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

Francisco Ferreira de Mendonça Júnior[1], **Obionor de Oliveira Nóbrega**[2], **Paulo Roberto Freire Cunha**[1]

[1] Centro de Informática - Universidade Federal de Pernambuco (UFPE)
CEP: 50740-540 – Recife – PE – Brasil

[2] Departamento de Estatística e Informática – Universidade Federal Rural de Pernambuco (UFRPE)
Recife – PE – Brasil

{ffmj, prfc}@cin.ufpe.br, obionor.nobrega@ufrpe.br

Abstract: *On the Internet of Things, devices with limitations in computational and network resources are connected directly to the Internet. In some scenarios, these devices need to exchange data whose length exceeds the amount of available space on its frames, causing fragmentation, which adversely impacts the performance and lifetime of these networks. This paper presents an analysis of the impact of fragmentation in the delivery delay of messages in a unicast transmission scenario in a 6LoWPAN network. The reduction in the transmission of one fragment of each device can cause reductions of 20% in the delay. The variation of the security level is considered feasible to reduce fragmentation.*

Resumo: *Na Internet das Coisas, dispositivos com limitações de recursos computacionais e de rede estão conectados diretamente à Internet. Em alguns cenários, essas redes precisam trafegar dados cujo comprimento excede a carga útil disponível nos quadros em sua camada de enlace. Isso causa fragmentação, que impacta negativamente em seu desempenho e tempo de vida. Este trabalho apresenta uma análise do impacto da fragmentação no atraso de entrega de mensagens num cenário de transmissão unicast numa rede 6LoWPAN. A manipulação do nível de segurança é utilizada para controlar a fragmentação. A redução de um fragmento na transmissão de cada dispositivo pode causar reduções de até 20% no atraso.*

1. Introdução

A Internet das Coisas tem surgido como um dos paradigmas que serve de base para a evolução da Internet do Futuro [Gubbi et al. 2013]. Trata-se da conexão de objetos à Internet através de sensores, atuadores e tecnologias sem fio. A adoção do IPv6 permite que cada objeto seja endereçado individualmente, tornando possível que eles se comuniquem e troquem dados mesmo sem a intervenção humana.

A conexão de objetos à Internet passa pela consolidação das Redes de Sensores e Atuadores sem Fio (RSASF) e das tecnologias de conexão dessas redes com a Internet. Geralmente a conexão com a Internet é realizada através de *Gateways*, dispositivos responsáveis por coletar e armazenar dados dos sensores de uma RSASF e transmiti-los quando necessário. [Rachedi et al. 2015] [Yick et al. 2008]

Nos últimos anos surgiram iniciativas que pretendem mudar o paradigma de conectividade das RSASF para que os dispositivos conectem-se à Internet sem intermediários. A subcamada 6LoWPAN (*IPv6 over Low power Wireless Personal Area Networks)* provê conectividade com a Internet para dispositivos que tenham camada de acesso ao meio e camada física diferenciadas. A adaptação consiste em tradução de endereços, compressão de cabeçalhos e tratamento de fragmentação [Montenegro et al. 2007]. A função do *gateway* foi substituída pela presença do *6LoWPAN Border Router* (6LBR), que já não armazena dados dos sensores, mas direciona as requisições e o envio de dados diretamente para os dispositivos. Dispositivos das RSASF passam a ser chamados de *6LoWPAN nodes* (6LN). [Shelby et al. 2012]

Quando conectadas à Internet, as redes 6LoWPAN entram em contato com redes com características diferenciadas, abrindo novos campos para o estudo de seu funcionamento. Uma das diferenças está relacionada à quantidade e ao tamanho dos dados trafegados. A unidade máxima de transmissão do IPv6 é de 1280 bytes [Deering and Hinden 1998]. Quando pacotes assim precisam trafegar por redes 6LoWPAN, eles passam por um processo de fragmentação.

Redes 6LoWPAN geralmente apresentam tráfego de dados, como sinalização e controle, que não excedem o espaço disponível em seus quadros [Kushalnagar et al. 2007]. Mas existem tipos de redes que precisam enviar registros de várias medições que não cabem em um único quadro. Esses registros podem variar de centenas de bytes a kilobytes . Alguns exemplos mostrados se referem ao monitoramento de ferrovias, cujos dados podem alcançam 7 KB; algumas aplicações de monitoramento de saúde podem alcanças 512 KB; e aplicações de monitoramento de vulcões podem alcançar 256 bytes. [Ludovici et al. 2014].

A fragmentação causa impactos negativos no desempenho, no consumo energético e pode causar perda de pacotes. Reduzir a fragmentação permite economizar os recursos escassos das redes 6LoWPAN [Hummen et al. 2013], [Silva et al. 2009], [Pope and Simon 2013], [Kuryla and Schönwälder 2011], [Ludovic, 2014], [Suh et al. 2008]. Este trabalho apresenta uma análise da variação do nível de segurança e sua relação com a fragmentação. Busca-se analisar em quais situações a variação do nível de segurança reduz a fragmentação. São propostos algoritmos que identificam essas situações utilizando apenas tecnologias de comunicação e segurança já padronizadas. Além disso, são analisados cenários onde a relação entre a quantidade de dispositivos, a quantidade de fragmentos e a modalidade de envio de mensagens constituem um ambiente mais amplo que os cenários comumente encontrados na literatura.

A próxima seção apresenta algumas características do padrão 802.15.4 com foco nos mecanismos de fragmentação e segurança. Na seção 3 serão discutidos trabalhos que tratam sobre fragmentação, suas falhas e as relações com o presente trabalho. Na seção 4 é feita uma análise da relação entre fragmentação e segurança. Busca-se investigar situações onde a redução do nível de segurança reduz a fragmentação, principalmente através da apresentação de equações que ajudam a identificar essas situações. Nas seções 5 e 6 se discute, através de um experimento e da apresentação dos resultados, a análise do impacto de fragmentação quando causada pela aplicação de segurança. Na seção 7 são apresentadas considerações finais e propostas para trabalhos futuros.

2. Padrão 802.15.4 – Fragmentação e Segurança

O padrão IEEE 802.15.4 especifica as camadas MAC e física para redes pessoais de baixa taxa de transferência (*Low Rate Wireless Personal Area Networks*, LR-WPAN) de. O foco da especificação foi manter simplicidade de implementação, baixo custo e baixo consumo energético [Daidone et al 2014]. Essas características permitiam uma ampla adoção do padrão pela comunidade de RSSF. [Sastry et al. 2004]

O padrão prevê 3 tipos de camada física que funcionam nas frequências 868 MHz (mega-hertz) , 915 MHz ou 2.4 GHz (giga-hertz). É possível alcançar velocidades de 20 kbps (kilobits por segundo), 40 kbps e 250 kbps, respectivamente, em cada frequência de operação. Independente da frequência de operação, a camada MAC utiliza o mesmo formato de quadro. Esse quadro possui, no máximo, 127 bytes [Callaway et al 2002]. As características diferenciadas de largura de banda e de formato de quadros fazem com que o padrão 802.15.4 necessite da subcamada 6loWPAN para se conectar à Internet.

2.1. Fragmentação em Redes 802.15.4

Quando um dado vindo da subcamada 6loWPAN não couber em apenas um quadro 802.15.4, ele deve ser fragmentado. Para isso é adicionado um cabeçalho auxiliar de fragmentação. Qualquer mecanismo de segurança, quando houver, é aplicado após o processo de fragmentação. [Raza et al. 2012][Montenegro et al. 2007]

O cabeçalho auxiliar de fragmentação varia de acordo com a quantidade de fragmentos. O primeiro fragmento recebe um cabeçalho auxiliar composto por 4 octetos. Esses octetos são divididos entre um preâmbulo de 5 bits, o campo "*datagram_size*" e o campo "*datagram_tag*". O cabeçalho auxiliar do primeiro fragmento pode ser visto na figura 1(a). A partir do segundo fragmento, o cabeçalho auxiliar ganha o campo "*datagram_offset*". O formato do cabeçalho auxiliar dos fragmentos subsequentes pode ser visto na figura 1(b). [Montenegro et al. 2007]

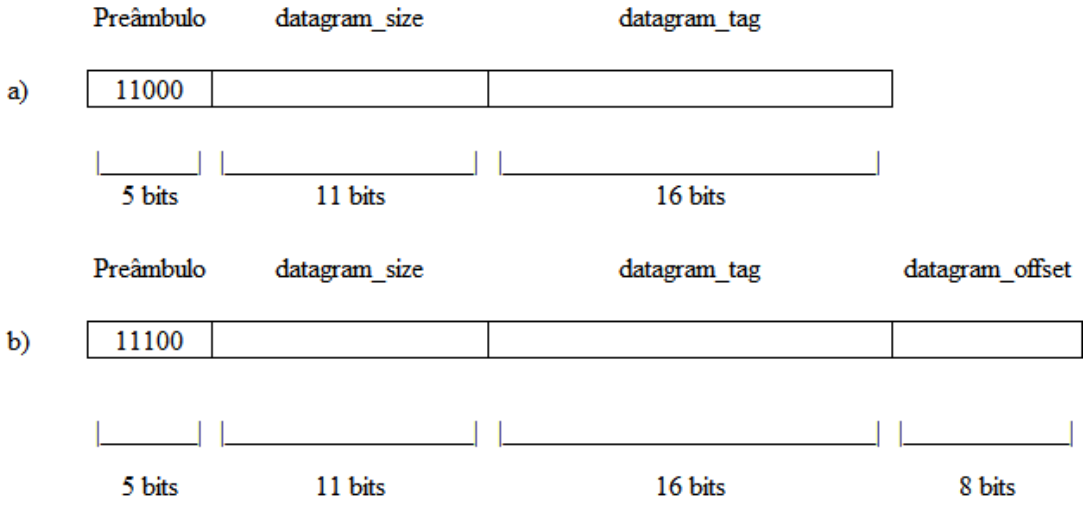


Figura 1: Formato dos cabeçalhos auxiliares de fragmentação para o primeiro fragmento (a) e para os demais fragmentos (b)

O preâmbulo identifica se aquele é o primeiro fragmento, chamado de FRAG1, ou algum fragmento subsequente, chamado de FRAGN. O campo "datagram_size" contém o comprimento do pacote completo, antes da fragmentação. Seu valor é comum

a todos os fragmentos, pois pode auxiliar na alocação de buffer caso os fragmentos cheguem fora de ordem. O campo "*datagram_tag*" contém um valor que identifica se um fragmento pertence a um determinado pacote. Esse valor é incrementado a cada novo pacote que necessita de fragmentação. O valor do campo "*datagram_offset*" indica o deslocamento de cada fragmento subsequente em relação ao primeiro fragmento. Ele permite que o pacote seja remontado de forma correta.

Redes 6LoWPAN são propensas a perdas e esses defeitos são agravados pela presença da fragmentação. O principal impacto para a transmissão de dados é que a fragmentação muda a modalidade de envio de mensagens. Geralmente, a taxa de geração de mensagens em uma rede é modelada por uma distribuição Poisson. Na presença de fragmentação, a rede se torna congestionada, uma vez que se considera que os fragmentos são transmitidos em rajadas [Pope and Simon 2013][Ludovic, 2014].

2.2. Segurança em Redes 802.15.4

Os mecanismos e opções de segurança no padrão 802.15.4 são conhecidos como a "subcamada de segurança" [Daidone et. al. 2014]. O padrão 802.15.4 prevê três modos de segurança: Modo Inseguro, Modo de ACL e o Modo Seguro. O Modo Inseguro não proporciona nenhuma proteção para os quadros transmitidos. No Modo de ACL (*Access Control List*), um dispositivo pode se comunicar apenas com dispositivos que estejam em uma lista pré-configurada. Quadros recebidos de outros dispositivos são descartados. Esse modo não fornece nenhuma garantia de confidencialidade, integridade ou proteção contra reenvio [Xiao et al. 2006].

O Modo Seguro prevê a utilização de 8 níveis de segurança para a camada de enlace e física. Os níveis podem ser vistos na Tabela 1. Esses níveis podem prover segurança nula, proteção de integridade, confidencialidade, ou proteção de integridade e confidencialidade combinadas. Existe também proteção contra reenvio de mensagens. [Xiao et al. 2006][Sastry et al. 2004]

Tabela 1. Níveis de segurança no padrão 802.15.4

Nível de Segurança	Descrição	Dados Criptografados	Proteção de Integridade e Autenticidade	Sobrecarga de segurança (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

O nível zero não prevê nenhuma proteção para as mensagens. A proteção de integridade é fornecida pela cifra AES-CBC-MAC-X. O X corresponde a extensão do Código de Integridade de Mensagem (*Message Integrity Code,* MIC). Essas mensagens não são criptografadas. Essa cifra protege a mensagem e seu cabeçalho com um código de integridade, que é calculado por blocos. O MIC é adicionado ao final da carga útil. [Sastry et al. 2004][Xiao et al. 2006]

A confidencialidade é provida pelas cifras AES-CTR e AES-CCM-X. A cifra AES-CTR protege os dados utilizando AES sobre blocos de dados. Para isso um dado é dividido em blocos de 16 Bytes. Cada bloco usa um contador diferente durante o processo de criptografia. O contador faz parte do Vetor de Inicialização (*Initialization Vector, IV*), também conhecido como *nonce*. O IV é formado pela conjunção de alguns campos como um marcador estático e o endereço do emissor. Também é formado por três contadores: o contador de quadros (4 Bytes), contador de chave (1 Byte) e o contador para os blocos (2 Bytes). O emissor inclui o contador de quadros e o contador de chave na carga útil do quadro [Sastry et al. 2004][Xiao et al. 2006]. Existem recomendações para a não utilização da cifra AES-CTR de forma isolada. A cifra não oferece proteção de integridade e de proteção contra reenvio de mensagens. [Sastry et al. 2004][Raza et al. 2012]

A cifra AES-CCM provê confidencialidade e proteção de integridade. Trata-se da aplicação dos dois mecanismos escritos anteriormente. Inicialmente é aplicado a proteção de integridade, que adiciona o MIC ao fim da carga útil. Em seguida, o processo de criptografia é aplicado sobre a carga útil e o MIC. O processo de criptografia adiciona os contadores à carga útil. Na figura 2 vemos o formato dos cabeçalhos e rodapés adicionais requeridos com a aplicação de segurança na camada física do padrão 802.15.4.

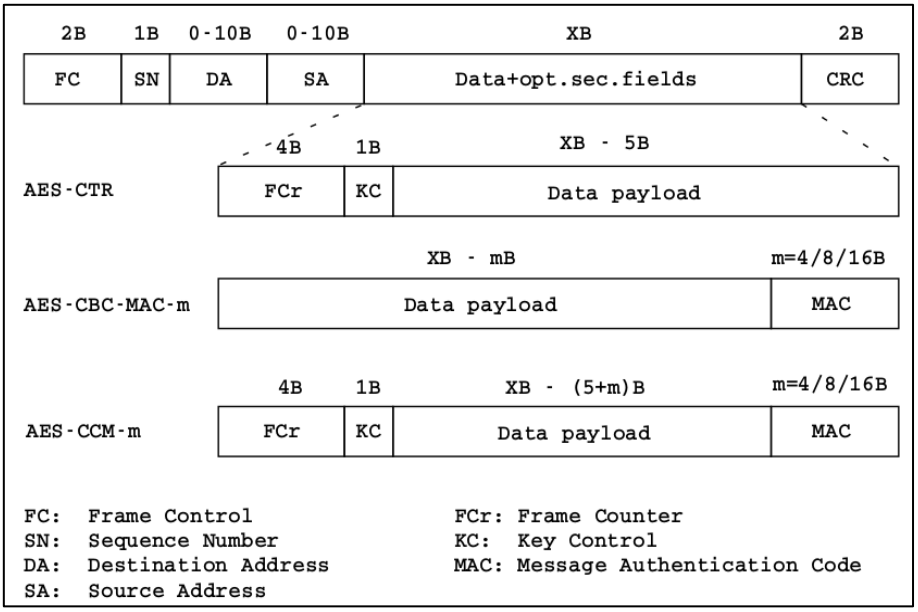


Figura 2: Formato do *quadro* do padrão 802.15.4 e sua relação com a segurança [Raza et al. 2012]

3. Trabalhos Relacionados

A preocupação com a fragmentação está presente desde o desenvolvimento das RSASF. Esse problema voltou à discussão quando se tornou necessário conectar esses dispositivos diretamente à Internet. Procura-se, desde então, propor mecanismos e melhorias nos mecanismos existentes para lidar com esse problema [Montenegro et al. 2007][Bormann and Shelby 2015]. Existem buscas de métodos para eliminar ou atenuar os efeitos da fragmentação, como pode ser visto em [Keoh et al. 2014]. Essa nova conectividade faz dispositivos das redes 6LoWPAN, cuja unidade máxima de

transmissão é 127 bytes, terem que lidar com o troca de dados diretamente com a Internet usando IPv6, cujo MTU (*Maximum Transmission Unity*) é de 1280 bytes [Hinden and Deering 1995].

Desde [Harvan and Schönwälder 2008] e [Cody-Kenny et al. 2008] até [Ludovici et al. 2014] essa preocupação com a fragmentação é constante. O trabalho de [Harvan and Schönwälder 2008] apresenta uma das primeiras análises do impacto da fragmentação em dispositivos limitados. Seus resultados apontam um crescimento no *round-trip time* usando ICMP (*Internet Control Message Protocol*) com mensagens *echo* que vão de 100 bytes a 1280 bytes. Apesar disso, seu cenário é simplificado com a presença de apenas um sensor. [Cody-Kenny et al. 2008] avaliaram o impacto no atraso e na perda de pacotes usando ICMP num *testbed* contendo 3 dispositivos e 1 estação base. Seus resultados mostraram aumento no atraso relacionado ao aumento no tamanho das mensagens. [Pope and Simon 2013] fizeram uma avaliação usando cenário com 16, 36 e 64 dispositivos, mas avaliaram apenas o processo de fragmentação até 2 fragmentos.

O estudo e correta avaliação do impacto na fragmentação não é necessário apenas em cenários de transmissão de dados. Alguns protocolos que auxiliem no gerenciamento, formação e manutenção de uma rede também podem precisar levá-la em consideração. [Kuryla and Schönwälder 2011] são levados a analisar o impacto da fragmentação no desenvolvimento de uma versão de SNMP para redes de dispositivos limitados. Algumas das mensagens trocadas pelo protocolo tinham tamanho próximo ou eram maiores que os 127 bytes permitidos no quadro do padrão 802.15.4. Essas mensagens sofriam fragmentação, e isso foi analisado para a avaliação do protocolo.

[Raza et al. 2013] preocupou-se com fragmentação no desenvolvimento de uma implementação de uma versão leve e segura do protocolo CoAP (*Constrained Application Protocol*). Métodos de compressão de mensagens de negociação do protocolo de segurança DTLS (*Datagram Transport Layer Protocol*) foram propostos. Mesmo assim, nem sempre era possível evitar fragmentação, pois algumas mensagens permaneciam com comprimento maior do que o máximo permitido.

O desenvolvimento de novos protocolos e a evolução dos antigos requer novas avaliações dos mecanismos de fragmentação existentes. O protocolo CoAP oferece a possibilidade de transferência de dados através de *blockwise transfer* [Bormann and Shelby 2015]. Trata-se de uma forma de dividir uma requisição ou uma resposta, de forma que cada parte seja transmitida como uma requisição independente nas camadas mais baixas da pilha de protocolos. Dessa forma, cada parte é transmitida e confirmada individualmente e pode ser retransmitida em caso de perda. Caso a requisição completa fosse enviada para as camadas inferiores e sofresse fragmentação, a perda de um dos fragmentos poderia gerar a retransmissão de toda a requisição. A retransmissão causa atrasos e aumento no consumo energético.

Pensando nisso, [Ludovic, 2014] realiza uma comparação entre fragmentação e *blockwise transfer*. Seus resultados apontam que a transmissão da requisição completa para que seja fragmentada na camada de rede pode ser mais eficiente que a utilização do mecanismo de *blockwise transfer*. Isso ocorre pois o CoAP demanda a troca de mais mensagens, gerando mais ocupação no canal que as confirmações da camada de rede.

[Rachedi et al. 2015] baseou-se no impacto da segurança para a construção de rotas pelo protocolo RPL em redes 6LoWPAN. Para isso ele se preocupou com o

impacto computacional de criptografar e decriptografar os dados. Esse impacto alimentava um controlador PID (*Proportional–Integral–Derivative controller*) para a construção de rotas do tipo AODV (*Ad-hoc On-demand Distance Vector*). Ainda assim não foram investigados os impactos que a fragmentação podia proporcionar, visto que a transmissão de dados acarreta a elevação do atraso e do consumo energético.

Apesar de estes trabalhos proporem melhorias, a maior parte dos cenários avaliados se constitui de cenários simplificados. As redes são formadas por poucos dispositivos. O modelo mais comum trata da avaliação utilizando apenas dois dispositivos, o que não condiz com a realidade de um cenário de Internet das Coisas. [Ludovic, 2014] realizou a avaliação em ambientes com mais dispositivos, mas não propôs mecanismos de eliminação ou atenuação dos efeitos da fragmentação.

4. Análise do Impacto da Fragmentação Causada pela Adição de Segurança

Visto que os cenários analisados na seção 3 são simplificados para o contexto da Internet das Coisas, é necessário avaliar a fragmentação em ambientes maiores e sob condições que simulem a troca de mensagens entre 6LN e a Internet. Técnicas que reduzam a fragmentação são necessárias, uma vez que seus impactos no aumento no atraso e taxa de entrega de mensagens são significativos [Harvan and Schönwälder 2008][Humenn, 2013][Pope and Simon 2013]. Serão analisadas as situações em que fragmentação pode acontecer devido à aplicação de segurança.

Esta análise é baseada na premissa de que a Qualidade de Serviço (*Quality of Service*, QoS) também é um fator importante para as aplicações de Internet das Coisas [Rachedi et al. 2015]. Estudos extensivos têm sido feitos em relação à ocupação de memória e consumo energético em RSASF [Yick et al. 2008]. Algumas métricas de QoS, como o atraso, tem sido deixadas em segundo plano em relação aos dois parâmetros citados.

É conhecido na literatura que o tamanho tem impactos no tempo de entrega das mensagens. Mesmo quando a fragmentação não é necessária, esse tempo pode variar dependendo da quantidade de mensagens, da quantidade de dispositivos na rede ou da quantidade de saltos. [Pope and Simon 2013][Rachedi et al. 2015]

Para esta análise serão utilizados apenas os níveis de segurança 5, 6 e 7, pois permitem o envio de dados criptografados e com proteção de integridade. Para que os dados sejam enviados com a máxima segurança habilitada é necessário acrescentar 21 bytes de informações de segurança em cada quadro, reduzindo a quantidade de dados que a aplicação pode enviar. Cada um dos níveis menores ocupa menos espaço por quadro.

Os limites da fragmentação correspondem à quantidade de bytes que podem ser economizados com a redução do nível de segurança. A quantidade de bytes necessários para a aplicação de cada nível está descrita na Tabela 1. À vista disso podem-se construir pseudocódigos para detectar os limites onde a redução do nível de segurança reduz o impacto da fragmentação.

No algoritmo 1, as variáveis "*SicsLowOneFragLen*", "*SicsLowFrag1Len*" e "*SicsLowFragNLen*" representam a quantidade de carga útil que um quadro pode transportar após a adição do MIC de acordo com o nível de segurança. A variável

"*SicsLowOneFragLen*" representa a carga útil de um quadro após a adição do MIC e quando não ocorre fragmentação. Essa variável representa uma quantidade maior de carga útil, pois nenhum cabeçalho de fragmentação foi adicionado.

Algoritmo 1: Algoritmo para identificação da quantidade de fragmentos de acordo com a nível de segurança

```
Algorithm Fragmentation Threshold Level
Input    len: Data Length
1 if len <= SicsLowOneFragLen then
2     fragments = 1
3 else
4     fragments = roundUp((len − SicsLowFrag1Len)/SicsLowFragNLen) + 1
5 return fragments
```

A variável "*SicsLowFrag1Len*" representa a carga útil do primeiro quadro de um dado fragmentado. Seu valor representa a quantidade de bytes disponíveis para dados após a adição do cabeçalho adicional de fragmentação e do MIC. Essa variável apresenta um valor maior que "*SicsLowFragNLen*". Isso acontece porque o cabeçalho de fragmentação nos fragmentos subsequentes é maior, reduzindo o espaço para carga útil nos fragmentos adicionais.

Os valores que podem ser atribuídos as variáveis do algoritmo 1 são relacionados com "XB", na figura 2. Esses valores são diferentes para cada nível de segurança e podem ser vistos na tabela 2. Na linha 1 do algoritmo 1, é feito o cálculo da quantidade de dados que não ativa a fragmentação. Este valor é representado pela variável "*SicsLowOneFragLen*". Valores maiores que o especificado na coluna "*SicsLowOneFragLen*" da tabela 2 provocam a fragmentação, de acordo com o nível de segurança.

Tabela 2. 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

A presença das "*SicsLowFrag1Len*" e "*SicsLowFragNLen*" na linha 3 do Algoritmo 1 é relacionada ao cabeçalho de fragmentação, que possui valores diferentes para o primeiro fragmento e para os fragmentos seguintes. No caso do nível 5, o valor 87 para "*SicsLowFrag1Len*" indica a quantidade de dados referente ao primeiro fragmento. A divisão por 86, referente à variável "*SicsLowFragNLen*", indica a quantidade de dados que os demais fragmentos podem transportar. Quanto maior o nível de segurança, menor é a quantidade de espaço disponível para dados. A mesma relação pode ser aplicada aos demais níveis de segurança.

O algoritmo 2 verifica se, para uma dada quantidade de dados, a redução no nível de segurança resultará na redução da quantidade de fragmentos. O acrônimo "FTL*" representa o "*Fragmentation Threshold Level* *", e faz referência ao algoritmo 1 quando este for alimentado com os valores da tabela 2, de acordo com o nível de segurança aplicado. No algoritmo 2, a quantidade de fragmentos resultante da aplicação de cada nível de segurança é comparada. Quando a quantidade de fragmentos for menor, para um nível menor de segurança, a redução no nível de segurança é acionada.

Algoritmo 2: Algoritmo para 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
```

Na figura 3 verifica-se o impacto do tamanho da mensagem na fragmentação quando a quantidade de dados que chega a subcamada 6LoWPAN está próxima dos limites de fragmentação. O gráfico foi aprimorado para demonstrar situações onde a redução no nível de segurança reduz a quantidade de fragmentos. Isso significa que esses pontos satisfazem as condições expostas nos algoritmos 1 e 2 para a redução da fragmentação. É possível observar que existe uma tendência a uma redução cada vez maior na quantidade de fragmentos conforme o tamanho na mensagem aumente Um mecanismo que faça utilização do nível de segurança para evitar fragmentação pode ser viável [Rachedi et al. 2015].

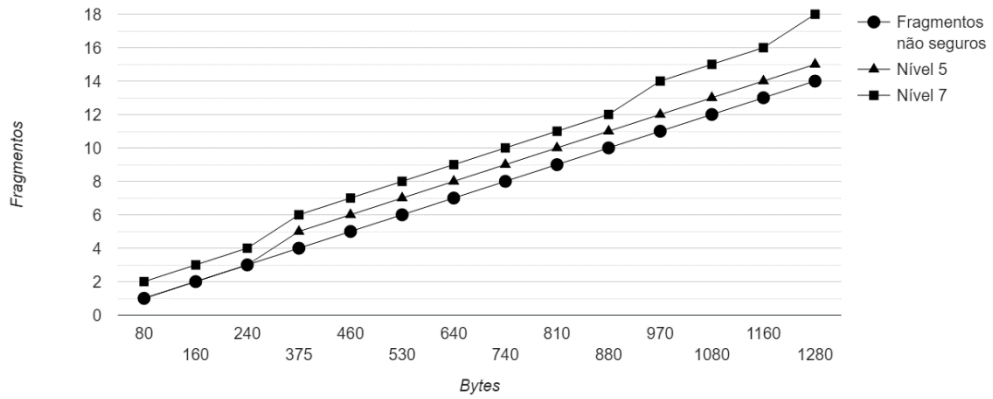


Figura 3: Aumento na quantidade de fragmentos relacionado a adição de segurança

5. Configuração do Experimento

Foram realizados experimentos para medir a economia de tempo ocasionada pela redução na quantidade de fragmentos. Os experimentos foram realizados usando ao simulador Cooja [Osterlind et al. 2006]. É possível simular dispositivos em três níveis: instruções em nível de máquina, nível de rede e sistema operacional. É possível coletar informações de cada um desses níveis.

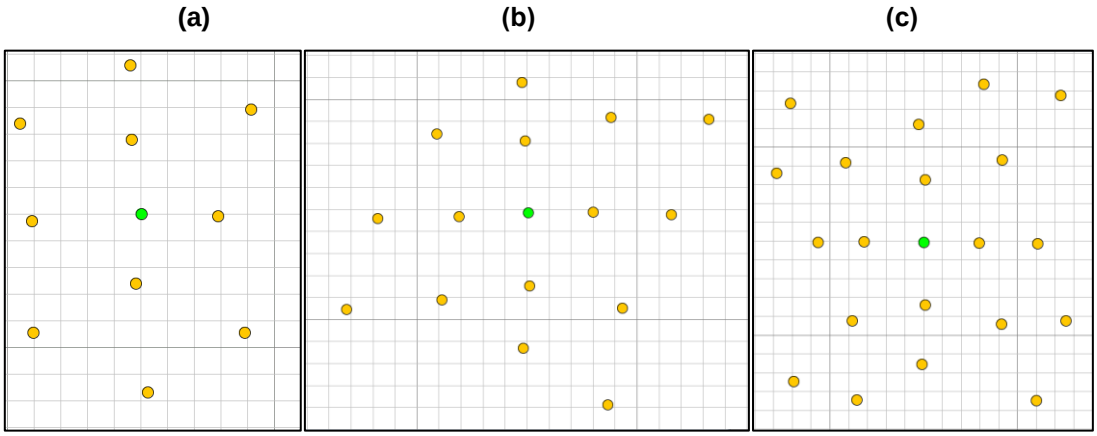
No simulador, foi configurada uma aplicação de entrega de mensagens utilizando UDP sobre 6loWPAN. Os dados são enviados a um receptor, no centro físico da rede em estrela, que emite uma mensagem na camada de aplicação quando recebe algum dado. Os experimentos foram feitos em redes de 11, 16 e 21 dispositivos [Ludovic, 2014]. Em cada rede, um dos dispositivos faz o papel de 6LBR e fica no centro da rede. Foram investigadas três taxas de envio de mensagens: 1, 5 e 10 mpm

(mensagens por minuto) [Ludovic, 2014]. O comprimento da mensagem foi controlado para simular o comportamento da manipulação de segurança sobre dados. Foi adotada a premissa de que o tempo gasto pelas operações criptográficas é desprezível quando realizado com o auxílio de aceleradores hardware [Lee et al. 2010].

Foram realizados experimentos em modelo fatorial completo para cada rede (3), cada quantidade de fragmentos (6) e cada modalidade de envio de mensagens (3), totalizando 54 tipos para simulação. Cada uma dessas simulações foi repetida por 10 vezes. Cada experimento foi executado durante 1 hora em tempo de simulação, de forma que são geradas até 13000 mensagens. O simulador gera sementes aleatórias da ordem de 19 dígitos para cada replicação. Cada experimento foi executado durante 1 hora em tempo de simulação, de forma que são geradas até 13000 mensagens.

A partir de cada uma das 10 repetições é gerada uma média. As amostras de 10 médias provenientes de simulações de quantidades de fragmentos adjacentes são comparadas. Para a comparação, são usados testes estatísticos para a diferença de duas amostras com intervalo de confiança de 90%. A hipótese alternativa do teste é que o atraso medido na rede que transmite mais fragmentos é maior que o atraso medido na rede com quantidade de fragmentos subjacente. Na figura 4 vemos os cenários da simulação para 11 dispositivos (a), 16 dispositivos (b) e 21 dispositivos (c).

Figura 4: Cenário da simulação



6. Análise dos Resultados

Pode-se observar, nos gráficos das figuras 5, 6 e 7, redução da fragmentação apresenta redução no atraso. Esses valores representam a redução no atraso médio quando o dado é enviado de um 6LN para o 6LBR. Porém, é possível observar que o aumento da quantidade de dispositivos e o aumento da quantidade de mensagens podem tornar os ganhos menos relevantes, uma vez que a rede está congestionada o tempo todo.

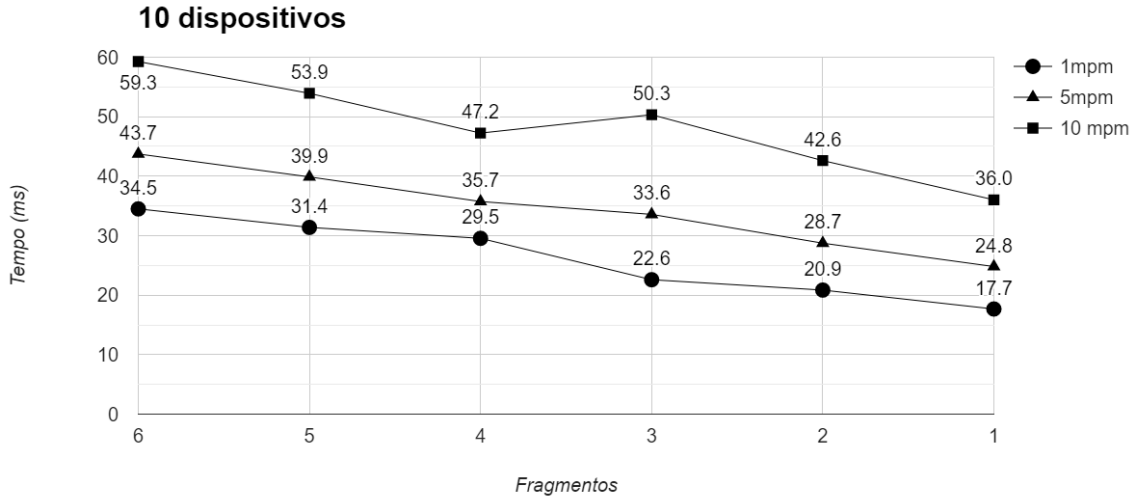


Figura 5: Redução média no atraso em redes de 10 dispositivos sob diferentes taxas de geração de dados

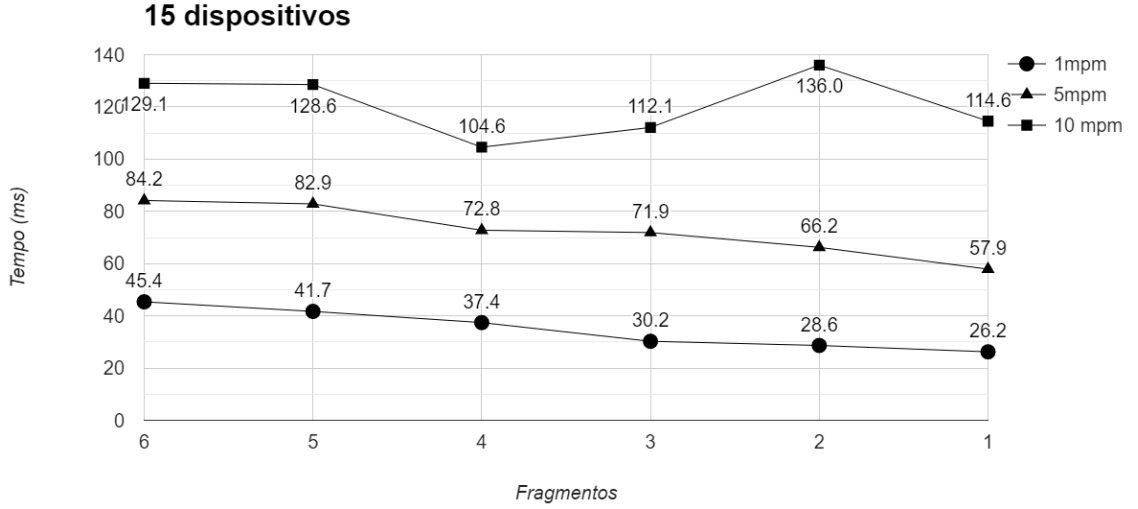


Figura 6: Redução média no atraso em redes de 15 dispositivos sob diferentes taxas de geração de dados

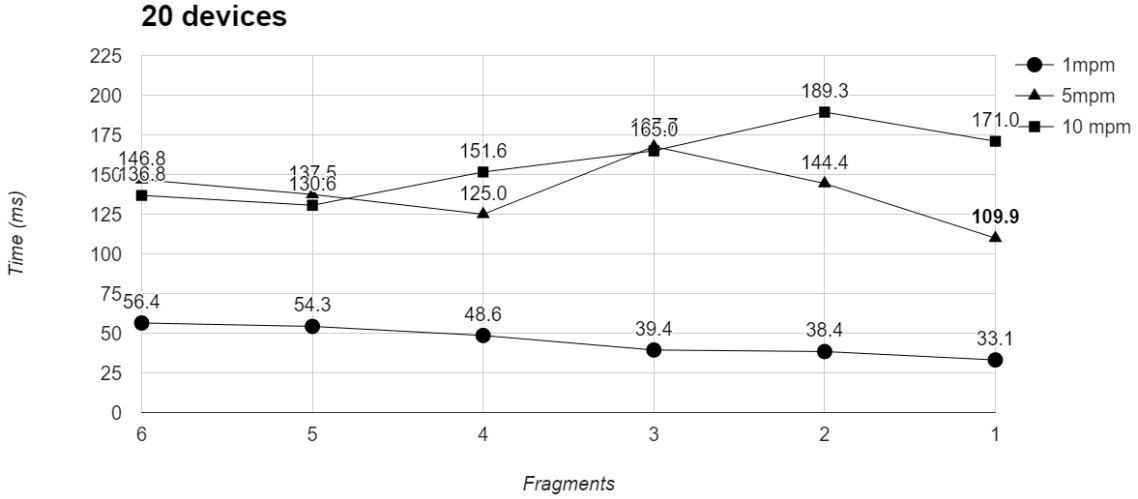


Figura 7: Redução média no atraso em redes de 10 dispositivos sob diferentes taxas de geração de dados

Na figura 5 é possível observar a redução no atraso médio da rede quando ocorre a redução de segurança na rede de 10 dispositivos. Nas modalidades de 1 mpm e 5 mpm todas as reduções apresentam ganhos significativos. Nas figuras 5, 6 e 7, no envio de 10 mpm, não existem ganhos estatisticamente significativos, apesar de existirem ganhos percentuais. Esse comportamento ocorre devido ao congestionamento da rede [Pope and Simon 2013] [Ludovic, 2014].

Redes 6LoWPAN cuja frequência de geração de dados está entre 1 e 5 mpm apresentam decréscimo significativo no atraso quando ocorre redução da fragmentação. Redes com até 10 dispositivos apresentam ganhos em todas as taxas.

Em redes com 15 e 20 dispositivos, os ganhos são expressivos quando o tráfego da rede é baixo. Nas redes com 15 dispositivos, os ganhos existem quando as mensagens são enviadas a, no máximo, 5 mpm. Até esse limite, são encontrados ganhos próximos a 20%. Nas redes de 20 dispositivos, os ganhos se concentram quando as mensagens são enviadas a 1 mpm. Quando a quantidade de mensagens aumenta, os ganhos passam a ser menos perceptíveis. Mesmo assim ainda são encontrados ganhos próximos a 20% nessas redes.

7. Considerações Finais e Trabalhos Futuros

Este trabalho avaliou as situações em que a redução do nível de segurança do padrão 802.15.4 auxilia na redução dos efeitos da fragmentação no atraso de redes 6LoWPAN. Foram propostos algoritmos para identificar essas situações e acionar a redução no nível de segurança. Foi possível analisar que existem casos em que ocorrem reduções de até 20% no atraso. As reduções ocorrem com mais significância em redes de 10 dispositivos. Em redes de 15 e 20 dispositivos os ganhos são significativos quando a taxa de transmissão de mensagens não ultrapassa 5 mpm. Conclui-se que a redução do nível de segurança é método viável para reduzir fragmentação e reduzir o atraso em redes 6LoWPAN.

Trabalhos futuros podem propor outras técnicas que utilizem a flexibilidade existente na subcamada de segurança do padrão 802.15.4, como demonstrado na seção 2.2, para economizar energia e diminuir o atraso no envio das mensagens. Podem ser

investigadas mais situações onde ganhos são expressivos. Também podem ser estudados os casos em que a criptografia é realizada por software, uma vez que parte dos rádios ainda não fornece suporte completo à criptografia realizada por hardware.

Referências

Bormann, C., & Shelby, Z. (2015). Blockwise Transfers in CoAP draft-ietf-core-block-18. Available 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.

Callaway, E., Gorday, P., Hester, L., Gutierrez, J. A., Naeve, M., Heile, B., & Bahl, V. (2002). Home networking with IEEE 802. 15. 4: a developing standard for low-rate wireless personal area networks. IEEE Communications magazine, 40(8), 70-77.

Daidone, R., Dini, G., Anastasi, G. (2014). On evaluating the performance impact of the IEEE 802.15. 4 security sub-layer. Computer Communications, 47, 65-76.

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.