Uma Proposta de Contramedida ao Ataque Jamming em Redes IEEE 802.15.4 utilizando Rádio Cognitivo

Fábio V. Almeida [1], **M. M. Bontempo** [1],
J. R. Santos [1], **Antônio M. Alberti**[1]

[1]ICT Lab - Instituto Nacional de Telecomunicações (Inatel),
CEP 37540-000 - Santa Rita do Sapucaí, Minas Gerais, Brasil.

fabio.almeida@mtel.inatel.br, mariliamartins@gee.inatel.br,

joserodrigo@gec.inatel.br, alberti@inatel.br

Abstract. *Wireless sensor networks use shared media for data transmission, making it easy for an attacker to interfere with these networks via a denial of service attack known as Jamming. These attacks can be done through equipment known as Jammers, which emit random data signals, in order to overturn communications from sensor networks. In this paper, we study the characteristics of the jamming attack in IEEE 802.15.4 networks and propose a solution to this interference attack using a software-defined cognitive radio system to detect and protect the network.*

Resumo. *As redes de sensores sem fio utilizam de meios de comunicação compartilhados para a transmissão de dados. Com isto, se torna fácil para um atacante interferir nas transmissões destas redes através de ataques de negação de serviço conhecidos como Jamming. Estes ataques podem ser feitos através de dispositivos chamados de Jammers, que emitem sinais aleatórios de dados, visando derrubar as comunicações das redes de sensores. Neste artigo, estudamos as características do ataque de interferência Jamming sobre a rede IEEE 802.15.4 e propomos uma contramedida a esse ataque utilizando um sistema de rádio cognitivo definido por software para detectar e proteger a rede.*

1. Introdução

As Redes de Sensores sem Fio (RSSF) consistem em centenas ou até mesmo milhares de dispositivos pequenos, cada um com capacidade de detecção, processamento e comunicação para monitorar o ambiente físico. As RSSF operam através de um meio de comunicação compartilhado, se tornando assim alvos para ataques de negação de serviço, uma vez que um usuário mal intencionado pode reduzir a disponibilidade do meio [Torrieri 1985]. Um destes ataques se caracteriza como sendo o envio de um sinal em um meio de comunicação compartilhado com o intuído de reduzir sua disponibilidade (através da redução da relação sinal ruído do meio). Este ataque é conhecido como *Jamming* [Wood et al. 2007].

Jamming é definido como sendo um tipo especial de ataque de negação de serviço (em inglês, DOS - *Denial Of Service*). Wood e Stankovic definem DOS como sendo "qualquer evento que diminua ou elimine a capacidade de uma rede para executar sua

função esperada" [Wood and Stankovic 2002]. Portanto, se torna necessário o uso de sistemas de segurança que protejam as RSSF contra estas interferências propositais, principalmente quando levamos em consideração as limitações deste tipo de rede, como baixa capacidade computacional, memória limitada e baixa eficiência energética.

O objetivo deste artigo é descrever o ataque de negação *Jamming* e seus efeitos sobre uma rede de sensores IEEE 802.15.4, assim como, propor uma solução a este tipo de ataque através do uso de rádio cognitivo. Um rádio cognitivo pode analisar as frequências de transmissão e recepção de um meio compartilhado e alterar suas características [Mitola and Maguire 1999]. Para testarmos a ferramenta de *jamming*, foi desenvolvido um agente para a ferramenta de gerência Zabbix com a função de monitorar o canal de transmissão dos sensores e sua mudança. Ainda, realizamos a criação de uma rede de sensores utilizando um roteador de borda SmartRf06EBK™ e sensores CC2650-sensortag™ fabricados pela Texas Instruments para avaliar em campo a contramedida proposta.

Este artigo está organizado da seguinte forma: na Seção II estão descritas as características do padrão do *Institute of Electrical and Electronic Engineers* IEEE 802.15.4. Na Seção III estão descritas as características e os tipos de ataque de *Jamming* conhecidos. Na Seção IV apresenta-se uma proposta de arquitetura de Rádio Cognitivo que emprega um sistema de Rádio definido por Software como contramedida ao ataque Jamming. Na Seção V listamos os trabalhos relacionados. Na seção VI é demonstrado os resultados experimentais e a análise da ferramenta. Na seção VII concluimos o artigo.

2. Característica do Padrão IEEE 802.15.4

O IEEE 802.15.4 é um padrão para *Wireless Personal Area Network* (WPAN) que propõe uma rede de dados pessoal sem fio de baixa taxa de dados. É caracterizada por permitir uma rede de baixa complexidade e um tempo de vida maior de bateria. Suas potenciais aplicações são sensores, brinquedos interativos, crachás inteligentes, controles remotos [sta 2015]. Seu alcance varia de 10 a 100 metros, com uma potência máxima de saída geralmente de 0 dBm. O padrão define as características da camada física (PHY) e *Medium Access Control* (MAC) do modelo de referência *Open System Interconnection* (OSI).

Conforme a Tabela 1, a camada física do padrão IEEE 802.15.4 opera em três faixas de frequência livres, sendo elas: 868MHz, 915MHz e 2,4GHz *Industrial, Scientific and Medical* (ISM). Assim como as frequências de 314–316MHz, 430–434MHz, e 779–787MHz para *Low Rate - Wireless Personal Area Network* (LR-WPAN) na China e 950–956MHz no Japão [sta 2015].

Conforme a Figura 1, o padrão divide o espectro em um total de 27 canais, sendo 1 canal para a frequência de 868MHz, 10 canais para a frequência de 915MHz e 16 canais para a frequência de 2,4GHz.

Direct Sequence Spread Spectrum (DSSS) é utilizado nas frequências de 868/915 MHz junto com a modulação *Binary Phase Shift Keying* (BPSK), que permite taxas de transmissão até 20 Kbps e até 40 Kbps. Já na frequência de 2.4 GHz utiliza-se modulação *Quadrature Phase Shift Keying* (QPSK), que permite uma taxa de transmissão até 250 kbps [sta 2015] [Misic and Misic 2008].

A partir da revisão IEEE 802.15.4a foram introduzidas novas opções para a ca-

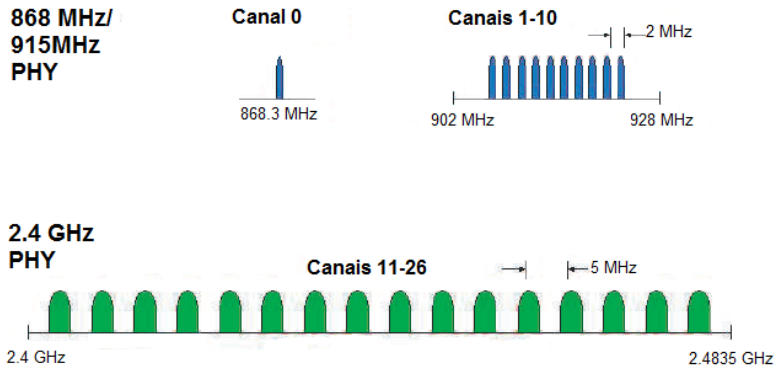


Figura 1. Espectro de radiofrequência IEEE 802.15.4 [Ergen 2004].

PHY	Banda de Frequência (MHz)	Taxa de Espalhamento (Kchip/s)	Modulação	Taxa de Bits (Kb/s)	Taxa de Símbolos	Símbolos
869/915	868-868,6	300	BPSK	20	20	BINÁRIO
	902-928	600	BPSK	40	40	BINÁRIO
2.450	2400-2483,5	2000	O-QPSK	250	62,5	16 símbolos

Tabela 1. Banda de Frequência e Taxa de Dados [Misic and Misic 2008].

mada física, permitindo um aumento nas taxas de dados e capacidade de alcance preciso e novas aplicações baseadas em informações sobre distância e posições dos dispositivos na rede. Estas melhorias começaram a partir da versão lançada em 2006 que já permitia se alcançar taxas de 250Kbps para as frequências de 868/915MHz. A camada física do padrão IEEE802.15.4a passou a ser baseada em duas diferentes tecnologias [Karapistoli et al. 2010] [De Nardis and Di Benedetto 2007]:

- ***Utra Wideband (UWB) impulse radio*** - que opera em um espectro não licenciado UWB. Suporta três bandas de frequência independentes:
  - Banda Sub-GigaHertz - um único canal (canal 0) ocupando o espectro de 249,6 até 749,6MHz.
  - *Low Band* - consiste em quatro canais (canais de 1 a 4) ocupando o espectro de 3.1 a 4.8GHz.
  - *High Band* - consiste em 11 canais (canais de 5 a 15) ocupando o espectro de 5.8 a 10.6GHz.
- ***Chirp Spread Spectrum (CSS)*** - baseado no espectro não licenciado de 2.4GHz. Foi criado para suportar enlaces de longo alcance e para dispositivos móveis movendo-se em alta velocidade. A taxa de dados da camada física CSS passa a ser de 1Mbps (nominal) e de 250Kbps (opcional).

3. Ataque *Jamming*

O *Jamming* é definido como sendo a transmissão de um sinal de rádio com o intuito de interferir nas comunicações de uma rede de radiofrequência (RF) de forma intencional [Adamy 2004]. Existe uma outra forma de interferência conhecida como interferência de radiofrequência (em Inglês, RFI - *radio frequency interference*), que ocorre devido

IEEE 802.11		IEEE 802.15.4	
Canal	**Freq. (GHz)**	**Canal**	**Freq. (GHz)**
1	2.401 - 2.423	11	2.405
2	2.404 - 2.428	12	2.410
3	2.411 - 2.433	13	2.415
4	2.416 - 2.438	14	2.420
5	2.421 - 2.443	15	2.425
6	2.426 - 2.448	16	2.430
7	2.431 - 2.453	17	2.435
8	2.436 - 2.458	18	2.440
9	2.441 - 2.463	19	2.445
10	2.446 - 2.468	20	2.450
11	2.451 - 2.473	21	2.455
Os canais 22 a 26 do padrão IEEE 802.15.4 não sofrem interferência			

Tabela 2. Tabela de Canais Sobrepostos do Padrão IEEE 802.11 e IEEE 802.15.4

a proximidade a outras redes de RF que transmitem no mesmo canal de comunicação. Conforme a Tabela 2, redes no padrão IEEE 802.15.4 podem sofrer interferência de redes IEEE 802.11, pois alguns canais de frequências na banda de 2.4GHz são coincidentes.

3.1. Tipos de Ataques *Jamming* e Dispositivos *Jammers*

Com base nas características físicas descritas do padrão IEEE 802.15.4, podemos definir que um nó sensor pode se conectar a uma rede utilizando um número limitado de canais de comunicação: 16 canais na faixa de 2,4 GHz (2400-2483,5 MHz), 10 canais (30 para 2006) em 902-928 MHz e 1 canal (3 para 2006) em 868,3 MHz. Levando ainda em consideração que a potência máxima é de geralmente 0 dBm, pode-se perceber que um atacante pode facilmente interferir no sinal de uma rede de sensores.

O ataque de interferência tem seu sucesso ligado diretamente a relação sinal ruído de uma transmissão. O ruído nada mais é do que a representação da flutuação do espectro eletromagnético dada pela relação SNR = P_{signal}/P_{noise}, onde P representa a potência média. Um ataque *Jamming* se torna efetivo para SNR$<$1. Existem vários métodos de ataque de *Jamming* [O'Flynn 2011], sendo eles:

- ***Jamming de pontos*** - Neste tipo de ataque, toda a potência do sinal é dirigido para apenas um canal de transmissão. Assim, o sinal original é substituído pelo sinal do atacante. Para este tipo de ataque a melhor solução seria a mudança de canal de transmissão da rede.
- ***Jamming de varredura*** - Este ataque utiliza saltos de canais, ao invés de um canal só. O sinal atacante muda de canal alternadamente, ocupando assim toda a banda de transmissão.
- ***Jamming de barragem*** - O bloqueio é feito em intervalos de frequência, ou seja, o sinal de interferência é transmitido em dois ou mais canais ao mesmo tempo. Este ataque pode bloquear múltiplas frequências.
- ***Jamming enganador*** - Pode ser aplicado a uma única frequência ou conjunto de frequências. Este ataque é usado quando o atacante não quer ser detectado.

Ele é feito inundando a rede com dados falsos, com o intuito de causar falhas de transmissão e perda de pacotes.

Os dispositivos usados para gerar as interferências são chamados de *Jammers*. Normalmente, são equipamentos de RF simples, mas que transmitem o sinal em alta potência. Existem vários tipos de *jammers*. Xu et al. [Xu et al. 2005], propõem vários modelos genéricos, sendo eles:

- **Constante** - Emite um sinal aleatório e constante de alta potência. Este *jammer* envia apenas *bits* aleatórios. Sua função é manter o canal ocupado, interrompendo as transmissões no canal.
- **Enganador** - Transmite um sinal usando as técnicas do *jamming* enganador, isto é, pode transmitir dados em uma única frequência ou em um conjunto de frequências.
- **Aleatório** - Este tipo de jammer alterna aleatoriamente seu estado de repouso e de ataque a rede. Seu tipo de ataque a rede também pode ser qualquer um dos mencionados acima.
- **Reativo** - Escuta o canal de transmissão e ao detectar uma transmissão emite um sinal constante e aleatório para interferir na rede.

4. Contramedida ao Ataque de *Jamming* usando Rádio Cognitivo

O Rádio cognitivo pode analisar as frequências e o ambiente em que está conectado e com isto alterar as suas características de transmissão e recepção, tais como frequência e potência do sinal, melhorando a experiência do usuário [Mitola and Maguire 1999]. Um rádio cognitivo pode ser implementado em um dispositivo conhecido como *Software Defined Radio* (SDR). Define-se SDR como sendo um dispositivo que consegue alterar suas características de transmissão e recepção via software, reduzindo assim o número de funções realizadas em hardware [Jondral 2005].

Em Alberti et al. [Alberti et al. 2017] é proposta uma arquitetura de rádio cognitivo que analisa e armazena as informações de uso do espectro de frequência da rede publicando assim os canais disponíveis e ocupados. Nossa proposta se baseia nesta arquitetura. Nela, um rádio cognitivo com um sistema SDR analisa o espectro de radiofrequência, identifica qual o canal com menor interferência e redireciona automaticamente a transmissão e recepção dos nós sensores e dos roteadores de borda para este novo canal. Este sistema é composto por um módulo de célula de detecção e um dispositivo de rede sem fio. Conforme a Figura 2, o módulo de célula de detecção é composto por um SDR chamado de HackRF One™ para detectar o espectro de frequência e um laptop com middleware para processar sinais e realizar o controle SDR. O HackRF One opera de 1 MHz a 6 GHz e possui 20 MHz de largura de banda.

Exemplificando, de acordo com a Figura 3, o sistema de sensoriamento ligado ao notebook, tem a função de analisar as frequências de transmissão do padrão IEEE 802.15.4. As informações de cada canal são armazenadas e analisadas pelo algoritmo de sensoriamento, detectando assim o canal de menor interferência nos canais de transmissão. Assim, o sistema envia um comando aos sensores e ao roteador de borda. Este comando teria como função alterar a frequência de transmissão da rede de sensores para a frequência de menor interferência.

Figura 2. Hardware usado para o modulo de célula

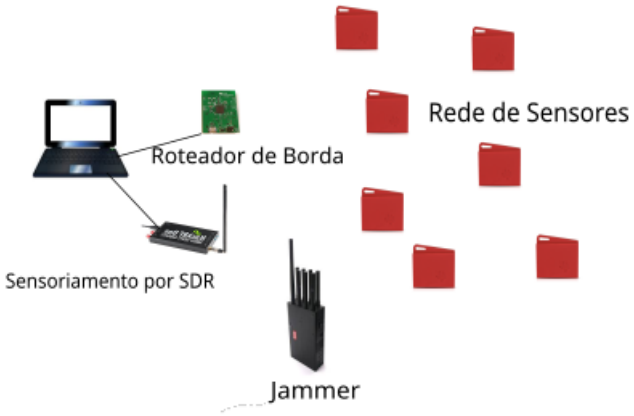


Figura 3. Exemplo de uma Rede de Sensores controlada pelo Sistema de Sensoriamento

4.1. Arquitetura do Sistema de Rádio Definido por Software

O SDR é controlado por um software que terá a função de detectar o melhor canal de transmissão. Este software opera através da plataforma GNU Radio, que é um conjunto de ferramentas usadas para a implementação de rádios definidos por software. Conforme o fluxograma definido na Figura 4, o algoritmo do GNU Radio transforma o fluxo de dados em vetores de 1024 posições, que são convertidos via bloco FFT para o domínio de frequência. Após esta conversão, calcula-se o módulo do fluxo gerado, que é convertido de tensão para energia em escala logarítmica.

Figura 4. Fluxograma do algoritmo de sensoriamento.

Para varrer os canais do padrão IEEE 802.15.4, um *script* executa o algoritmo de sensoriamento executando as trocas de frequência de 5 em 5 MHz, conforme a banda de canal do padrão. Os valores das amostras dos canais são armazenados em arquivos binários. Um outro *script* então, irá realizar os cálculos de energia do canal e trocar o canal dos nós sensores e dos roteadores de borda para o canal com menor energia detectado. A Figura 5 demonstra o fluxograma de funcionamento do *script* de sensoriamento.

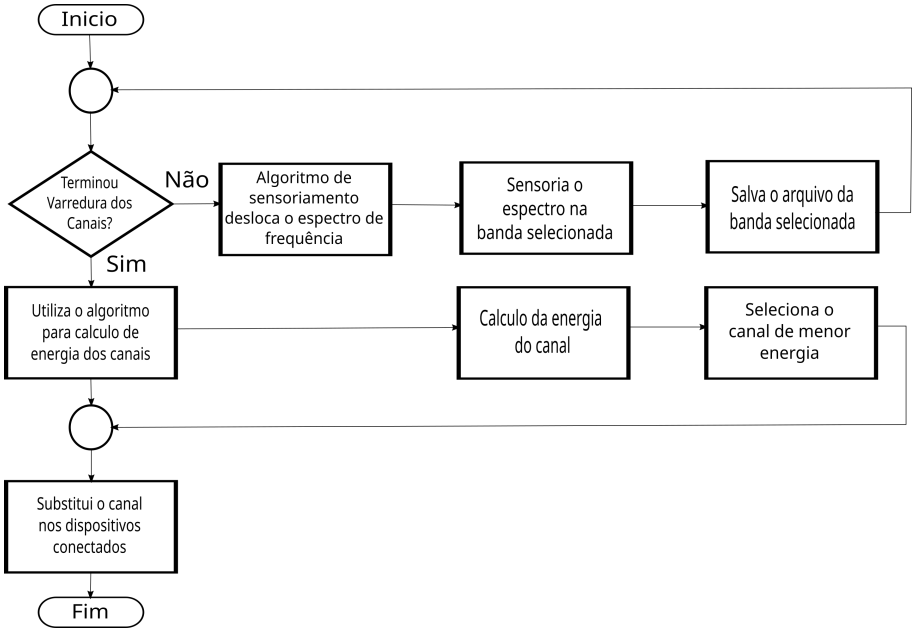


Figura 5. Fluxograma completo do sistema.

5. Trabalhos Relacionados

Um grande número de trabalhos de pesquisa sugerem soluções ao ataque de bloqueio *(Jamming)*, tendo como base os hardwares usados nas redes de sensores [Mpitziopoulos et al. 2009, Muraleedharan and Osadciw 2006, Xu et al. 2006]. Outros trabalhos sugerem novos designs para o nó como forma de combate ao ataque [Mpitziopoulos et al. 2007]. Em DeBruhl e Tague, é proposto como solução ao ataque a inclusão de um filtro digital nos receptores que teriam a função de filtrar o espectro de RF gerado pelos bloqueadores [DeBruhl and Tague 2011]. Em Mpitziopoulos et al. são discutidas várias técnicas de solução tendo como base o espalhamento espectral com saltos de frequência (em Inglês, FHSS - *Frequency-hopping spread spectrum*) e o espalhamento espectral de sequência direta (em Inglês, DSSS - *Direct Sequence Spread Spectrum*), sendo estas consideradas pelos autores as melhores soluções para as interferências de frequência [Mpitziopoulos et al. 2007]. Em Mpitziopoulos et al. é proposto o algoritmo JAID (*Jamming Avoidance Itinerary Design*), baseado na tecnologia conhecida como MA (*Mobile Agent*) proposta na literatura de RSSF. Este algoritmo calcula rotas quase ótimas para os MAs que fundem os dados de forma incremental ao visitar os nós e diante de ataques de bloqueio contra a WSN, modificam as rotas das MAs ignorando a área de interferência. Isso sem interromper a disseminação eficiente de dados pelos sensores [Mpitziopoulos et al. 2009]. Em Xu et al. são abordadas duas técnicas de proteção ao ataque de interferência. A primeira técnica conhecida como evasão de canal, visa sair do canal que o invasor está atacando e a outra visa competir com o atacante, ajustando alguns valores da rede, como potência de transmissão e codificação [Xu et al. 2006]. Em Muraleedharan e Osadciw, é proposto um novo mecanismo de segurança contra ataques de DOS. Este mecanismo é baseado em um algoritmo denominado *Ant System* que detecta o ataque de interferência nos nós sensores [Muraleedharan and Osadciw 2006]. Em Wood et al. é apresentado como solução a ataques de interferência o DEEJAM (*Defeating Energy-Efficient Jamming)*, um novo protocolo de camada MAC para o padrão IEEE

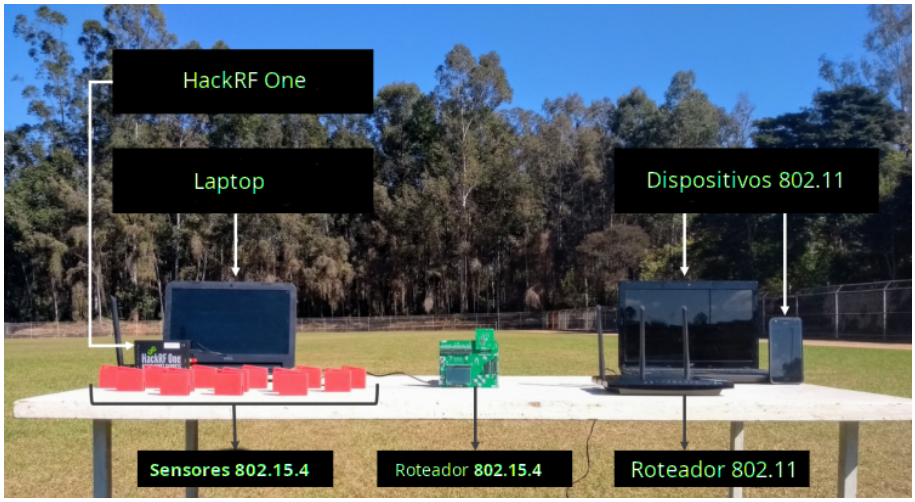


Figura 6. Cenário utilizado para o experimento.

802.15.4 [Wood et al. 2007]. No trabalho de Hamieh e Ben-Othman, os autores propõem como forma de detecção do ataque de interferência um novo método que se baseia na medição da distribuição de erros na rede [Hamieh and Ben-Othman 2009].

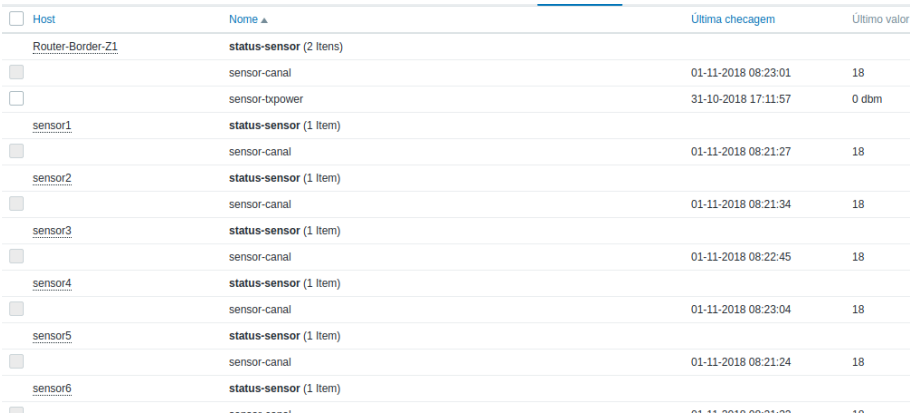
Nossa proposta de difere das demais, pois nosso sistema roda de maneira autônoma na rede, como um dispositivo a parte, que analisa todas as frequências sem assim gerar pacotes e filtros desnecessários na RSSF. Com isto, não afetando de maneira alguma a latência e não levando a perdas de pacotes.

6. Resultados Experimentais e Análise

A RSSF considerada neste experimento, ilustrada na Figura 6, opera no padrão IEEE 802.15.4. Ela é composta por um roteador de borda SMARTRF06EBK^{TM} ligado a um laptop rodando o programa de gerência de rede Zabbix, que tem como função monitorar os canais da rede de sensores e caso ocorra alguma alteração disparar uma notificação de mudança de dados e sensores CC2650-sensortag^{TM} fabricados pela Texas Instruments. Como Jammer é utilizado um roteador TP-Link N750 OpenWRT e dois laptops que se comunicam via canal 8, criando tráfego no canal de transmissão. O experimento foi executado em campo aberto, evitando assim outras interferências de redes sem fio.

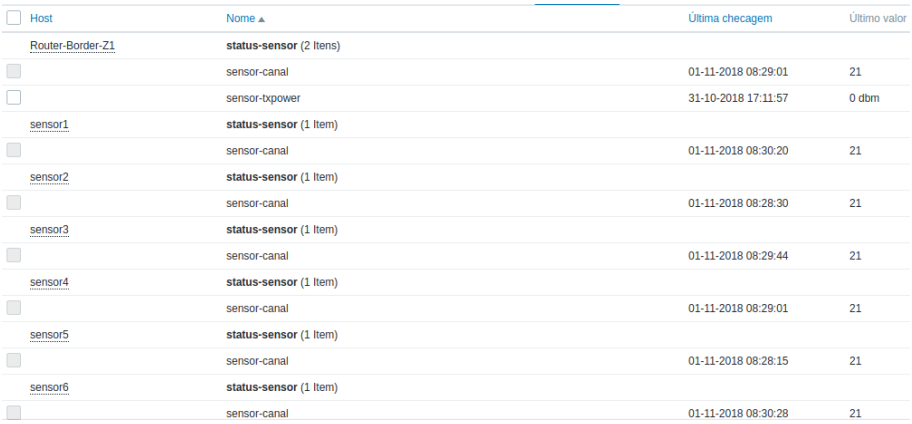
O roteador de borda e os sensores rodam o sistema operacional Contiki[Dunkels et al. 2004] e operam no canal 18. O canal 18 do padrão IEEE 802.15.4 e o canal 8 do padrão IEEE 802.11 são canais sobrepostos, gerando assim ruido de interferência de uma rede sobre a outra. O HackRF One está ligado ao laptop, onde está sendo executado o algoritmo de sensoriamento e análise de interferência. O laptop também está conectado ao roteador de borda da rede 802.15.4 para que possa ser coletado os dados para o Zabbix e para ser enviado o comando de troca de canal ao sensores e roteador de borda.

No inicio do experimento somente a rede de sensores está funcionando para que se possa levantar os dados do roteador e dos sensores no programa Zabbix, conforme mostra a Figura 7. Após alguns minutos, a rede 802.11 foi ligada, e foi gerado tráfego entre seus dispositivos para ser criado um aumento de interferência. Sem a interferência



Host	Nome ▲	Última checagem	Último valor
Router-Border-Z1	**status-sensor** (2 Itens)		
	sensor-canal	01-11-2018 08:23:01	18
	sensor-txpower	31-10-2018 17:11:57	0 dbm
sensor1	**status-sensor** (1 Item)		
	sensor-canal	01-11-2018 08:21:27	18
sensor2	**status-sensor** (1 Item)		
	sensor-canal	01-11-2018 08:21:34	18
sensor3	**status-sensor** (1 Item)		
	sensor-canal	01-11-2018 08:22:45	18
sensor4	**status-sensor** (1 Item)		
	sensor-canal	01-11-2018 08:23:04	18
sensor5	**status-sensor** (1 Item)		
	sensor-canal	01-11-2018 08:21:24	18
sensor6	**status-sensor** (1 Item)		

Figura 7. Tela inicial do experimento: sensores e roteador no canal 18.



Host	Nome ▲	Última checagem	Último valor
Router-Border-Z1	**status-sensor** (2 Itens)		
	sensor-canal	01-11-2018 08:29:01	21
	sensor-txpower	31-10-2018 17:11:57	0 dbm
sensor1	**status-sensor** (1 Item)		
	sensor-canal	01-11-2018 08:30:20	21
sensor2	**status-sensor** (1 Item)		
	sensor-canal	01-11-2018 08:28:30	21
sensor3	**status-sensor** (1 Item)		
	sensor-canal	01-11-2018 08:29:44	21
sensor4	**status-sensor** (1 Item)		
	sensor-canal	01-11-2018 08:29:01	21
sensor5	**status-sensor** (1 Item)		
	sensor-canal	01-11-2018 08:28:15	21
sensor6	**status-sensor** (1 Item)		
	sensor-canal	01-11-2018 08:30:28	21

Figura 8. Tela final do experimento: sensores e roteador no canal 21.

do Wi-Fi AP, a taxa de transferência do IEEE 802.15.4 foi de 1120 bps. Após a operação simultânea do Wi-Fi no canal 8, a taxa de transferência do 802.15.4 diminuiu para 520 bps. O sistema de sensoriamento então trocou automaticamente a rede 802.15.4 do canal 18 para o 21, conforme Figura 8. Para confirmação da troca de canais, a Figura 9 mostra os eventos de incidente gerados pelo Zabbix em relação aos canais do roteador e dos sensores.

7. Conclusão

Neste artigo, propomos e testamos um esquema de sensoriamento, utilizando Rádio Cognitivo sobre um sistema de SDR, para redes de sensores no padrão IEEE 802.15.4 , com o intuito de proteger a rede contra ataques de *Jamming*. Nos testes em rede real, que utilizaram sensores CC2650 da Texas Instruments, o sistema se mostrou satisfatório no auxilio ao combate dos seguintes tipos de *Jamming*: pontos, varredura e barragem. Nestes ataques o invasor direciona seu ataque para uma frequência específica ou para um grupo de frequências. Em nosso teste, nosso sistema pode detectar sempre qual a melhor frequência e executar a alteração dos sensores e do roteador de borda. Não houve em nenhum dos testes uma mudança no sistema de latência da rede e nem um aumento de perda de pacotes válidos, apenas, uma perda de acesso do roteador de borda aos sensores durante a troca dos canais.

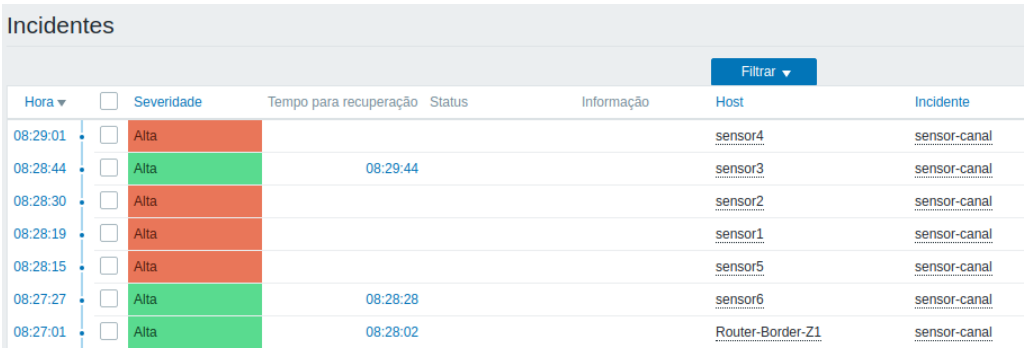


Figura 9. Tela de incidentes do Zabbix relatando mudança de canal dos sensores.

Agradecimentos

Este trabalho foi parcialmente financiado pela RNP, com recursos do MCTIC, processo No 01250.075413/2018-04, sob o projeto Centro de Referência em Radiocomunicações (CRR) do Instituto Nacional de Telecomunicações – Inatel, Brasil. Os autores agradecem também a FAPEMIG, CNPq e CAPES.

Este estudo foi parcialmente financiado pela Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Finance Code 001.

Referências

(2015). *IEEE Std 8 02.15.4TM TM-2 2015 - Revision of IEEE Std 802.15.4-2011*. IEEE.

Adamy, D. (2004). *EW 102: a second course in electronic warfare*. Artech House.

Alberti, A. M., Mazzer, D., Bontempo, M., de Oliveira, L. H., da Rosa Righi, R., and Sodré Jr, A. C. (2017). Cognitive radio in the context of internet of things using a novel future internet architecture called novagenesis. *Computers & Electrical Engineering*, 57:147–161.

De Nardis, L. and Di Benedetto, M.-G. (2007). Overview of the ieee 802.15. 4/4a standards for low data rate wireless personal data networks. In *Positioning, Navigation and Communication, 2007. WPNC'07. 4th Workshop on*, pages 285–289. IEEE.

DeBruhl, B. and Tague, P. (2011). Digital filter design for jamming mitigation in 802.15. 4 communication. In *Computer Communications and Networks (ICCCN), 2011 Proceedings of 20th International Conference on*, pages 1–6. IEEE.

Dunkels, A., Gronvall, B., and Voigt, T. (2004). Contiki-a lightweight and flexible operating system for tiny networked sensors. In *Local Computer Networks, 2004. 29th Annual IEEE International Conference on*, pages 455–462. IEEE.

Ergen, S. C. (2004). Zigbee/ieee 802.15. 4 summary. *UC Berkeley, September*, 10:17.

Hamieh, A. and Ben-Othman, J. (2009). Detection of jamming attacks in wireless ad hoc networks using error distribution. In *Communications, 2009. ICC'09. IEEE International Conference on*, pages 1–6. IEEE.

Jondral, F. K. (2005). Software-defined radio: basics and evolution to cognitive radio. *EURASIP journal on wireless communications and networking*, 2005(3):275–283.

Karapistoli, E., Pavlidou, F.-N., Gragopoulos, I., and Tsetsinas, I. (2010). An overview of the ieee 802.15. 4a standard. *IEEE Communications Magazine*, 48(1).

Misic, J. and Misic, V. (2008). *Wireless personal area networks: Performance, interconnection, and security with IEEE 802.15. 4*, volume 1. John Wiley & Sons.

Mitola, J. and Maguire, G. Q. (1999). Cognitive radio: making software radios more personal. *IEEE personal communications*, 6(4):13–18.

Mpitziopoulos, A., Gavalas, D., Konstantopoulos, C., and Pantziou, G. (2009). Jaid: An algorithm for data fusion and jamming avoidance on distributed sensor networks. *Pervasive and Mobile Computing*, 5(2):135–147.

Mpitziopoulos, A., Gavalas, D., Pantziou, G., and Konstantopoulos, C. (2007). Defending wireless sensor networks from jamming attacks. In *Personal, Indoor and Mobile Radio Communications, 2007. PIMRC 2007. IEEE 18th International Symposium on*, pages 1–5. IEEE.

Muraleedharan, R. and Osadciw, L. A. (2006). Jamming attack detection and countermeasures in wireless sensor network using ant system. In *Wireless Sensing and Processing*, volume 6248, page 62480G. International Society for Optics and Photonics.

O'Flynn, C. P. (2011). Message denial and alteration on ieee 802.15. 4 low-power radio networks. In *New Technologies, Mobility and Security (NTMS), 2011 4th IFIP International Conference on*, pages 1–5. IEEE.

Torrieri, D. J. (1985). *Principles of secure communication systems*. Artech House, Inc.

Wood, A. D. and Stankovic, J. A. (2002). Denial of service in sensor networks. *computer*, 35(10):54–62.

Wood, A. D., Stankovic, J. A., and Zhou, G. (2007). Deejam: Defeating energy-efficient jamming in ieee 802.15. 4-based wireless networks. In *Sensor, Mesh and Ad Hoc Communications and Networks, 2007. SECON'07. 4th Annual IEEE Communications Society Conference on*, pages 60–69. IEEE.

Xu, W., Ma, K., Trappe, W., and Zhang, Y. (2006). Jamming sensor networks: attack and defense strategies. *IEEE network*, 20(3):41–47.

Xu, W., Trappe, W., Zhang, Y., and Wood, T. (2005). The feasibility of launching and detecting jamming attacks in wireless networks. In *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*, pages 46–57. ACM.