Fraud detection in dynamic interaction network

R. Karunamurthy[1], G. Ramasubramaian[2]

[1]*Dept of Computer Science, School of Arts and Science, Vinayaka Mission's Research Foundation, Chennai, India.*
Email : kdkaran2016@gmail.com

[2]*Associate Professor, Dept of Computer Science, School of Arts and Science, Vinayaka Mission's Research Foundation, Chennai, India.*
Email: ramasubramanian.csa@avit.ac.in

ABSTRACT

With the advent of smart devices and lowering prices of sensing devices, adoption of Internet of Things (IoT) is gaining momentum. These IoT devices come with greater threat of being attacked or compromised that could lead to Denial of Service (DoS) and Distributed Denial of Service (DDoS). The high volume of IoT devices with high level of heterogeneity, magnify the possibility of security threats. So far, there is no protocol to guarantee the security of IoT devices. But to enable resilience, continuous monitoring is required along with adaptive decision making. These challenges can be addressed with the help of Software Defined Networking (SDN) which can effectively handle the security threats to the IoT devices in dynamic and adaptive manner without any burden on the IoT devices. In this paper, we propose an SDN-based secure IoT framework called Soft Things to detect abnormal behaviors and attacks as early as possible and mitigate as appropriate.

Keywords: IoT, SDN, DDOS, Cloud, Dynamic Attack Detection.

I. INTRODUCTION

You use the "cloud storage" technology anytime you save your photos online instead of on your home computer, or when you use webmail or a social networking site. Of example, if you are an enterprise and want to use an online invoicing program instead of upgrading the one you have been using in-house for many years, the online invoicing software is a "cloud computing" service. Cloud computing relates to computational services being distributed over the Internet. Instead of keeping data on your own hard drive or upgrading software to match your needs, you use an Internet service to archive the information or use the apps at another venue. Doing so could give rise to certain consequences for privacy.

The Internet of Things (IoT) is becoming increasingly popular in daily life because it can link the physical phenomena known as things with the virtual world, i.e. the Web. Not only new age smart devices, wearables, cameras, smart lights, but also household appliances such as washers, refrigerators, doors to the house are connected to the Internet, creating a vibrant IoT ecosystem. The development of sensor technology has enabled the rapid growth and the widespread consumption of the stuff since the last decade. It's estimated that the Web would link 11.8 billion items by 2018. IoT has also opened up tremendous commercial and industrial possibilities in such fields as smart mobility, industrial automation. With this exponential development of IoT, shielding certain systems from cyber attacks is becoming critically important. Then, unauthorized consumers or criminals will take control of the machines and, apart from breach of privacy, critical things will be at risk. Another issue is that these IoT systems have no or very little device-level security functionality.

So it may not be possible to provide protection at device level for a large number of heterogeneous IoT systems.

The introduction of Software Defined Networking (SDN) provides complex, flexible and remote control of a network. SDN's main objective is to separate the control plane from the data plane. Therefore, data forwarding actions are conducted separately than networking protocols ' conceptual procedures. We will draw on SDN capabilities to offer many IoT security benefits. With the support of SDN, irregular flows can be identified at SDN-enabled switches sooner, with faster response. Due to different traffic characteristics with various IoT apps, and different usage habits over time, it becomes difficult. While targeting IoT systems, SDN may play a significant role in handling the complex flow and minimizing the assault by preventing or restricting the suspected flows. The identification of the threat can be moved towards the edge of the IoT network. Such early detection allows for early response to attacks through prevention and separation of the systems being targeted. This early detection often helps to reduce resource wastage due to traffic assaults like DoS or DDoS that use a large amount of network bandwidth. In fact, SDN will help improve the accuracy of detection mechanisms by running clever, sophisticated algorithms.

Related Works

Gubbi et al [2] provided a Cloud-centric view of the Internet of Things being applied worldwide. It addresses the core supporting technologies and technology domains which are likely to drive IoT work in the near future. Presentation of a software architecture utilizing Aneka, which is focused on private and public cloud connections. We conclude our IoT dream by building on the need for WSN, the Internet, and global technical science community-oriented computing convergence.

Abu Rajab et al [5] are trying to clear the confusion around botnets in this paper by con-structuring a multi-faceted and distributed system of measurement. They have used this network over a span of more than three months to map 192 specific scale IRC botnets varying from a few hundred to several thousand infected end-hosts.

Palani et al [8] exploring what's going to happen in the IoT if we develop their structures the same way. They gather data and model the blooms of bugs and patching delays in historical networks. They show the models and discuss future IoT networks where identical blooms do exist but there is no patching. They address initial results, and our plans to expand the models in our upcoming work to look more closely into these topics.

Zhang et al [9] in the sense of calculating comparisons, or equivalently spatial differences, they find visual category identification to be conceptual representations of categories. This method is quite versatile, and allows for identification in a homogeneous context based on colour, texture, and particularly form. While in this setting the nearest neighbor classifiers are normal, in the case of small sampling they suffer from the issue of high variance (in bias-variance decomposition). Instead, one might use vector support machines but they require time-consuming computation and pair distance measurement. They suggest a combination of these two approaches that deals with multiclass setting inherently, has fair computational complexity in both training and run-time, and produces excellent results in practice.

III. PROPOSED SYSTEM

We are tackling the IoT security problem. Through SDN support, we aim to prevent network-level attacks instead of device-level. Our goal is to protect the IoT systems from malicious attacks and to reduce the damage following an attack. The

assault can be initiated or the computer is the target from the IoT system itself. This helps to identify threats on IoT devices easily, and implement protection when necessary. We've been using machine learning methods to spot traffic irregularities. To multiple assault scenarios we tested our setup and strategies utilizing Mininet related emulation experiments.

We discuss in this paper the design and implementation of an integrated resource management program that maintains a good balance between the two goals of IoT. Two goals are avoiding overload and green computing.

1. Overload avoidance: A PM's capability should be sufficient to meet the resource needs of all SDNs that operate on it. Otherwise the PM is overwhelmed and its SDNs will result in deteriorated results.

2. Green computing: The amount of PMs used should be reduced as long as the demands of all SDNs can still be met. It is possible to switch off unused PMs to save electricity.

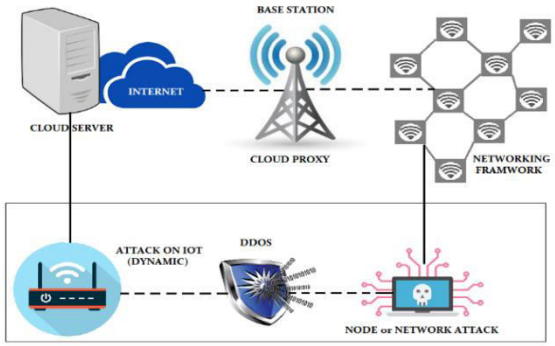

Fig.1. Overall architecture of Proposed System

We are proposing the following recommendations from the proposed system:

- We are designing a resource allocation method that can effectively prevent congestion within the network while reducing the number of servers used.
- To calculate an unequal use of a computer, we introduce the concept of "skewness." In terms of multidimensional resource constraints, we will improve the overall use of servers by reducing skewness.
- We build a load prediction algorithm that correctly captures potential device resource usages without looking inside the SDNs. The algorithm will catch the rising trend in resource consumption trends and help significantly raising the turnover of placement.

A. Network topology Construction

A Network Topology that consist of routers linked to local area networks that are no.of. Thus, either a router may receive data from the closest router, or from the local area network. A boundary router gets packets from their local network. Many routers get packets from a core router. The routers no.of linked to a single router are named as router degree. This is placed in a table and measured. All router's Upstream interfaces also need to be found and placed in the configuration list.

B. Path Selection

The route is said to be the way the chosen packet or file to be sent to the destination from source. Growing router's Upstream interfaces must be identified and stored in the interface table. The optimal path between the chosen source and destination can be specified with the help of that interface table.

C. Packet Sending

For the transformation process one of the packet or file must be chosen. The packet is sent from the source LAN to destination LAN using IOT along the given route. The destination LAN receives the packet and tests whether it was sent along the stated path or not.

D. Packet Marking and Logging

Packet marking is the step in which the successful Packet Marking algorithm is implemented along the given path at each router. It

determines the importance of the Pmark and stores it in a hash table. If the P-mark is not exceeding than the router's ability, it will be redirected to the next router. Otherwise the hash table is indexed, and the algorithm is implemented again.

E. Path Reconstruction

After implementing the algorithm, once the packet has reached its destination, it tests whether it has sent it from the appropriate upstream interfaces. If any of the attack is detected, the path reconstruction demands it. Path reconstruction is the process of finding a new path for the same source and the destination where there can be no attacks.

F. Attacker

Routing attacks will misuse the mechanisms of routing protocols in IoT for route discovery and topology generation. For eg, an intruder might advertise routes with hop counts that are higher or lower than actual routes. To the advantage of the intruder, this could be used to draw traffic to compromised nodes. Malicious behavior can lead to; data theft, packet sinking, and packet alteration. All of these findings hinder the capacity of the networks to maintain safe, confidential, and effective SDN communication. Unsecured pro-active routing protocols pose susceptibility to replay and exploit packets. Wormhole and Sybil attacks were examined by protocols such as SAODV and SOLSR, and discussed. The protection offered by these protocols is oriented towards securing network routing services. Such protocols do not cover data transmitted along protected routes.

G. Authentication

Authentication guarantees the identities of IoT nodes that interact. Participation in a closed network is limited to approved nodes, and correspondence is authenticated to discourage third party interpretation of network communication contents. Authentication is required to allow the existing network members to join new nodes and be treated as valid. Any packet that SOLSR sends is signed digitally using a mutual password. If the signature of an incoming packet becomes unreadable, it discards the packet as being unauthentic. This is a point-to-point operation, and does not authenticate the source. SOLSR utilizes time-stemped packets to block replay assaults. If a valid node sees a time-stamp twice, then the packet will be discarded. Authentication provides a means of defining a node as being respected. Two nodes can authenticate one-another based on their mutual Trusted Authority by using a certificate to confirm they share a trusted authority.

IV. EXPERIMENTAL RESULTS

In this part, we showed the proposed model implementation result.

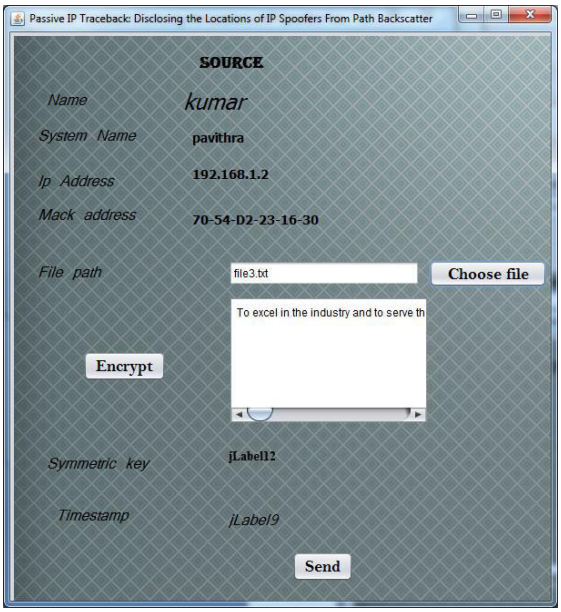

Fig.2. Showed the File Selecting Result

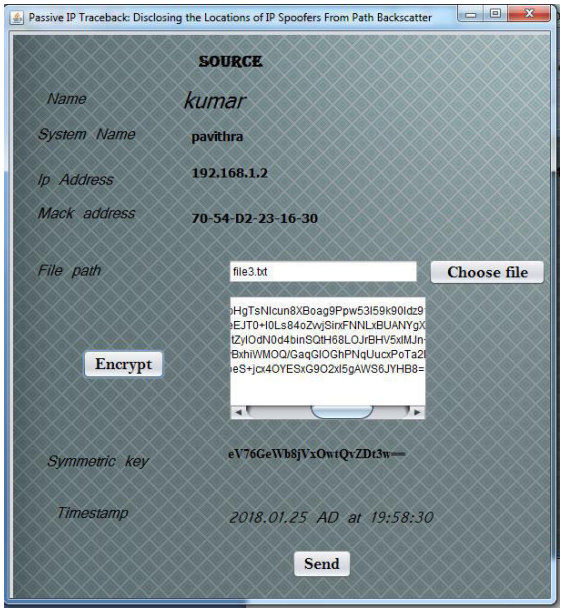

Fig.3. Showed the File Encryption Result

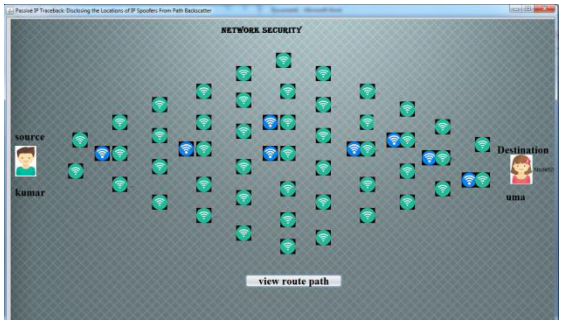

Fig.4. Path Creation

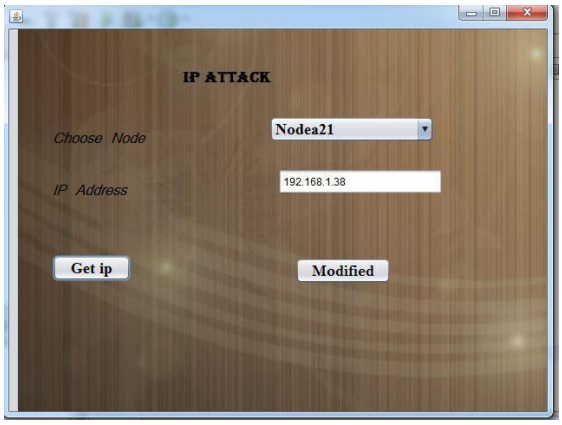

Fig.5. IP login

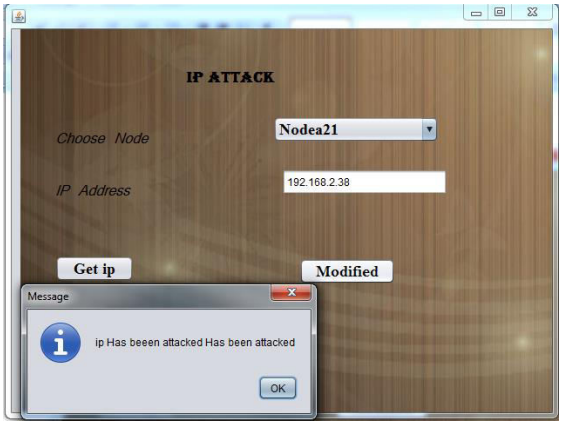

Fig.6. IP creation

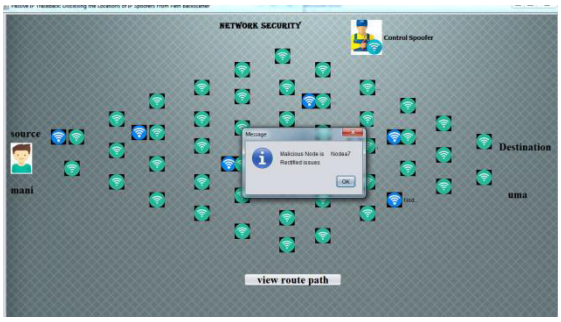

Fig.7.Shortest Path detection

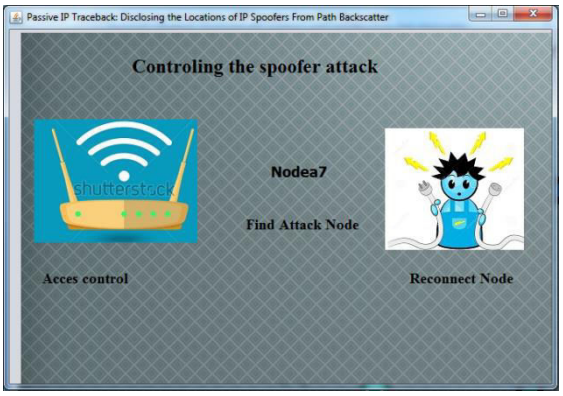

Fig.8. IP attacks

V. CONCLUSION

IoT systems are vulnerable to attacks because of poor safety standard of the system. We tackled the problems resulting from such attacks by using SDN's capabilities. We introduced a SDN-based platform for identifying and minimizing anomaly in IoT flow, named Soft Things. The purpose of this system network, rather than detecting at the network's heart or higher level. We also suggested IP Trace back (PIT) monitoring spoofers based on route backscatter messages and details available to the public. On route backscatter, we explain causes,

sets, and statistical effects. We defined how to apply PIT when both topology and routing are known, or the routing is uncertain or none is established. We provided two successful algorithms for applying PIT to large-scale networks and proved their accuracy. We also shown PIT's usefulness dependent on both deduction and simulation. A single efficient method protects the routing and device data these tests can further expose IP spoofing, which has been researched for a long time but never understood so well.

REFERENCES

[1] ITU report, "The Internet of Things," 2005.

[2] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," Elsevier FGCS, vol. 29, no. 7, pp. 1645–1660, 2013.

[3] Gartner report, "Forecast: IoT Security, Worldwide," 2016.

[4] IDC report, "Internet of Things: Security Practices," 2016.

[5] M. Abu Rajab, J. Zarfoss, F. Monrose, and A. Terzis, "A multifaceted approach to understanding the botnet phenomenon," 6th ACM SIGCOMM conference on Internet measurement, pp. 41–52, 2006.

[6] Dyn attack 2016, http://dyn.com/blog/dyn-analysis-summary-of-fridayoctober-21-attack/, [Online; accessed 18-07-2017].

[7] Mirai Malware 2016, http://blog.malwaremustdie.org/2016/08/mmd0056-2016-linuxmirai-just.html, [Online; accessed 18-07-2017]. '

[8] K. Palani, E. Holt, and S. Smith, "Invisible and forgotten: Zero-day blooms in the IoT," IEEE PerCom Workshops, pp. 1–6, 2016.

[9] H. Zhang, A. C. Berg, M. Maire, and J. Malik, "SVM-KNN: Discriminative nearest neighbor classification for visual category recognition," IEEE CVPR Conference, pp. 2126–2136, 2006.

[10] K. Sood, S. Yu, and Y. Xiang, "Software-defined wireless networking opportunities and challenges for Internet-of-Things: A review," IEEE Internet of Things Journal, vol. 3, no. 4, pp. 453–463, 2016.

[11] N. Bizanis and F. A. Kuipers, "SDN and virtualization solutions for the Internet of Things: A survey," IEEE Access, pp. 5591–5606, 2016.

[12] A. El-Mougy, M. Ibnkahla, and L. Hegazy, "Software-defined wireless network architectures for the Internet-of-Things," 40th IEEE LCN Workshops, pp. 804–811, 2015.

[13] Y. Jararweh, M. Al-Ayyoub, E. Benkhelifa, M. Vouk, A. Rindos et al., "SDIoT: a Software Defined based Internet of Things framework," Journal of Ambient Intelligence and Humanized Computing, vol. 6, no. 4, pp. 453–461, 2015.

[14] O. Flauzac, C. Gonzalez, A. Hachani, and F. Nolot, "SDN based ´ architecture for IoT and improvement of the security," 29th IEEE WAINA Conference, pp. 688–693, 2015.

[15] V. Sivaraman, H. H. Gharakheili, A. Vishwanath, R. Boreli, and O. Mehani, "Network-level security and privacy control for smart-home IoT devices," 11th IEEE WiMob Conference, pp. 163–167, 2015.