**CATComp: A Compression-Aware Authorization Protocol for Resource-Efficient Communications in IoT Network [Summary]**

The Internet of Things(IoT) describes the network of physical objects that are embedded with sensors, software and other technologies for the aim of connecting & exchanging data with other devices and systems over the internet. Intelligent devices and machines are connected to each other and also the Internet. They capture relevant information about theirfirect environment, then analyze and link it. The IoT devices need to exchange certificates & Authorization tokens over the **IEEE 802.15.4** radio medium which can support a maximum transmission unit of 127 bytes. A large number of fragments needed due to significantly larger than MTU credentials. As those devices are battery powered and the fragment process increases the power consumption, **it limits the ability to server real-time requests and shorter battery life**.

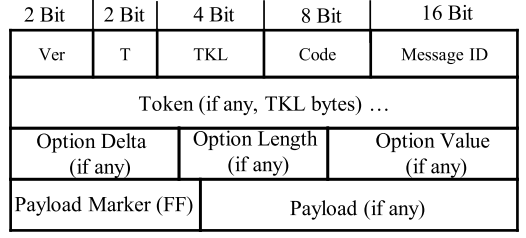
In this paper, they proposed **CATComp**- “Compression-aware authorization protocol” for “Constrained application protocol” **(CoAP)** along with datagram transport layer security**(DTLS)**. It is able to enable IoT devices to exchange small-sized certificates and capability tokens over the **IEEE 802.15.4** media. **Here “IEEE 802.15.4” is a low-cost, low-data-rate wireless access technology for devices that are operated or work on batteries.** CATComp adds an additional message in the CoAP & DTLS handshake. Through this, the communicating devices use compression methods which decrease the size of the security materials and minimize the total number of packet fragments before sending them over the network(IEEE 802.15.4 link).

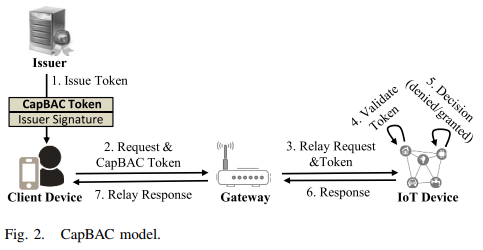
It also minimizes the communication overheads for package delivery, package processing delay and energy consumption. It will help the devices in order that they will respond to requests faster and therefore the device can have longer battery life. Their experiment results show that the communication latency and energy consumption are reduced when the CATComp is integrated with CoAP and DTLS. Additionally, the changes of fragmentation attacks are reduced as devices exchange a fewer number of certificate and token fragment when compression is applied using CATComp.

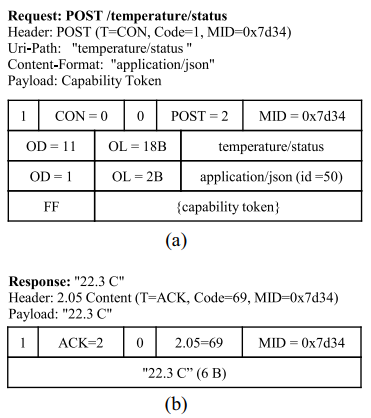
The revolution of the computer devices with the modern technological advancement of communication, the IoT concept is utilized by Several application domains [1]. Recent research anticipates that in a year, on an average, around one million new IoT devices will be deployed to different application domains for the next few years[8]. IoT devices are resource constrained and operate on low power and lossy networks[9]. In DTLS, IoT devices issued X.509 certifications, where in exchange for mutual authentication, A sender device attaches its token with a CoAP request. Also a receiver device validates the token to ensure the client is authorized to access the requested services or resources. The contribution of this paper follows:

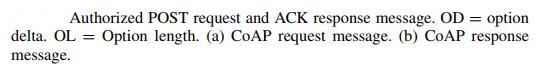
1. Handshake at the DTLS and CoAP layers that enables IoT devices to compress and decompress at the application layer and transport layers.
2. Designed various customized messages which can allow a sender device to negotiate a particular compression method with a receiver device while establishing DTLS session.
3. Introduced multiple headers at the CoAP layer that allows a sender device to instruct the DTLS layer to compress outgoing authorization tokens.
4. Implemented a prototype of CATComp using RE-Mote IoT devices to demonstrate the feasibility of the proposed schema.
5. Provided experimental evaluations, which show that communication overheads for fragment delivery and energy costs for data processing were reduced when CSTComp were adopted to exchange CoAP messages over DTLS sessions.

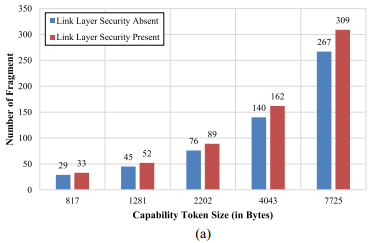
CoAP as Application Layer Protocol: CoAP implements a request and response model.

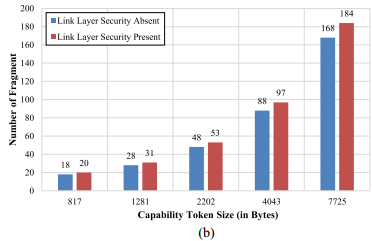
Here a client will send a CoAP request over a UDP packet. Then the recipient will reply with a CoAP response message. This thing is shown in figure on the left side. The message uses binary format which includes 4-byte header(Fixed size), variable token, sequence of CoAP options, payload. Ver indicates CoAP, T indicates ‘type of CoAP message’ where T=0 means confirmable message, T=1 means non confirmable message, T=2 means acknowledge message and T=3 means reset message. 

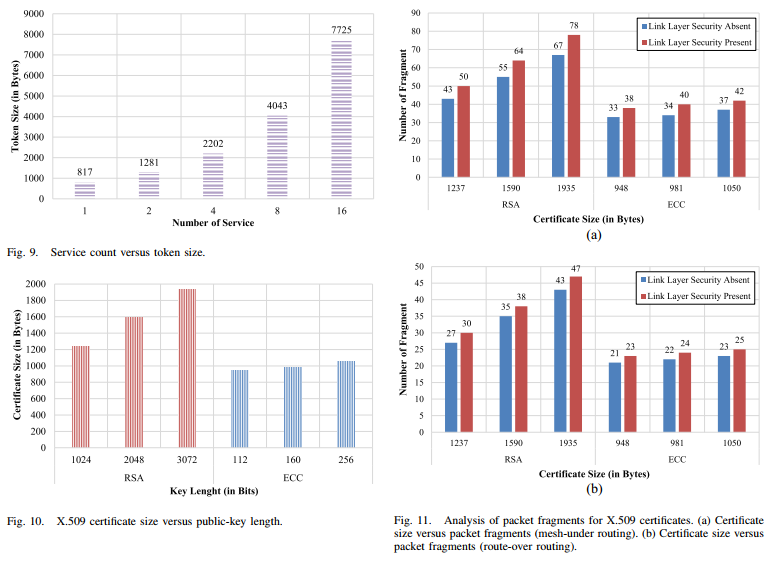
The code indicates the message type of requests like GET(1), POST(2), PUT(3), DELETE(4). This ID works as a identifier of a message. Every CoAP option is assigned an option number such as Uri-Host(1), Uri-Port(3), Uri-Path(11), Content Format(12), Uri-Query(15). 





CoAP was designed to avoid fragmentation of a UDP packet. As the X.509 certificates and authorization tokens were sent in a large number of fragments, they do not fit in a single frame and those large number of fragments increases the packet delivery time. The processing of these packets fragmentation on the sender end and reassembly on the receiver end- increases energy consumption by the sender and receiver IoT devices. 



****

Their proposed scheme CATComp- a protocol that facilitates certificate and authorization token compression at DTLS and CoAP layers, respectively. The size of the certificates and CoAP requests are reduced after the compression, which results in a minimal number of packet fragments for a service request. The time to delivery a request to a receiver IoT node increases with an increase in the number of packet fragments.

In the article, their proposed CATComp compression aware protocol that enables IoT devices to exchange compressed X.509 certificates and authorization tokens. In 6LoWPAN networks, often, certificates and authorization tokens. In 6LoWPAN networks, often, certificates and authorization tokens contribute a significant portion in a communication packet. Therefore, the number of packet fragments varies with the size of these certificates and authorization tokens. CATComp enables communicating devices to compress X.509 certificates and authorization tokens at the DTLS and CoAP layers before sending them over the low-powered and lossy networks. Thus, CATComp enables devices to minimize the number of packet fragments significantly. We implemented a prototype of CATComp on Contiki-enabled RE-Mote IoT devices and provided a performance analysis of CATComp in terms of communication and energy efficiency. The experimental results showed that sizes of the DTLS and CoAP payloads were reduced significantly by compressing certificates and authorization tokens. The smaller sized payloads resulted in decreasing the number of packet fragments, which yielded less communication overhead and energy consumption for fragment processing. As such, devices could exchange messages faster and experience longer battery life.

**REFERENCES**

[1] R. Petrolo, V. Loscri, and N. Mitton, “Towards a smart city based on cloud of things, a survey on the smart city vision and paradigms,” Trans.

Emerg. Telecommun. Technol., vol. 28, no. 1, 2017, Art. no. e2931.

[2] A. S. Deese et al., “Long-term monitoring of smart city assets via

Internet of Things and low-power wide-area networks,” IEEE Internet

Things J., vol. 8, no. 1, pp. 222–231, Jan. 2021.

[3] Y. Meng, W. Zhang, H. Zhu, and X. S. Shen, “Securing consumer IoT in

the smart home: Architecture, challenges, and countermeasures,” IEEE

Wireless Commun., vol. 25, no. 6, pp. 53–59, Dec. 2018.

[4] M. Hossain, S. M. R. Islam, F. Ali, K.-S. Kwak, and R. Hasan, “An

Internet of Things-based health prescription assistant and its security

system design,” Future Gener. Comput. Syst., vol. 82, pp. 422–439,

May 2018.

[5] F. Zhu, Y. Lv, Y. Chen, X. Wang, G. Xiong, and F.-Y. Wang, “Parallel

transportation systems: Toward IoT-enabled smart urban traffic control

and management,” IEEE Trans. Intell. Transp. Syst., vol. 21, no. 10,

pp. 4063–4071, Oct. 2020.

[6] H. Sedjelmaci, M. Hadji, and N. Ansari, “Cyber security game for intelligent transportation systems,” IEEE Netw., vol. 33, no. 4, pp. 216–222,

Jul./Aug. 2019.

[7] O. Elijah, T. A. Rahman, I. Orikumhi, C. Y. Leow, and M. N. Hindia,

“An overview of Internet of Things (IoT) and data analytics in agriculture: Benefits and challenges,” IEEE Internet Things J., vol. 5, no. 5,

pp. 3758–3773, Oct. 2018.

[8] Forbes. (2017). Roundup of Internet of Things Forecasts. [Online].

Available: https://goo.gl/iVf5uz

[9] R. Hummen, J. Hiller, H. Wirtz, M. Henze, H. Shafagh, and K. Wehrle,

“6LoWPAN fragmentation attacks and mitigation mechanisms,” in

Proc. 6th ACM Conf. Security Privacy Wireless Mobile Netw., 2013,

pp. 55–66.

[10] Y. Luo and L. Pu, “Practical issues of RF energy harvest and data transmission in renewable radio energy powered IoT,” IEEE Trans. Sustain.

Comput., early access, Jun. 4, 2020, doi: 10.1109/TSUSC.2020.3000085.

[11] M. Hossain and R. Hasan, “P-HIP: A lightweight and privacy-aware

host identity protocol for Internet of Things,” IEEE Internet Things J.,

vol. 8, no. 1, pp. 555–571, Jan. 2021.

[12] T. Winter, “RPL: IPv6 routing protocol for low-power and lossy

networks,” Internet Eng. Task Force, Fremont, CA, USA, RFC 6550,

2012.

[13] A. M. Efendi, A. F. P. Negara, O. S. Kyo, and D. Choi, “A design of

6LoWPAN routing protocol border router with multi-uplink interface:

Ethernet and Wi-Fi,” Adv. Sci. Lett., vol. 20, no. 1, pp. 56–60, 2014.

[14] N. Kushalnagar, G. Montenegro, and C. Schumacher, “IPv6 over

low-power wireless personal area networks (6LoWPANs): Overview,

assumptions, problem statement, and goals,” Internet Eng. Task Force,

Fremont, CA, USA, RFC 4919, 2007.

[15] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler,

“Transmission of IPv6 packets over IEEE 802.15.4 networks,” Internet

Eng. Task Force, Fremont, CA, USA, RFC 4944, 2007.

[16] Z. Shelby, K. Hartke, and C. Bormann, “The constrained application

protocol (CoAP),” Internet Eng. Task Force, Fremont, CA, USA, RFC

7959, 2016.

[17] M. Masirap, M. H. Amaran, Y. M. Yussoff, R. Ab Rahman, and

H. Hashim, “Evaluation of reliable UDP-based transport protocols for

Internet of Things (IoT),” in Proc. IEEE Symp. Comput. Appl. Ind.

Electron. (ISCAIE), 2016, pp. 200–205.

[18] G. A. Akpakwu, G. P. Hancke, and A. M. Abu-Mahfouz, “CACC:

Context-aware congestion control approach for lightweight COAP/UDPbased Internet of Things traffic,” Trans. Emerg. Telecommun. Technol.,

vol. 31, no. 2, 2020, Art. no. e3822.

[19] E. Rescorla and N. Modadugu, “Datagram transport layer security version 1.2,” Internet Eng. Task Force, Fremont, CA, USA, RFC 6347,

2012.

[20] S. Gusmeroli, S. Piccione, and D. Rotondi, “A capability-based security

approach to manage access control in the Internet of Things,” Math.

Comput. Model., vol. 58, no. 5, pp. 1189–1205, 2013.

[21] J. L. Hernandez-Ramos, A. J. Jara, L. Marın, and A. F. Skarmeta,

“Distributed capability-based access control for the Internet of Things,”

J. Internet Services Inf. Security (JISIS), vol. 3, nos. 3–4, pp. 1–16,

2013.

[22] H. Kim, “Protection against packet fragmentation attacks at 6LoWPAN

adaptation layer,” in Proc. Int. Conf. Converg. Hybrid Inf. Technol., 2008,

pp. 796–801.

[23] M. Hossain, Y. Karim, and R. Hasan, “SecuPAN: A security scheme to mitigate fragmentation-based network attacks in

6LoWPAN,” in Proc. CODASPY, 2018, pp. 307–318. [Online].

Available: https://doi.org/10.1145/3176258.3176326

[24] Re-Mote. (2017). Z1 6LoWPAN IoT Device. [Online]. Available:

http://zolertia.io/z1

[25] O. Bergmann. (Feb. 15, 2013). Tinydtls. [Online]. Available:

http://tinydtls.sourceforge.net/Visited

[26] Contiki-CoAP. (2017). Contiki CoAP Library. [Online]. Available:

https://github.com/contiki-os/contiki/tree/master/apps/er-coap

[27] Contiki. (2016). Contiki OS: An Open Source Operating System for the

Internet of Things. [Online]. Available: http://www.contiki-os.org/

[28] R. Hummen, J. H. Ziegeldorf, H. Shafagh, S. Raza, and K. Wehrle,

“Towards viable certificate-based authentication for the Internet of

Things,” in Proc. 2nd ACM Workshop Hot Topics Wireless Netw. Security

Privacy, 2013, pp. 37–42.

[29] T. Kothmayr, C. Schmitt, W. Hu, M. Brünig, and G. Carle, “DTLS based

security and two-way authentication for the Internet of Things,” Ad Hoc

Netw., vol. 11, no. 8, pp. 2710–2723, 2013.

[30] A. H. Chowdhury et al., “Route-over vs mesh-under routing in

6LoWPAN,” in Proc. Int. Conf. Wireless Commun. Mobile Comput.

Connect. World Wirelessly, 2009, pp. 1208–1212.

[31] J. Arkko, V. Devarapalli, and F. Dupont, “Using IPsec to protect mobile

IPv6 signaling between mobile nodes and home agents,” Internet Eng.

Task Force, Fremont, CA, USA, RFC 3776, 2004.

[32] S. Praptodiyono, M. I. Santoso, T. Firmansyah, A. Abdurrazaq,

I. H. Hasbullah, and A. Osman, “Enhancing IPsec performance in

mobile IPv6 using elliptic curve cryptography,” in Proc. 6th Int. Conf.

Electr. Eng. Comput. Sci. Inform. (EECSI), 2019, pp. 186–191.

[33] Weptech. (2017). 6LOWPAN IoT Gateway [Online]. Available: https://

www.weptech.de/en/6lowpan/gateway-saker.html

[34] Heatshrink. (2017). An Implementation of the LZSS Compression

Method. [Online]. Available: https://github.com/atomicobject/heatshrink

[35] RIOT. Lightweight Compression Library. Accessed: Oct. 8, 2020.

| [Online].  html#details | Available: | http://doc.riot-os.org/group\_pkg\_heatshrink. |
| --- | --- | --- |

[36] Contiki. Contiki Clock Library. Accessed: May 8, 2017. [Online].

Available: http://www.eistec.se/docs/contiki/a02184.html

[37] Contiki. (2017). Contiki APIS for Measuring Energy Consumption.

| [Online].  source.html | Available: | http://contiki.sourceforge.net/docs/2.6/a00452\_ |
| --- | --- | --- |

[38] S. Raza, D. Trabalza, and T. Voigt, “6LoWPAN compressed DTLS

for CoAP,” in Proc. IEEE 8th Int. Conf. Distrib. Comput. Sens. Syst.

(DCOSS), 2012, pp. 287–289.

[39] S. Raza, S. Duquennoy, T. Chung, D. Yazar, T. Voigt, and U. Roedig,

“Securing communication in 6LoWPAN with compressed IPsec,” in

Proc. Int. Conf. Distrib. Comput. Sens. Syst. Workshops (DCOSS), 2011,

pp. 1–8.

[40] S. Raza, H. Shafagh, K. Hewage, R. Hummen, and T. Voigt, “Lithe:

Lightweight secure CoAP for the Internet of Things,” IEEE Sensors J.,

vol. 13, no. 10, pp. 3711–3720, Oct. 2013.

[41] R. Hummen, J. Hiller, M. Henze, and K. Wehrle, “Slimfit—A HIP DEX

compression layer for the IP-based Internet of Things,” in Proc. 9th

Int. Conf. Wireless Mobile Comput. Netw. Commun. (WiMob), 2013,

pp. 259–266.

[42] C. Bormann et al., “Robust header compression (ROHC): Framework

and four profiles: RTP, UDP, ESP, and uncompressed,” Internet Eng.

Task Force, Fremont, CA, USA, Rep. RFC 3095, 2001.

[43] C. Bormann, “Guidance for light-weight implementations of the Internet

protocol suite,” Internet Eng. Task Force, Fremont, CA, USA, InternetDraft draft-bormann-lwig-guidance-01, 2013.

[44] J. Granjal, E. Monteiro, and J. S. Silva, “Enabling network-layer security

on IPv6 wireless sensor networks,” in Proc. IEEE Global Telecommun.

Conf. (GLOBECOM), 2010, pp. 1–6.

[45] J. Granjal, E. Monteiro, and J. S. Silva, “Security for the Internet of

Things: A survey of existing protocols and open research issues,” IEEE

Commun. Surveys Tuts., vol. 17, no. 3, pp. 1294–1312, 3rd Quart., 2015.

[46] D. Garcia-Carrillo and R. Marin-Lopez, “Multihop bootstrapping with

EAP through CoAP intermediaries for IoT,” IEEE Internet Things J.,

vol. 5, no. 5, pp. 4003–4017, Oct. 2018.

[47] C.-S. Park, “Security architecture for secure multicast CoAP applications,” IEEE Internet Things J., vol. 7, no. 4, pp. 3441–3452, Apr. 2020.

[48] X. Sun and N. Ansari, “Traffic load balancing among brokers at the IoT

application layer,” IEEE Trans. Netw. Service Manag., vol. 15, no. 1,

pp. 489–502, Mar. 2018.

[49] A. G. Roselin, P. Nanda, S. Nepal, X. He, and J. Wright, “Exploiting the

remote server access support of CoAP protocol,” IEEE Internet Things

J., vol. 6, no. 6, pp. 9338–9349, Dec. 2019.

[50] Fortinet. (2020). Technical Note: Using DTLS to Improve SSL

VPN Performance. [Online]. Available: https://kb.fortinet.com/kb/

documentLink.do?externalID=FD38162

[51] C. Bormann, “6LoWPAN generic compression of headers and headerlike payloads,” Internet Eng. Task Force, Fremont, CA, USA, RFC 7400,

2013.

[52] C. Bormann and Z. Shelby, “Block-wise transfersin the constrained

application protocol (CoAP),” Rep. RFC 7959, Aug. 2016. [Online].

Available: https://datatracker.ietf.org/doc/html/rfc7959