measuring Technology and Mechatronics Automation (ICMTMA), 2014 Sixth International Conference on Measuring Technology and Mechatronics Automation, IEEE.

[3] Christopher D McDermott, FarzanMajdani, and Andrei V Petrovski (2018), "Botnet detection in the internet of things using deep learning approaches", International Joint Conference on Neural Networks (IJCNN), pp. 1–8. IEEE.

[4] Douglas H. Summerville, Kenneth M. Zach, and Yu Chen (2015), "Ultra-lightweight deep packet anomaly detection for internet of things devices", In Computing and Communications Conference (IPCCC), 2015 IEEE 34th International Performance, pp. 1–8. IEEE.

[5] Eirini Anthi, Lowri Williams, Małgorzata Słowi´nska, George Theodorakopoulos, Pete Burnap (2018), "A Supervised Intrusion Detection System for Smart Home IoT Devices", Cardiff University, School of Computer Science & Informatics, 5 The Parade, Roath, Cardiff, CF24 3AA.

[6] Eirini Anthi, Lowri Williams, and Pete Burnap (2018), "Pulse: An adaptive intrusion detection for the internet of things", School of Computer Science and Informatics, Cardiff University.

[7] Liang Xiao, Xiaoyue Wan, Xiaozhen Lu, Yanyong Zhang, and Di Wu (2018), "IoT security techniques based on machine learning".

[8] Mahmudul Hasan, Md. Milon Islam, Engineering (SOSE), 2015 IEEE Symposium on, pp. 78–87. IEEE.

[9] Nanda Kumar Thanigaivelan, Ethiopia Nigussie, Rajeev Kumar Kanth, Seppo Virtanen, and JouniIsoaho (2016), "Distributed internal anomaly detection system for internet-of-things", In Consumer Communications & Networking Conference (CCNC), 2016 13th IEEE Annual, pages 319–320. IEEE.

[10] Olivier Brun, Yonghua Yin, and Erol Gelenbe (2018), "Deep learning with dense random neural network for detecting attacks against iot-connected home environments", Procedia computer science, 134:458–463.

[11] Philokypros Ioulianou, Vasileios Vasilakis, Ioannis Moscholios (2018), and Michael Logothetis, "A signature-based intrusion detection system for the internet of things", Information and Communication Technology Form.

[12] Prabhakaran Kasinathan, Claudio Pastrone, Maurizio A Spirito, and Mark Vinkovits (2013). Denial-of-service detection in 6lowpan based internet of things. In Wireless and Mobile Computing, Networking and Communications(WiMob), 2013 IEEE 9thInternational Conference on, pages 600–607. IEEE.

[13] Prachi Shukla (2017), "Ml-IDS: A machine learning approach to detect wormhole attacks in internet of things", In Intelligent Systems Conference (IntelliSys), pages 234–240. IEEE.

[14] R Stephen and L Arockiam (2017), "Intrusion detection system to detect sinkhole attack on rpl protocol in internet of things", International Journal of Electrical Electronics & Computer Science Engineering Volume 4, Issue 4

[15] Rohan Doshi, Noah Apthorpe, New Jersey (2018), "Machine Learning DDoS Detection for Consumer Internet of Things Devices", IEEE Symposium on Security and Privacy Workshops.

[16] ShahidRaza, Linus Wallgren and Thiemo Voigt. Svelte (2015), "Real-time intrusion detection in the internet of things", International Journal of Computer Applications, vol. 121, no. 9.

[17] Tariqahmad Sherasiya, Hardik Upadhyay, "Intrusion Detection System for Internet of Things", IJARIIE, vol. 2, no. 3, 2016.