# ANALYSIS SECURITY THREATS IN COAP BASED IOT: A SURVEY

Vraj Shah[1]

[1] *Student M.Tech. in Cyber Security, Dep. of Computer Engineering, Marwadi University, Gujarat, India*

**ABSTRACT**

*In the past several years, the Internet of Things (IoT) has grown into protocols. Application protocol for constrained applications (CoAP) is unique to communications protocols. This protocol is a lightweight protocol, often used in Internet of things. Maximum IoT devices are constrained network devices that are related to the internet and perform sensing tasks. That system is understood through its special address and makes use of one of the key communication protocols for the network is the CoAP. Survey on several major attacks against the CoAP protocol carried out in the Internet of Things (IoT).*

**Keyword :** - *Internet of Things, Constrained Network, CoAP, DTLS, DOS, Sniffing, MitM*

## 1. INTRODUCTION

In the new smart world, we are continuous use smart home, smart cars, smart watches and among others. We can use such devices as we can imagine in our dreams, where things are intelligent and interconnecting. IoT's a promising field, Which means everything is linked to the net via the network and transmits data like live actions on secondary objects. In the business world, the IoT (Internet of Things) changed immensely our view, use and interaction with smart devices. The people is utilizing the existing IoT emerging technologies for sensing, networking and automation has revealed the reality that it brings major variations in the transportation, goods and services, And the socio-economic strengthening thus has an effect on these changes. At least 50 billion ' things ' are expected to become connected to the Internet by 2020 [2].

CoAP is emerging a standard web protocol for the precise requirements of constrained environment, building automation, and various machine-to-machine (M2M) functions [12].

### 1.1 CoAP Architecture

The communication model of CoAP is similar to the server and client configuration of HTTP. [Fig 1] indicates that the structure of CoAP. CoAP is an architecture of two layers. The last layer is the UDP and Asynchronous Message layer and the Coordination method is the layer of request and response [11].

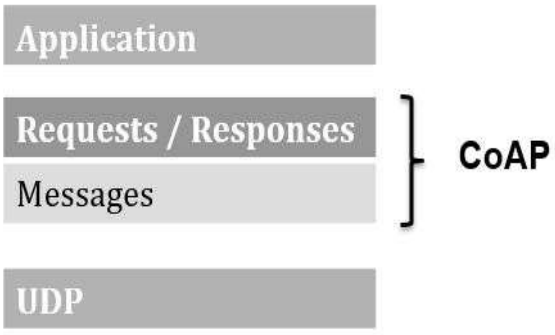


**Fig -1**: Layers of CoAP

[Fig 2] Provides CoAP architecture. As shown, it expands traditional HTTP clients to users with limited resources. Such customers are CoAP customers, too. The proxy device bridges the gap from the standard HTTP protocol

internet environment to a unified environment. The same server administrates all HTTP and CoAP protocol messages.

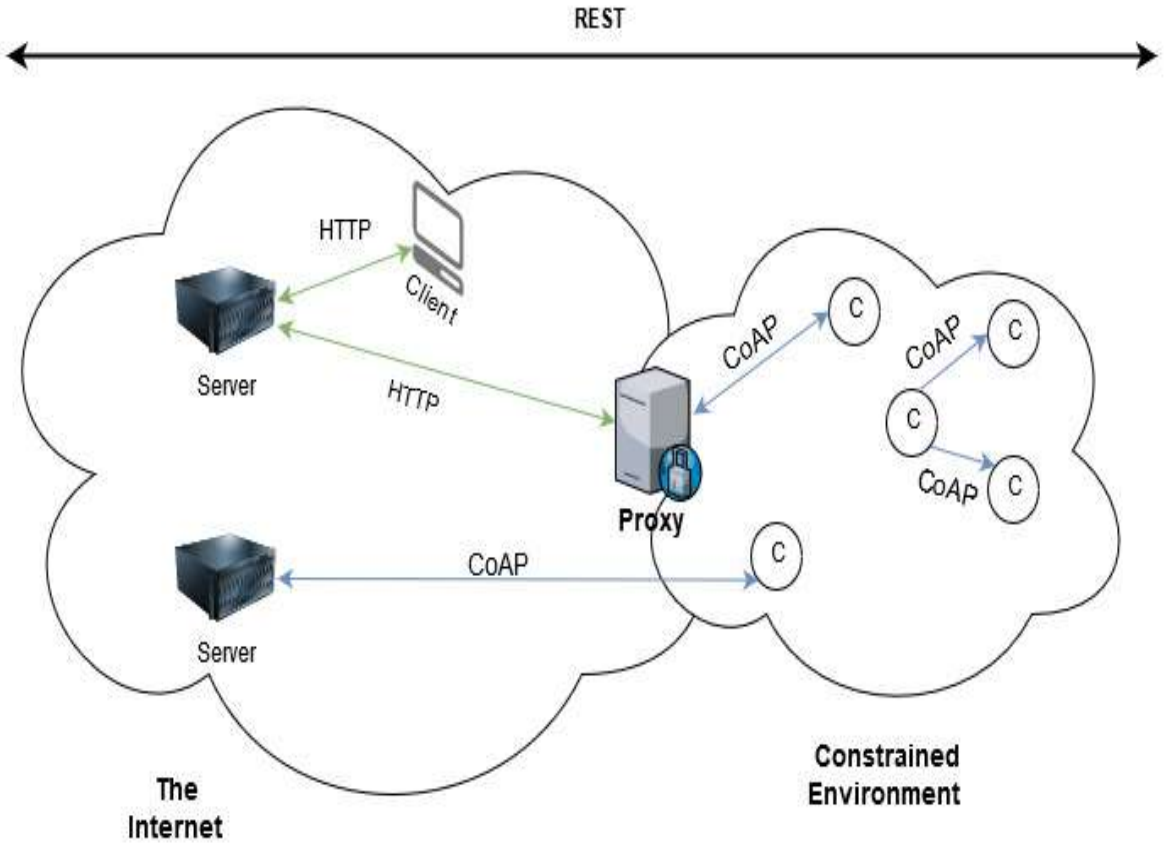


**Fig -2**: CoAP Architecture

**1.2 DTLS-Secured CoAP**

Use of Transport Layer Security (TLS) over TCP is protected by HTTP, use of Datagram TLS (DTLS) is secured by CoAP over UDP. DTLS is TLS with elements supplied to address the unreliable nature of UDP transportation [Fig 3].

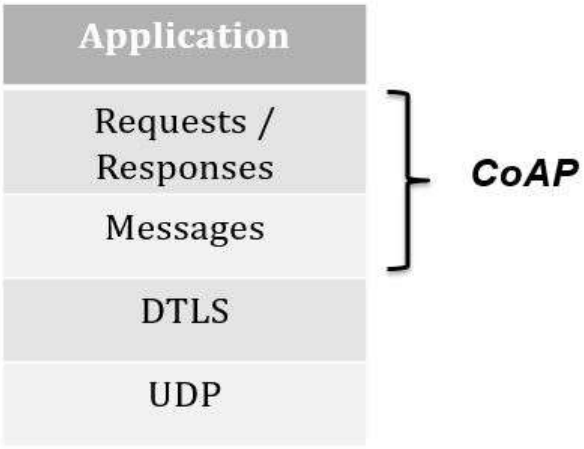


**Fig -3**: DTLS-Secured CoAP

### 1.3 CoAP Implementation

There are a variety of techniques of executions of CoAP. In below, Table display the most common implementations

**Table -1:** CoAP Tools

| | |
|---|---|
| **Constrained Devices** | Erbium, libcoap, tinydtls, SMCP, microcoap, cantcoap |
| **Browser – based** | Copper, thethings.IO |
| **Server – Side** | Python, Erlang, CoAPSharp |

## 2. RELATED WORK

In this paper [2], they have talk about the some security issue. Like sniffing CoAP proxy setup, client, server attacks on the test network, they have successfully penetrate and gain access to Intel on the type information exchanged between the server and client.
Paper [9] in this paper, they proposed framework. In this proposed framework, a type of ticket is used and packet formats are specified to allow for the use of well-known authentication protocols such as Kerberos or RADIUS. The CoAP extension of this mechanism provides the best way for a CoAP-based server/service to be exploited. They have given Security elements of the proposed platform against distinctive attacks like Dos, Spoofing, Man in the middle attack.
Paper [10] The DOS detection system based on a network structure of ebbits was used to detect DoS attacks successfully. It happens in relation to situations from the real world. In addition, they have given list of threats relevant to 6LoWPAN smart objects and identify them. DTLS and IPSec protocols were suggested to protect the CoAP. In this paper, examine and evaluate these suggested protocols to protect the CoAP [7].
Based on the associated work, what are the frequent threats centered in CoAP environment and they provide a framework [9, 10] or attack detection [10].

## 3. Threats within the CoAP Protocol

Whereas authentication mechanisms were implemented in CoAP, it is suffering from common attacks.

The vulnerabilities were listed from the various white papers in which the researchers found such vulnerabilities and possible threats in the sub-sections below.

### 3.1 Explanation specific vulnerability and attacks in CoAP

- **Denial of Service:** DoS attacks are measured as an integral security problem. These attacks can be initialized with regular commands from remote locations, mixed with advanced tools; attackers are even expected to perform distributed DoS attacks that are effective in taking down massive networks. There is no protection against such attacks in the CoAP.

- **Man In The Middle:** MitM happens when an attacker captures packets or communications between two operations to either cover or shift traffic between them. Attackers might use MitM attacks to sniper login credentials, spy on a victim, sabotage or corrupt information.

- **Sniffing:** Sniffing is a monitoring and capture procedure for all data packets that pass through a given network. Attackers use sniffers to seize packets of data that contain sensitive information like passwords, account information, etc.

- **Application Layer:** Constrained application protocol is being standardized as the application protocol for 6LoWPAN. Since still many securities, concern should arise in future. Some vulnerabilities are cross-protocol attack, Threat of amplification, Proxying and caching, SYN flood, IP address spoofing [10].

## 4. Analysis of CoAP Attacks

According to Dennis Rand, founder of eCrimeLabs, CoAP devices has exploded since November 2017. CoAP's count of devices increased to over 26,000 in November 2017 from a low of 6,500. The situation became worse in 2018 because, according to Shodan, a search engine for internet-connected devices, by May this number was 278,000, which currently hovered at 580,000 - 600,000 [8].


## 5. CONCLUSIONS

The Internet of Things is considered one of the greatest strides in the direction of a technologically strong future. It is important to have a stable IoT network to develop and integrate this technology into our daily lives. This paper provides a comprehensive evaluation of the security of CoAP through a discussion on vulnerabilities and attacks. A CoAP's multiple implementations have significantly increased market interest in IoT technology. The future of all applications is expected to change by CoAP. Future work should concentrate on evaluating these attacks with different tools and the effect of the attack on the environment of CoAP.

## 6. REFERENCES

[1]. R. A. Rahman and B. Shah, "Security analysis of IoT protocols: A focus in CoAP," 2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC), Muscat, 2016, pp. 1-7.
[2] S. Arvind and V. A. Narayanan, "An Overview of Security in CoAP: Attack and Analysis," 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), Coimbatore, India, 2019, pp. 655-660.
[3] V. Lakkundi and K. Singh, "Lightweight DTLS implementation in CoAP-based Internet of Things," 20th Annual International Conference on Advanced Computing and Communications (ADCOM), Bangalore, 2014, pp. 7-11.
[4] L. Canuto, L. Santos, L. Vieira, R. Gonçalves and C. Rabadâo, "CoAP Flow Signatures for the Internet of Things," 2019 14th Iberian Conference on Information Systems and Technologies (CISTI), Coimbra, Portugal, 2019, pp. 1-6.
[5] R. K. Kodali, B. Yatish Krishna Yogi, G. N. Sharan Sai and J. Honey Domma, "Implementation of Home Automation Using CoAP," TENCON 2018 - 2018 IEEE Region 10 Conference, Jeju, Korea (South), 2018, pp. 1214-1218.
[6] S. Raza, D. Trabalza and T. Voigt, "6LoWPAN Compressed DTLS for CoAP," 2012 IEEE 8th International Conference on Distributed Computing in Sensor Systems, Hangzhou, 2012, pp. 287-289.

[7] T. A. Alghamdi, A. Lasebae and M. Aiash, "Security analysis of the constrained application protocol in the Internet of Things," Second International Conference on Future Generation Communication Technologies (FGCT 2013), London, 2013, pp. 163-168
[8] Cimpanu, C. (2020). The CoAP protocol is the next big thing for DDoS attacks | ZDNet. [online] ZDNet. Available at: https://www.zdnet.com/article/the-coap-protocol-is-the-next-big-thing-for-ddos-attacks/ [Accessed 28 Jan. 2020].
[9] P. P. Pereira, J. Eliasson and J. Delsing, "An authentication and access control framework for CoAP-based Internet of Things," IECON 2014 - 40th Annual Conference of the IEEE Industrial Electronics Society, Dallas, TX, 2014, pp. 5293-5299.
[10] P. Kasinathan, C. Pastrone, M. A. Spirito and M. Vinkovits, "Denial-of-Service detection in 6LoWPAN based Internet of Things," 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Lyon, 2013, pp. 600-607.
[11] Chen, X. (2020). Constrained Application Protocol for Internet of Things. [online] Cse.wustl.edu. Available at: https://www.cse.wustl.edu/~jain/cse574-14/ftp/coap/ [Accessed 3 Jan. 2020].
[12] Tools.ietf.org. (2020). RFC 7252 - The Constrained Application Protocol (CoAP). [online] Available at: https://tools.ietf.org/html/rfc7252 [Accessed 3 Jan. 2020].