Avaliação do Impacto da Segurança sobre a Fragmentação em Redes de Sensores Sem Fio na Internet das Coisas

Francisco Ferreira de Mendonça Júnior (UFPE)

ffmj@cin.ufpe.br

Obionor de Oliveira Nóbrega (UFRPE)

obionor.nobrega@ufrpe.br

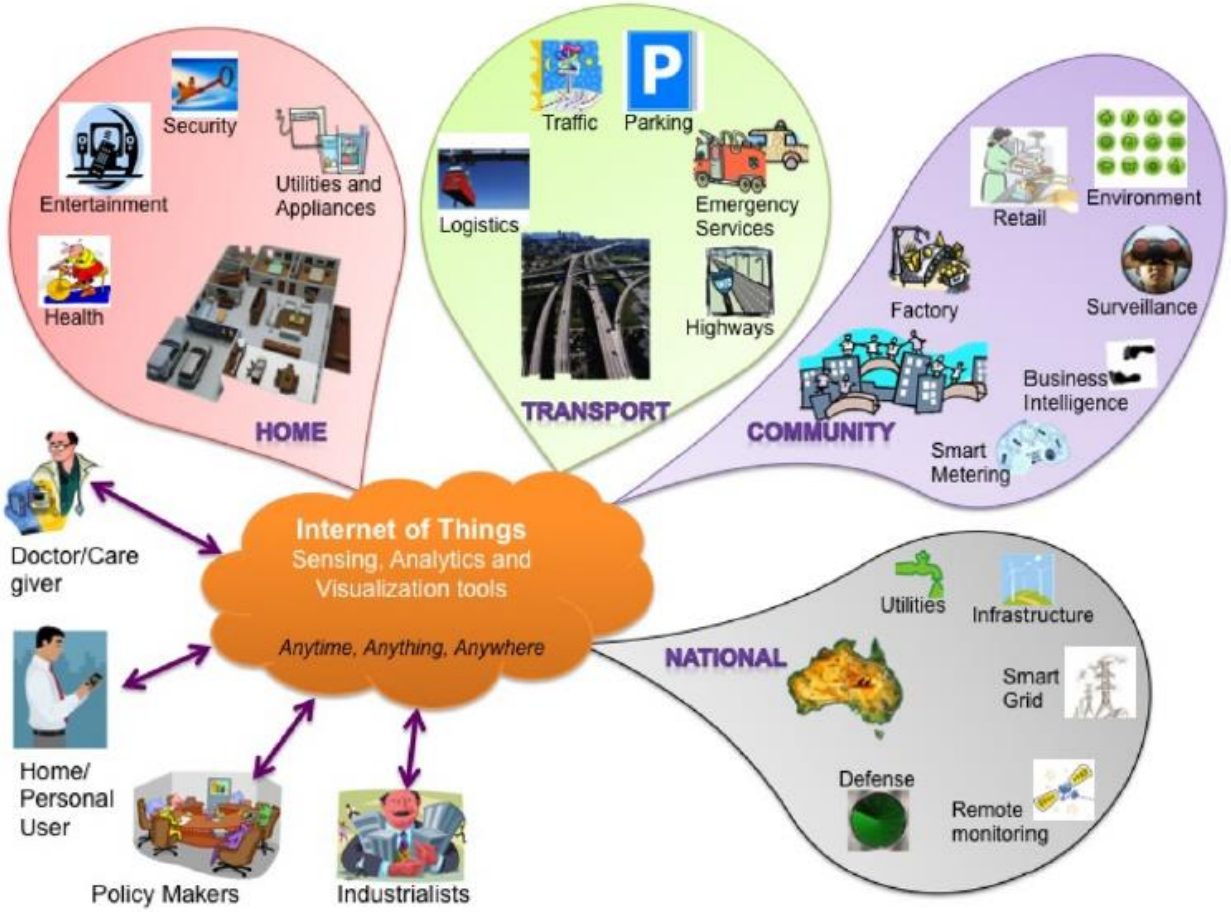
Paulo Roberto Freire Cunha (Orientador)(UFPE)

prfc@cin.ufpe.br

Estrutura

1. Motivação
    1. Internet das Coisas, Fragmentação e Segurança
2. Proposta
3. Experimento
4. Resultados e Conclusões

Internet das Coisas (Arquiteturas)



Fim a Fim

CoAP
(Aplicação)

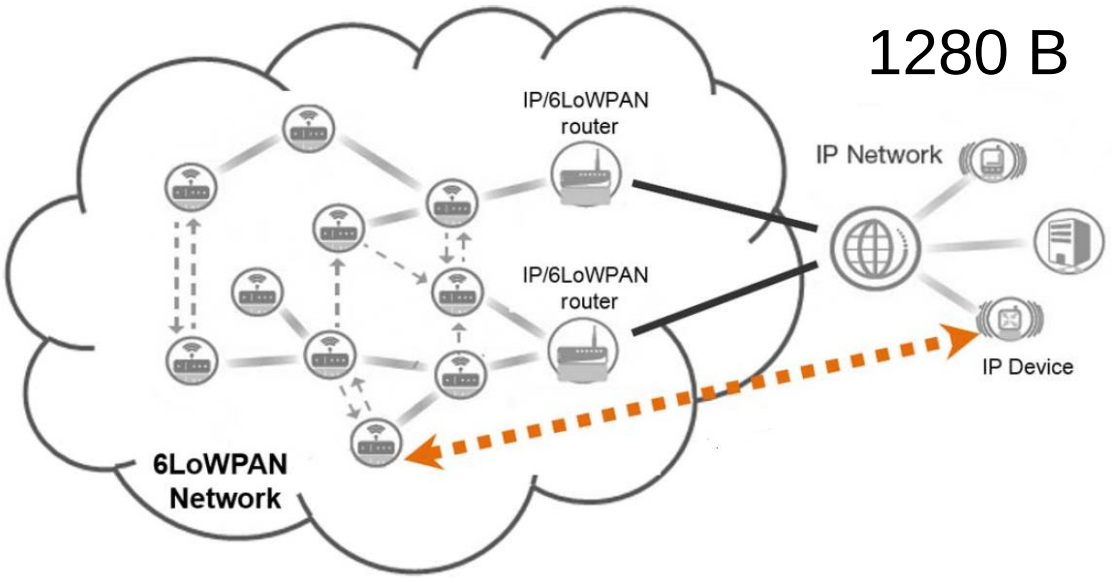
UDP
(Transporte)

IPv6
(Rede)
6loWPAN

802.15.4
(MAC e
Física)

127 B

1280 B



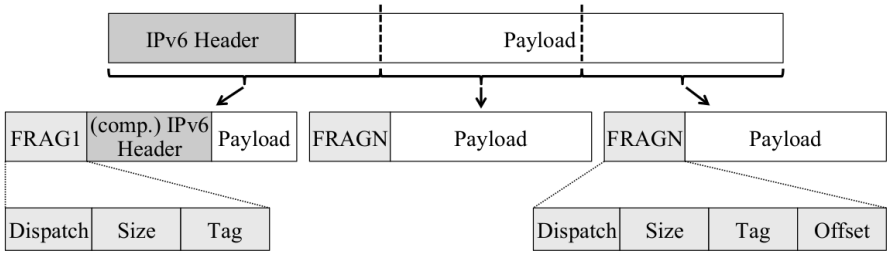
Fragmentação em 6loWPAN

Aumento na quantidade de transmissões

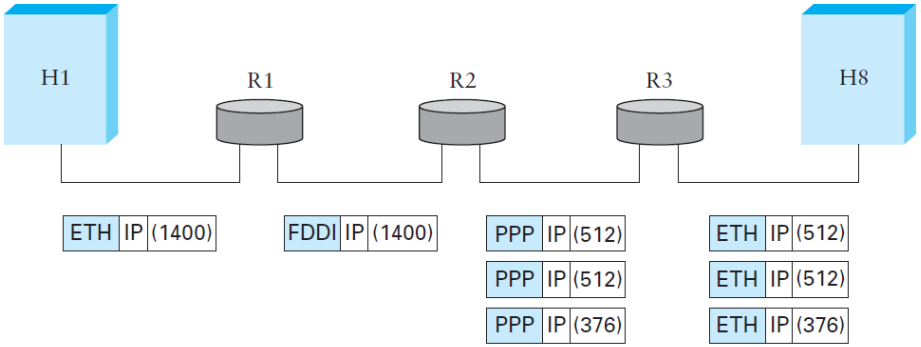
Aumento no processamento de pacotes

Probabilidade de perda

Retransmissão



[Hummen et al. 2013]



[Peterson and Davie 2007]

Segurança no padrão 802.15.4

Security Level	Description	Dados Criptografados	Proteção de Integridade e Autenticidade	Security Overhead (bytes)
0	Unsecure			0
1	AES-CBC-MAC-32		X	4
2	AES-CBC-MAC-64		X	8
3	AES-CBC-MAC-128		X	16
4	AES-CTR	X		5
5	AES-CCM-32	X	X	9
6	AES-CCM-64	X	X	13
7	AES-CCM-128	X	X	21

Segurança (Autenticidade)

					PORCENTAGEM DO QUADRO
CABEÇALHO	F		CARGA ÚTIL 95 Bytes	CRC	75%
CABEÇALHO	F	NÍVEL 5	CARGA ÚTIL 87 Bytes	CRC	69%
CABEÇALHO	F	NÍVEL 7	CARGA ÚTIL 75 Bytes	CRC	59%

REDUÇÃO

Revisão de Literatura (Fragmentação)

	[Harvan and Schönwälder 2008]	[Cody-Kenny et al. 2008]	[Pope and Simon 2013]
Descrição	RTT em ICMP de 100 bytes a 1280 bytes	Atraso e perdas em ICMP	16, 36 e 64 dispositivos
Pontos Negativos	1 sensor	4 sensores	2 fragmentos

Revisão de Literatura (Impacto da Fragmentação)

	[Kuryla and Schönwälder 2011]	**[Raza et al. 2013]**	**[Ludovic, 2014]**	**[Rachedi et al. 2015]**
Descrição	SNMP para redes de sensores	Mensagens de negociação de DTLS	Comparação com blockwise tranfer	Segurança para determinação de rotas
Pontos Negativos	Sem proposta de redução	Sem proposta de redução	Sem proposta de redução	Sem avaliação da fragmentação

Problema de Pesquisa e Proposta

Fragmentação em 6loWPAN

- Impactos negativos no **atraso**, no processamento (consumo energético) e na perda de pacotes

Variação do nível de segurança no padrão 802.15.4

- Análise e avaliação da variação do nível de segurança por frame para a redução da fragmentação

Objetivos

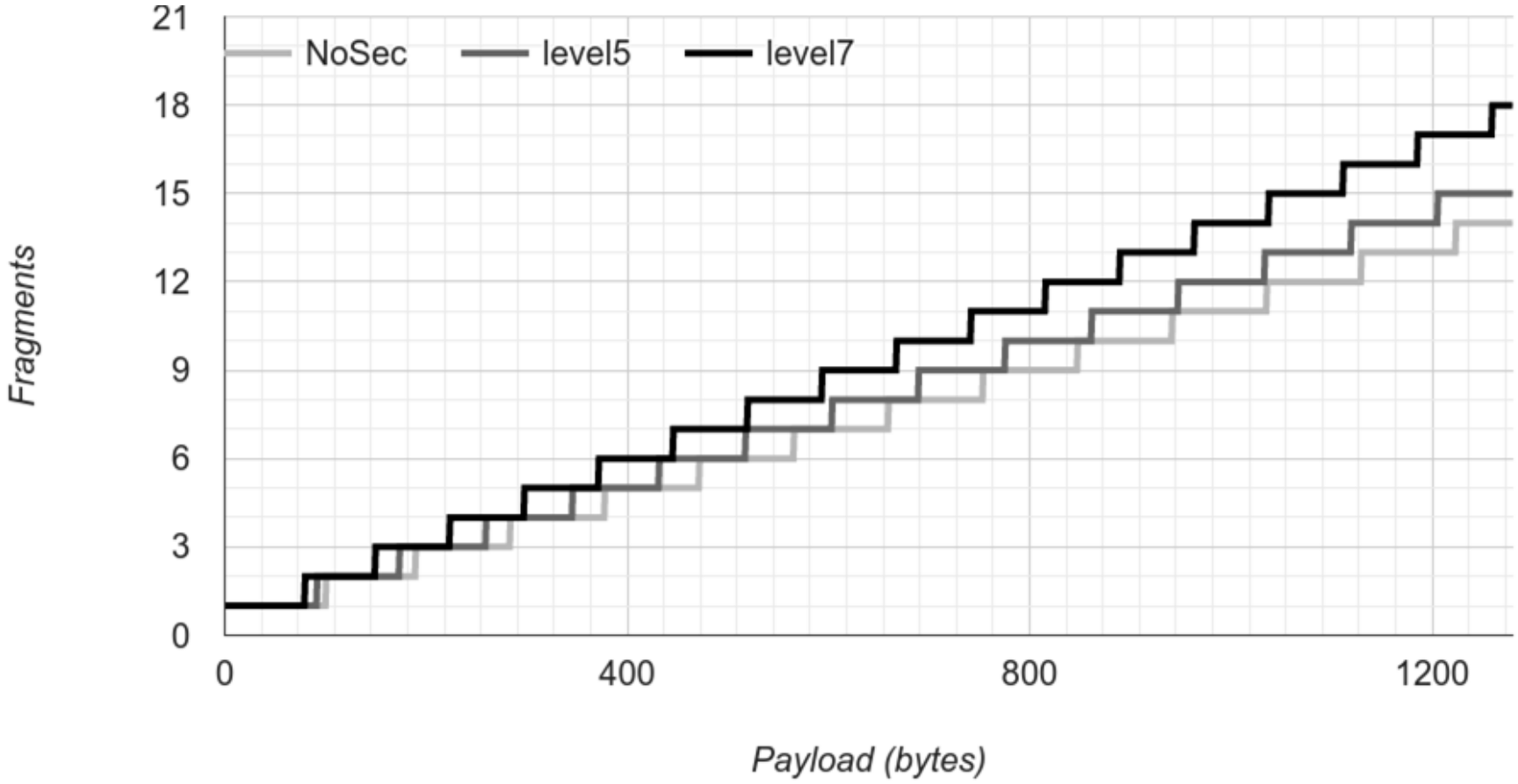
Identificação de Situações

- Identificar quantidade de dados e cenários onde a aplicação de segurança influencia na fragmentação

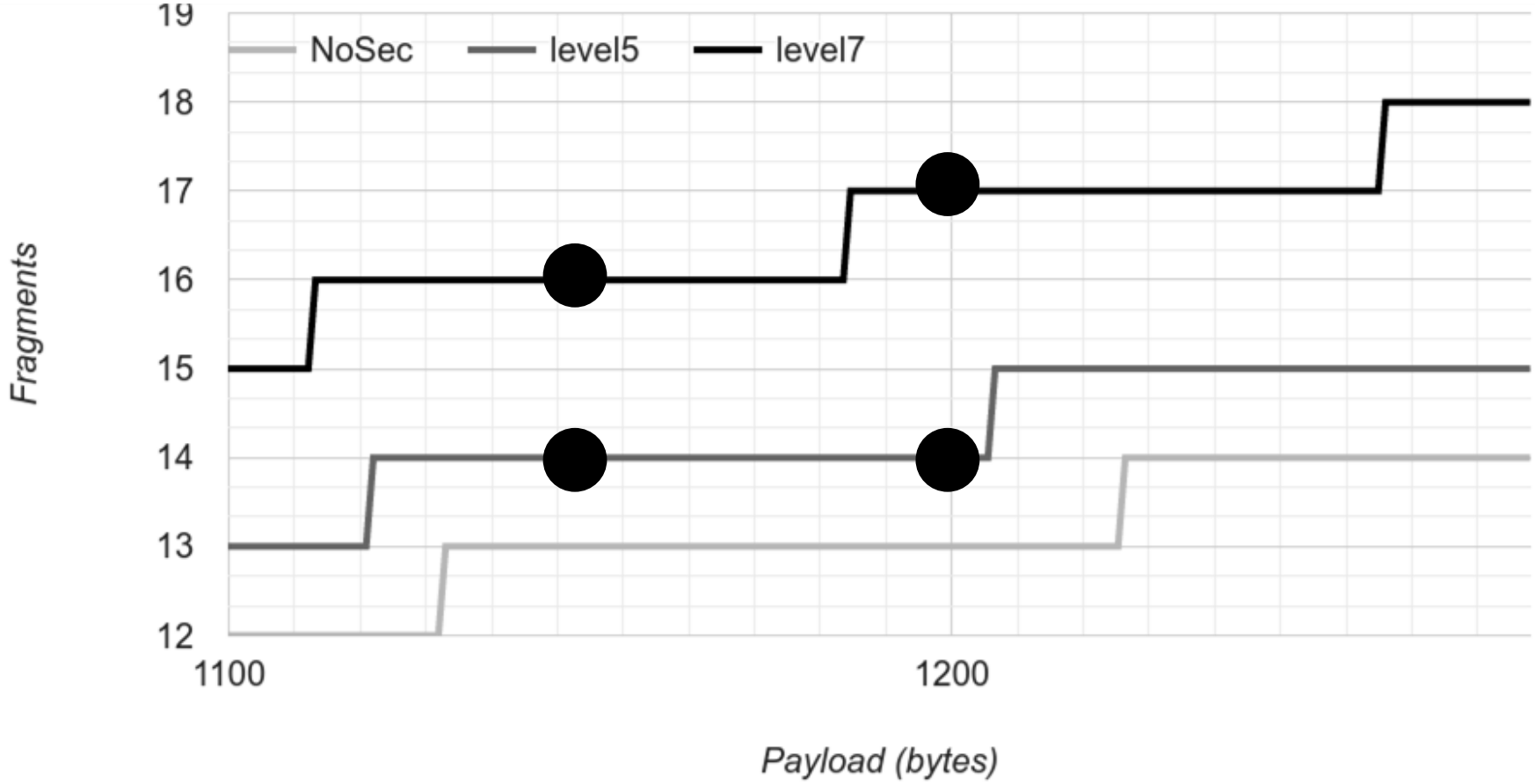
Avaliação de Benefícios

- Avaliar os benefícios da redução da fragmentação

Relação entre carga útil e fragmentos



Relação entre carga útil e fragmentos



Estimativa e Redução da quantidade de Fragmentos

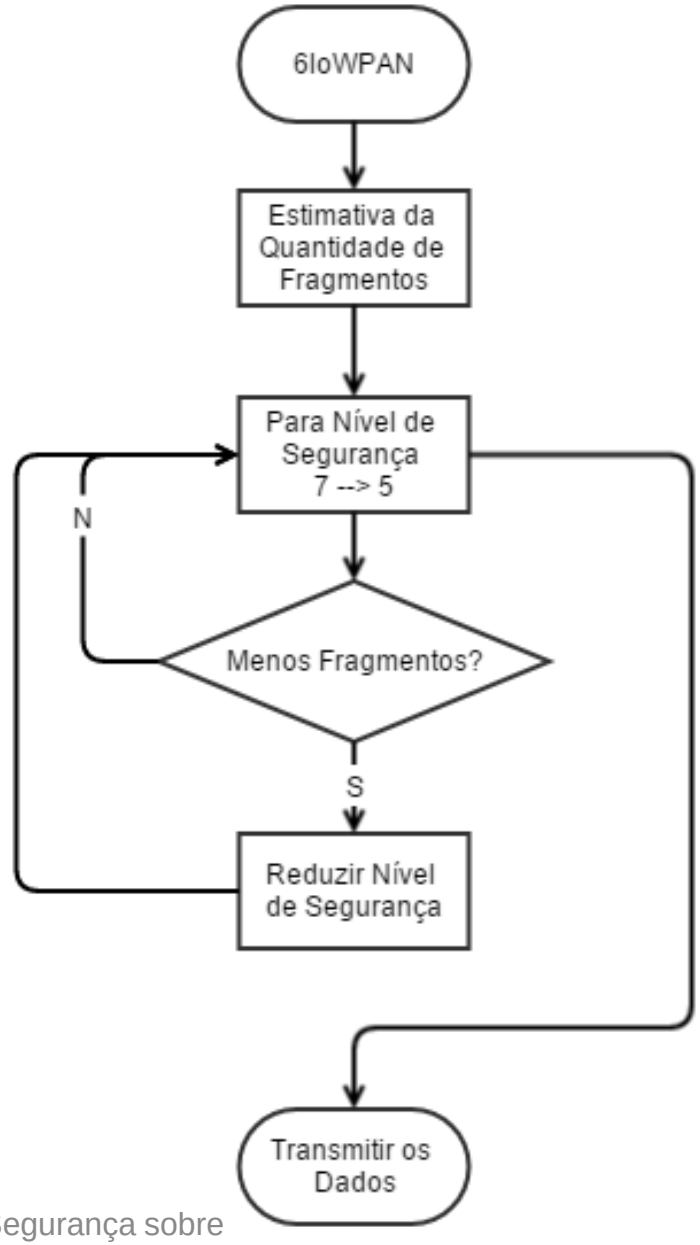
Algoritmos

Algorithm *Fragmentation Threshold Level*
Input len: Data Length

```
if len <= SicsLowOneFragLen then
    fragments = 1
else
    fragments = roundUp((len − SicsLowFrag1Len)/SicsLowFragNLen) + 1
return fragments
```

Algorithm *Thresholds*
Input $frag7$: FTL7
$frag6$: FTL6
$frag5$: FTL5

```
if frag5 < frag6 || frag6 < frag7 || frag5 < frag7 then
    decreaseSecurityLevel()
return fragments
```



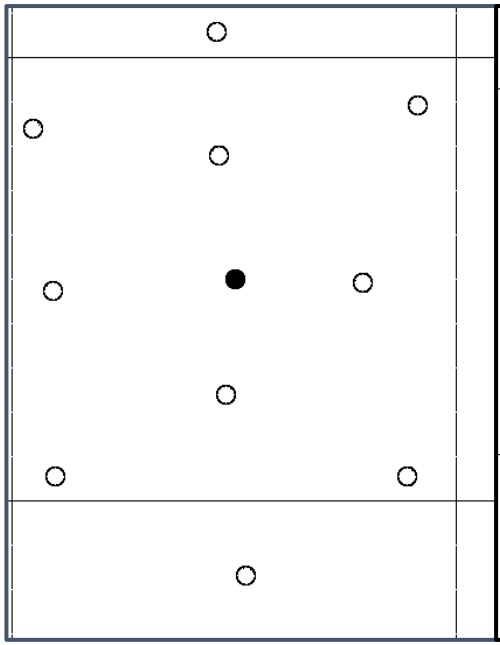
Experimento

- Simulador Cooja [Osterlind et al. 2006]
- Tempo de criptografia desprezível [Lee et al. 2010]

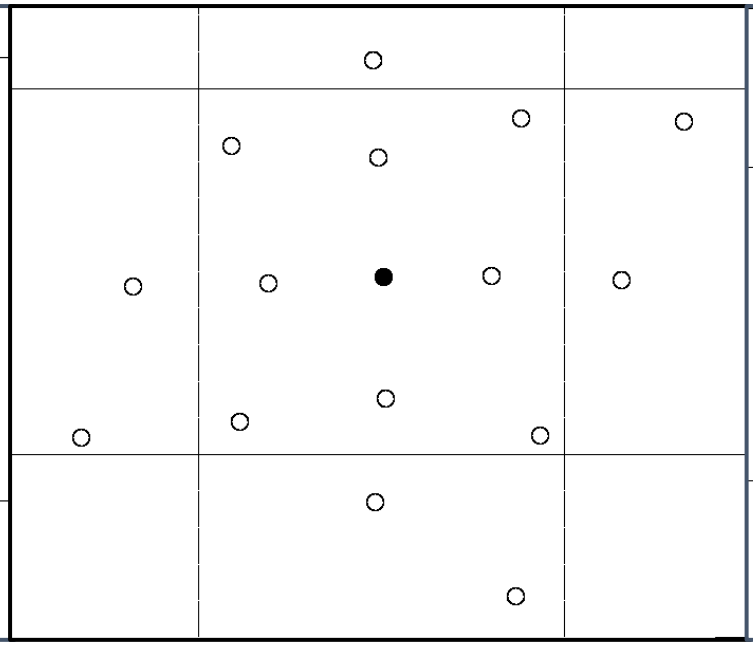
Quantidade de Dispositivos	Taxa de Transmissão (mpm)	Carga Útil		Fragmentos
		Nv5	Nv7	
11	1	69		1
16	5	148	71	2
21	10	264	148	3
		313	264	4
		375	313	5
			375	6

Cenários

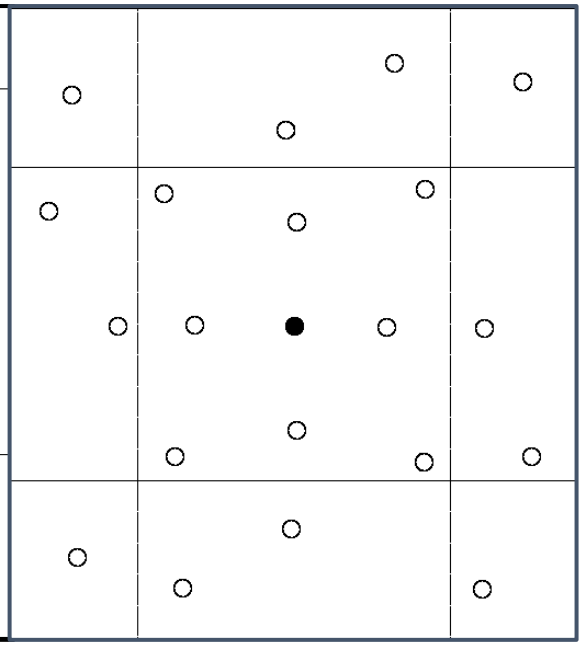
10 dispositivos



15 dispositivos



20 dispositivos

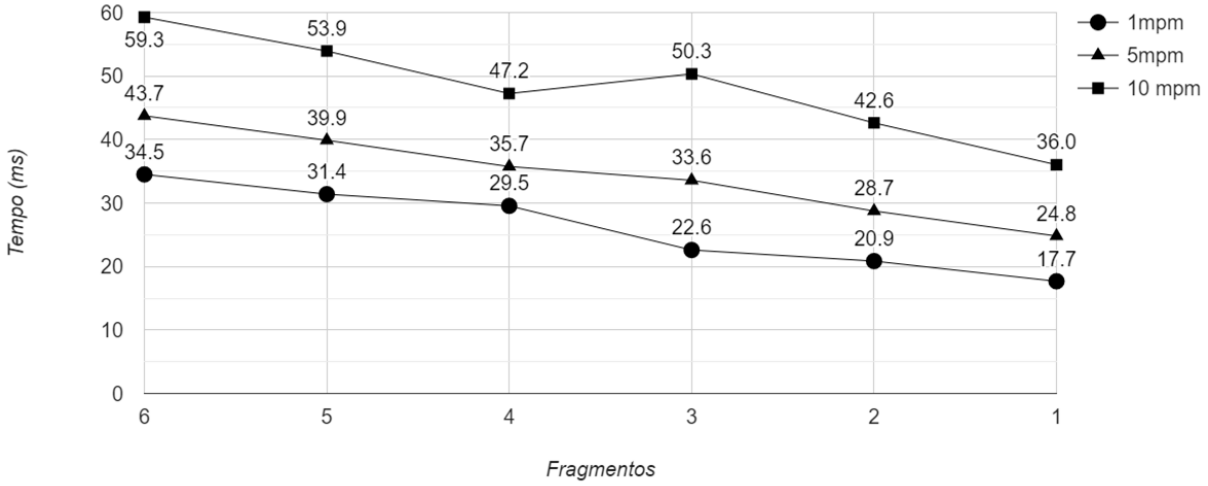


[Ludovic et. al. 2014

Experimento

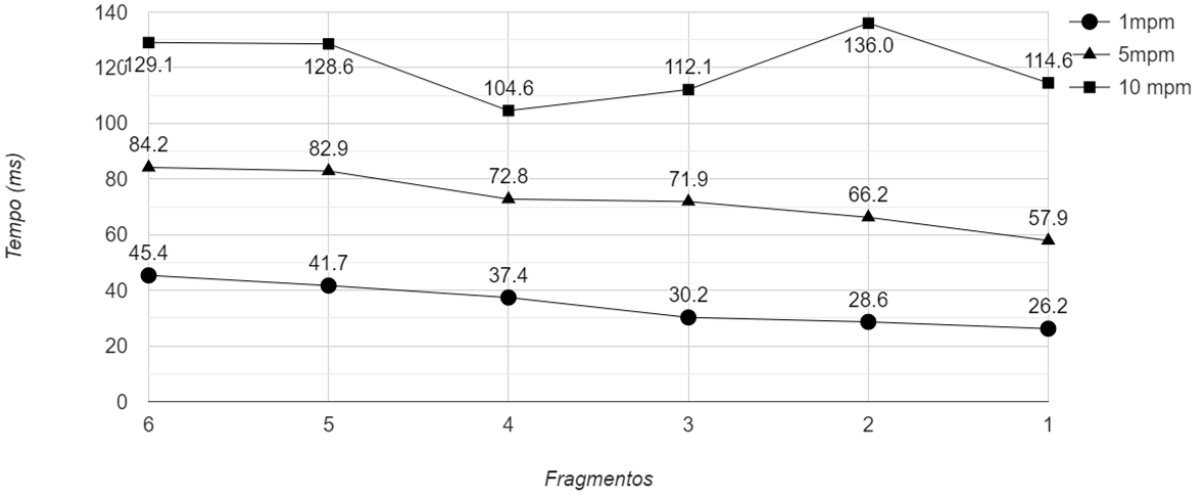
- Fatorial completo
  - 3 redes * 3 taxas * 6 fragmentos = 54 experimentos
  - 10 repetições cada = 540 experimentos
- Estatística
  - Cada repetição gera uma média
  - Amostras de 10 médias são comparadas
  - Estatística para a diferença entre amostras 90% de confiança

10 dispositivos



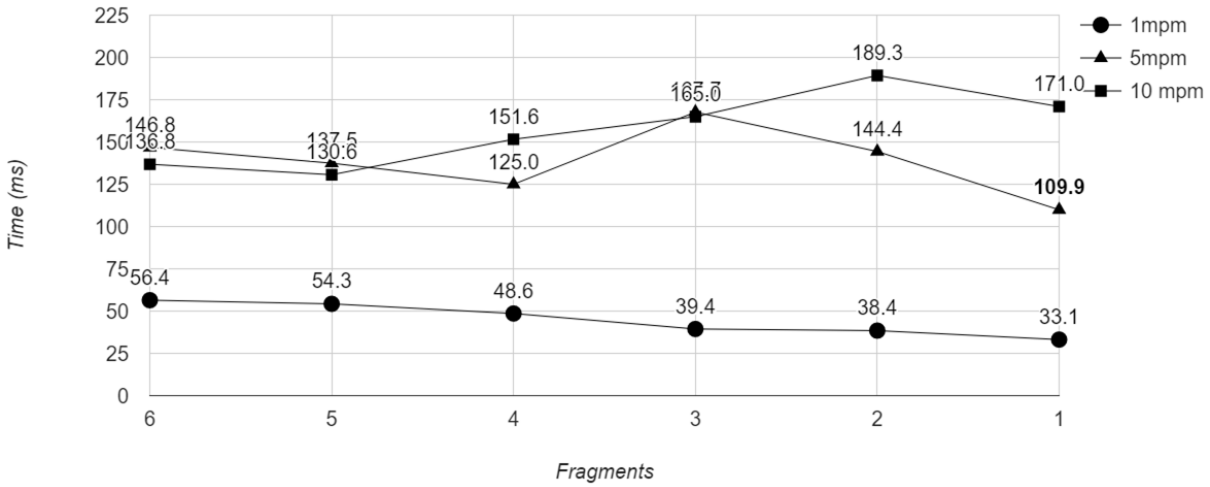
Redução de fragmentos	1 mpm	5 mpm	10 mpm
2 para 1	15%	14%	15%
3 para 2	8%	14%	15%
4 para 3	24%	6%	-7%
5 para 4	6%	10%	12%
6 para 5	9%	9%	9%

15 dispositivos



Redução de fragmentos	1 mpm	5 mpm	10 mpm
2 para 1	9%	13%	16%
3 para 2	5%	8%	-21%
4 para 3	19%	1%	-7%
5 para 4	10%	12%	19%
6 para 5	8%	2%	0%

20 dispositivos



Redução de fragmentos	1 mpm	5 mpm	10 mpm
2 para 1	14%	24%	10%
3 para 2	2%	14%	-15%
4 para 3	19%	-34%	-9%
5 para 4	11%	9%	-16%
6 para 5	4%	6%	5%

Conclusões

- Existem casos em que ocorrem reduções de até 20% no atraso
- Em redes de 15 e 20 dispositivos os ganhos são significativos enquanto a taxa de transmissão de mensagens não ultrapassa 5 mpm

Trabalhos Futuros

- Propor outras técnicas que utilizem a flexibilidade existente na subcamada de segurança do padrão 802.15.4 para economizar energia e diminuir o atraso no envio das mensagens
- Podem ser investigados mais cenários, além das analisados, onde ganhos são expressivos
- Podem ser estudados os casos em que a criptografia é realizada por software

Avaliação do Impacto da Segurança sobre a Fragmentação em Redes de Sensores Sem Fio na Internet das Coisas

Francisco Ferreira de Mendonça Júnior (UFPE)

ffmj@cin.ufpe.br

Obionor de Oliveira Nóbrega (UFRPE)

obionor.nobrega@ufrpe.br

Paulo Roberto Freire Cunha (UFPE)

prfc@cin.ufpe.br

Referências →

Referências

- Bormann, C., & Shelby, Z. (2015). Blockwise Transfers in CoAP draft-ietf-core-block-18. Avaiable online: http://tools. ietf. org/html/draft-ietf-core-block-18 (accessed on 25 nov 2015).
- Cody-Kenny, B., Guerin, D., Ennis, D., Simon Carbajo, R., Huggard, M., & Mc Goldrick, C. (2009, October). Performance evaluation of the 6LoWPAN protocol on MICAz and TelosB motes. In Proceedings of the 4th ACM workshop on Performance monitoring and measurement of heterogeneous wireless and wired networks (pp. 25-30). ACM.
- Deering, S. E. Hinden, R (1998). Internet protocol, version 6 (IPv6) specification. (No. RFC 2460).
- Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7), 1645-1660.
- Harvan, M., & Schönwälder, J. (2008). TinyOS Motes on the Internet: IPv6 over 802.15. 4 (6LoWPAN). PIK-Praxis der Informationsverarbeitung und Kommunikation, 31(4), 244-251.
- Hinden, R., & Deering, S. (1995). Internet protocol, version 6 (IPv6) specification.
- Hummen, R., Hiller, J., Wirtz, H., Henze, M., Shafagh, H., & Wehrle, K. (2013, April). “6LoWPAN fragmentation attacks and mitigation mechanisms”. In Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks (pp. 55-66). ACM.

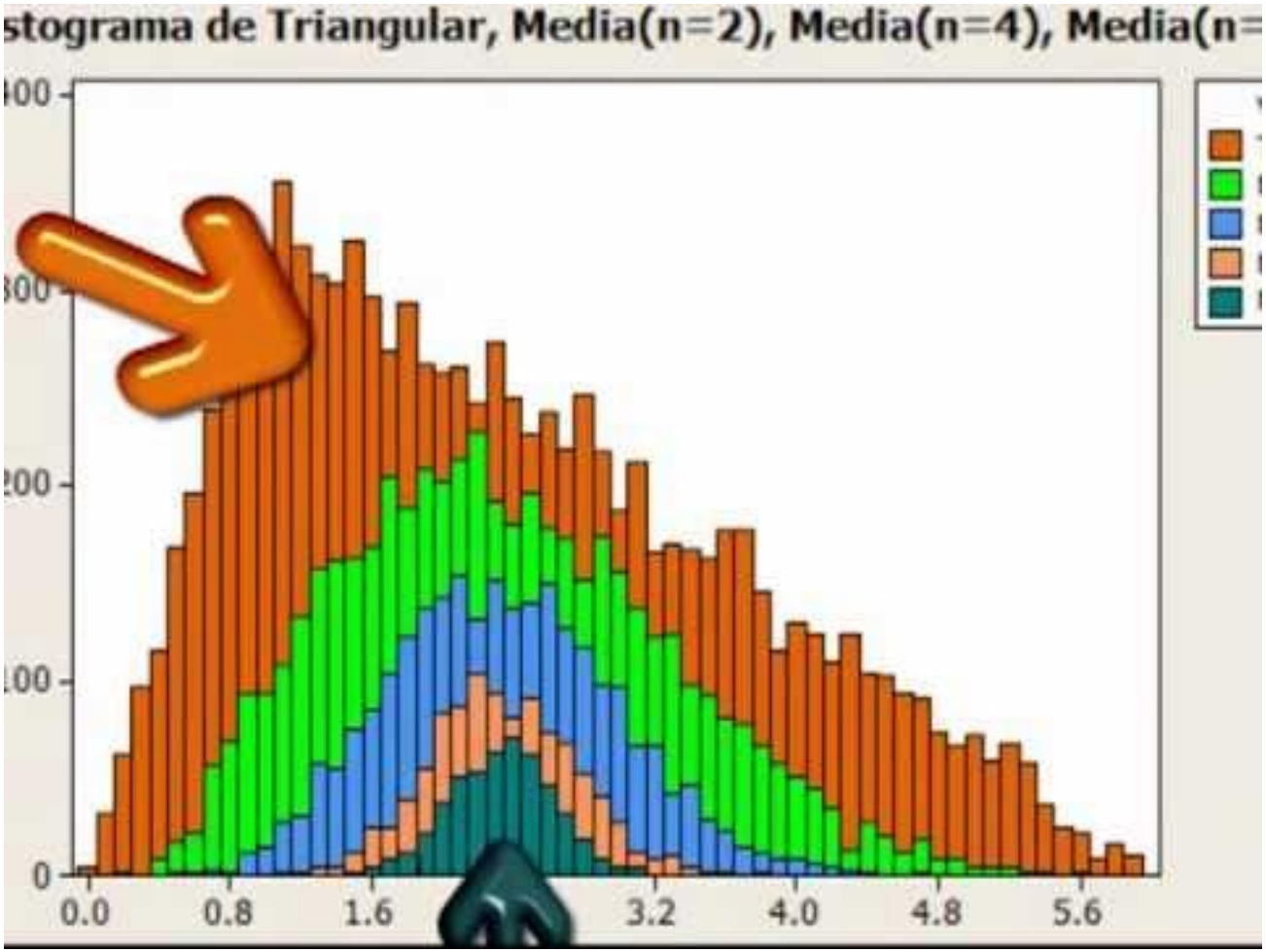
- Keoh, S. L., Kumar, S. S., & Tschofenig, H. (2014). Securing the internet of things: A standardization perspective. Internet of Things Journal, IEEE, 1(3), 265-275.
- Kuryla, S., & Schönwälder, J. (2011). Evaluation of the resource requirements of snmp agents on constrained devices. In Managing the Dynamics of Networks and Services (pp. 100-111). Springer Berlin Heidelberg.
- Kushalnagar, N., Montenegro, G., & Schumacher, C. (2007). IPv6 over low-power wireless personal area networks (6LoWPANs): overview, assumptions, problem statement, and goals (No. RFC 4919).
- Lee, J., Kapitanova, K., & Son, S. H. (2010). The price of security in wireless sensor networks. Computer Networks, 54(17), 2967-2978.
- Ludovici, A., Marco, P. D., Calveras, A., & Johansson, K. H. (2014). Analytical model of large data transactions in CoAP networks. Sensors, 14(8), 15610-15638.
- Montenegro, G., Kushalnagar, N., Hui, J., & Culler, D. (2007). Transmission of IPv6 packets over IEEE 802.15. 4 networks (No. RFC 4944).
- Osterlind, F., Dunkels, A., Eriksson, J., Finne, N., & Voigt, T. (2006, November). Cross-level sensor network simulation with cooja. In Local Computer Networks, Proceedings 2006 31st IEEE Conference on (pp. 641-648). IEEE.
- Pope, J., & Simon, R. (2013). The Impact of Packet Fragmentation and Reassembly in Resource Constrained Wireless Networks. CIT. Journal of Computing and Information Technology, 21(2), 97-107.

- Rachedi, A., & Hasnaoui, A. (2015). Advanced quality of services with security integration in wireless sensor networks. Wireless Communications and Mobile Computing, 15(6), 1106-1116.
- Raza, S., Duquennoy, S., Höglund, J., Roedig, U., & Voigt, T. (2012). Secure communication for the Internet of Things—a comparison of link layer security and IPsec for 6LoWPAN. Security and Communication Networks.
- Raza, S., Shafagh, H., Hewage, K., Hummen, R., & Voigt, T. (2013). Lithe: Lightweight secure CoAP for the internet of things. Sensors Journal, IEEE, 13(10), 3711-3720.
- Sastry, N., & Wagner, D. (2004, October). Security considerations for IEEE 802.15. 4 networks. In Proceedings of the 3rd ACM workshop on Wireless security (pp. 32-42). ACM.
- Shelby, Z., Chakrabarti, S., Nordmark, E., & Bormann, C. (2012). Neighbor discovery optimization for IPv6 over low-power wireless personal area networks (6LoWPANs) (No. RFC 6775).
- Silva, R., Silva, J. S., & Boavida, F. (2009). Evaluating 6LoWPAN implementations in WSNs. Proceedings of 9th Conferncia sobre Redes de Computadores Oeiras, Portugal, 21.
- Suh, C., Mir, Z. H., & Ko, Y. B. (2008). Design and implementation of enhanced IEEE 802.15. 4 for supporting multimedia service in Wireless Sensor Networks. Computer Networks, 52(13), 2568-2581.
- Xiao, Y., Chen, H. H., Sun, B., Wang, R., & Sethi, S. (2006). MAC security and security overhead analysis in the IEEE 802.15. 4 wireless sensor networks. EURASIP Journal on Wireless Communications and Networking, 2006(2), 81-81.
- Yick, J., Mukherjee, B., & Ghosal, D. (2008). Wireless sensor network survey. Computer networks, 52(12), 2292-2330.

Valores para as variáveis do Algoritmo 1 de acordo com o nível de segurança

	SicsLowOneFragLen	SicsLowFrag1Len	SicsLowFragNLen
Level 5	91	87	86
Level 6	87	83	82
Level 7	79	75	74

Diferença entre amostras



Taxonomia

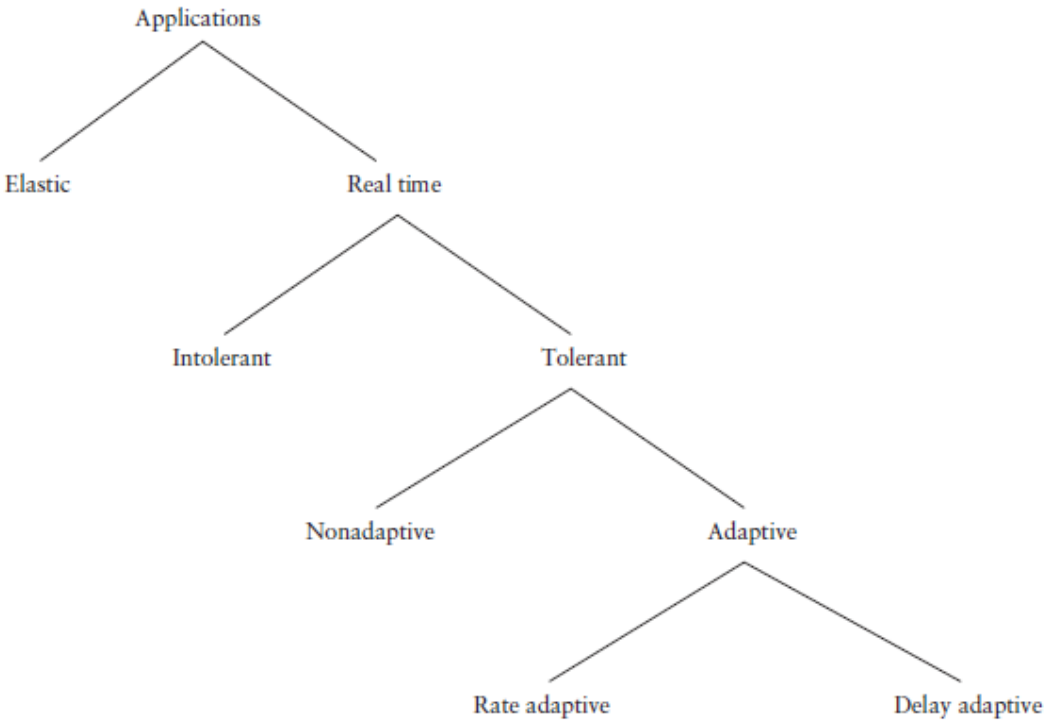
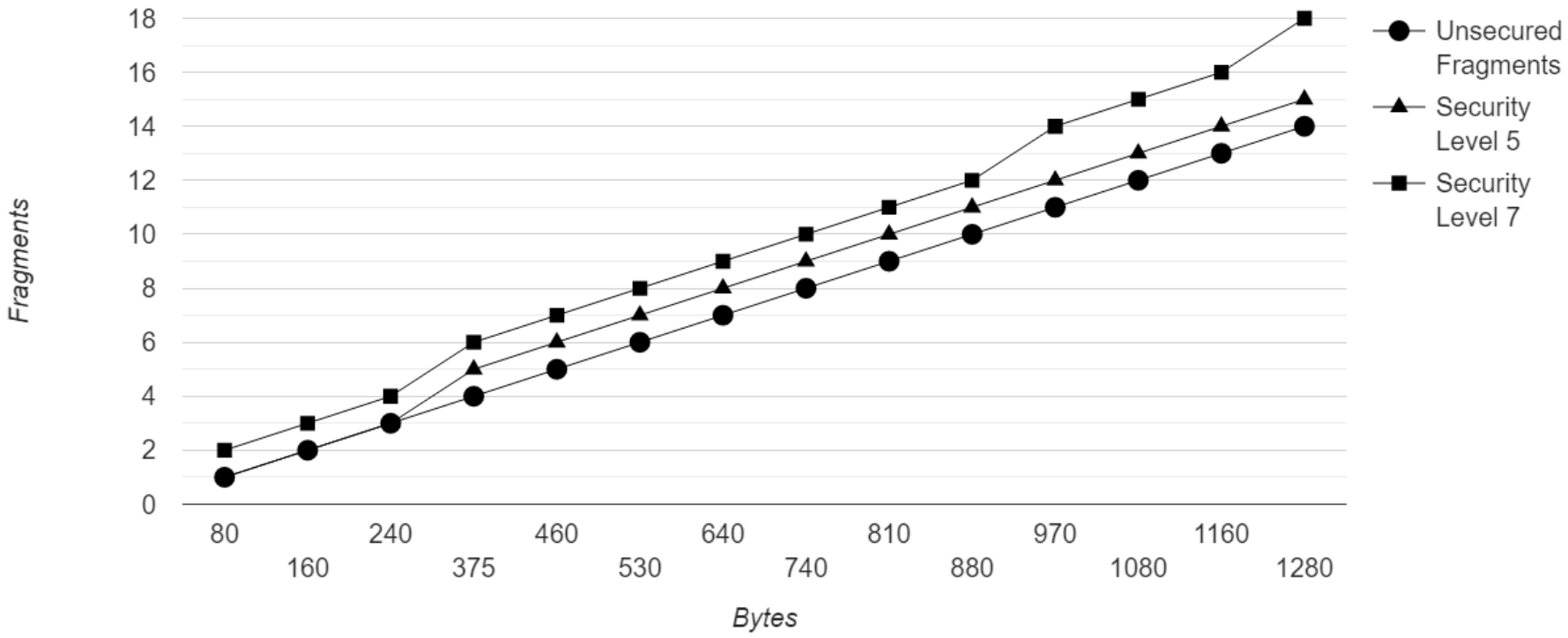


Figure 6.23 Taxonomy of applications.

[Peterson and Davie 2007]

Relação entre carga útil e fragmentos



Identificação da quantidade de fragmentos de acordo com a nível de segurança

Algorithm *Fragmentation Threshold Level*
Input len: Data Length

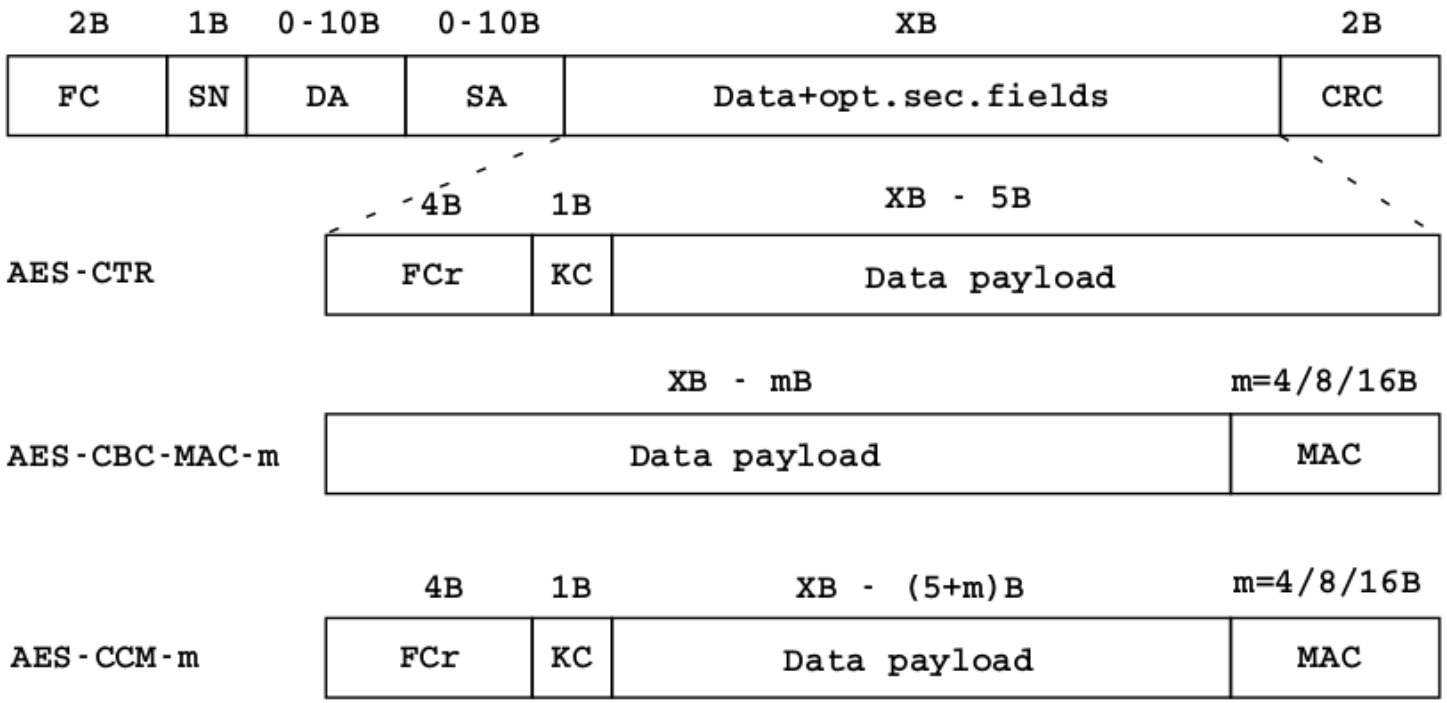
```
if len <= SicsLowOneFragLen then
    fragments = 1
else
    fragments = roundUp((len − SicsLowFrag1Len)/SicsLowFragNLen) + 1
return fragments
```

Redução da quantidade de fragmentos

Algorithm *Thresholds*
Input $frag7$: FTL7
$frag6$: FTL6
$frag5$: FTL5

```
1 if frag5 < frag6 || frag6 < frag7 || frag5 < frag7 then
2     decreaseSecurityLevel()
3 return fragments
```

Segurança



FC: Frame Control
SN: Sequence Number
DA: Destination Address
SA: Source Address

FCr: Frame Counter
KC: Key Control
MAC: Message Authentication Code

[Raza et al. 2012]

Para cada nível de segurança

- A quantidade de dados disponível quando o dado não é fragmentado
  - SicsLowOneFragLen
- A quantidade de dados disponível quando o dado é fragmentado
  - SicsLowFrag1Len
  - SicsLowFragNLen

Superframe

- Aplicações com quantidade de dados bem definidos
- Pode apresentar problemas se houverem muitos saltos