Uma Análise Experimental de Ataques *Jamming* no Acesso ao Meio em Redes de Sensores Sem Fio

Fernando Henrique Gielow, Aldri Santos, Michele Nogueira

NR2 - Núcleo de Redes Sem Fio e Redes Avançadas
DINF – Universidade Federal do Paraná
Caixa Postal 19.081 – 81.531-980 – Curitiba – PR – Brasil

{fhgielow,michele,aldri}@inf.ufpr.br

Abstract. *The use of wireless sensors is increasingly common today, promoting ubiquitous and pervasive applications. However, wireless communication is susceptible to noise and interference, being vulnerable to several kinds of attack, particularly those which undermine the wireless medium. As wireless devices communicate in specific transmission frequencies, a jamming attack aims at overloading these frequencies with malicious traffic, intending to cause collisions on transmissions of legitimate nodes. Currently, the majority of existing works deal with jamming only through simulations or by analytical models. However, it is important to investigate the impact of these attacks in real networks. This work conducts an experimental study about the impact of jamming attacks in real scenarios, followed by a verification and a comparative between experimental and simulation results, highlighting the differences among them. It is also expected to show the way in which the variation of the used transmission power can increase the efficiency of the jamming attack or improve the quality of communication.*

Resumo. *O uso de sensores sem fio é cada vez mais comum no mundo atual, dando suporte ao desenvolvimento de aplicações ubíquas e pervasivas. Entretanto, comunicação sem fio está sujeita a ruídos e a interferências, sendo vulnerável a diversos tipos de ataque, especialmente aqueles que sabotam o meio sem fio como um todo. Como os dispositivos sem fio se comunicam por meio de uma frequência de transmissão, o ataque jamming visa sobrecarregá-las através da geração de tráfego malicioso, com a intenção de causar colisões nas transmissões dos nós legítimos. Atualmente, a maioria dos trabalhos existentes tratam dos ataques jamming apenas por meio de simulações ou de maneira analítica. Porém, é importante realizar estudos do impacto destes ataques em redes reais. Este trabalho apresenta um estudo experimental sobre o impacto do ataque jamming em cenários reais, seguindo da verificação e comparação entre os resultados experimentais e de simulações e destacando suas diferenças. Espera-se ainda mostrar a maneira com que a variação da potência de transmissão empregada pelos nós sensores pode aumentar a eficiência do ataque jamming ou melhorar a qualidade da comunicação.*

1. Introdução

Com a evolução das tecnologias sem fio e o advento de peças de *hardware* mais baratas, sensores sem fio estão cada vez mais infiltrados na sociedade atual. Tais dispositivos dependem do meio sem fio para realizar suas tarefas de monitoramento. Como o meio de comunicação sem fio é aberto, ele está sujeito a interferências, sejam elas maliciosas ou não. Um ataque *jamming* consiste na negação do serviço de clientes legítimos em uma dada frequência que é sobrecarregada com uma quantidade massiva de tráfego ilegítimo (malicioso). Considerando que o atacante *jammer* não precisa ouvir respostas, este é um ataque simples e de grande impacto na rede, dado que atacantes conseguem poluir o espectro de frequência utilizando-se de suas bandas de transmissão inteiras. Assim, a interferência no meio é atenuada e o número de colisões de pacotes cresce, impossibilitando a comunicação entre clientes legítimos da rede [Mpitziopoulos et al. 2009].

Este trabalho consiste na análise do impacto de ataques *jamming* em uma Rede de Sensores Sem Fio (RSSF) real. Embora diversos estudos realizem análises de desempenho deste ataque, esses estudos, em sua maioria, não consideram implementações práticas para experimentação [Chiang and Hu 2011, Sang and Arora 2009, Xu et al. 2006]. Neste trabalho, o caso do ataque *jamming* proativo será considerado. Tal ataque independe do uso legítimo do meio sem fio – o atacante estará sempre enviando tráfego malicioso em *broadcast*, a fim de impedir a comunicação dos demais nós.

Por fim, são realizados experimentos com nós do tipo MicaZ. Estes nós operam na faixa de 2.4 GHz através do protocolo IEEE 802.15.4 na camada de enlace, base para a especificação de comunicação ZigBee [Ramya et al. 2011]. Os sensores MicaZ são comumente utilizados em redes densas que visam a coleta de dados escalares e permitem o uso do sistema operacional TinyOS. Desta forma, este sistema operacional teve as componentes de comunicação utilizadas pelo nó MicaZ alteradas, a fim de que um ataque *jamming* **fosse** implementado e por fim experimentado. Este artigo tem como contribuição a comparação entre resultados de experimentação e simulação, ressaltando um caso em especial, no qual há grande diferença entre ambos.

Este artigo segue como descrito. A Seção 2 analisa os trabalhos relacionados. A Seção 3 apresenta os fundamentos necessários para o entendimento do restante do artigo, sendo eles referentes à especificação dos nós MicaZ, às características gerais do sistema operacional para sensores TinyOS, assim como a implementação do TinyOS para o rádio CC2420, um rádio popular que considera a comunicação eficiente em energia. Em seguida, a Seção 4 detalha a implementação do ataque *jamming* realizado nos experimentos. A Seção 5 apresenta a análise dos experimentos e a comparação destes resultados com os de simulações. Por fim, a Seção 6 conclui este artigo.

2. Trabalhos relacionados

Em [Xu et al. 2005], os autores realizam um estudo experimental sobre ataques *jamming*. São considerados quatro tipos de ataque: constante (fluxo contínuo de dados maliciosos), reativo (envio de dados maliciosos quando é detectada uma transmissão legítima), aleatório (alternância entre modo de transmissão contínua e modo desativado) e deceptivo (ao invés de dados aleatórios, pacotes reais são transmitidos, porém sem intervalos de espera). Este trabalho, entretanto, foca na avaliação experimental de técnicas de detecção dos ataques. Embora seja dito que eles comprometem a taxa de entrega de pacotes e afetem a latência, tais métricas não são avaliadas experimentalmente.

Questões de segurança nas redes de sensores sem fio são investigadas por Martinovic et al. em [Martinovic et al. 2009]. Os autores propõem um mecanismo que realiza um ataque *jamming* defesivamente, contra os atacantes maliciosos. A idéia base do mecanismo é detectar ataques *jamming* e tentar barrá-los através de outros ataques, disparados por nós legítimos, contra os atacantes. Tal abordagem é adequada para ataques de *jamming* deceptivo, isto é, quando pacotes com formatos reais são enviados, porém contendo dados falsos. Por fim, embora este trabalho realize uma análise rigorosa de impactos do ataque, seu foco é claramente avaliar o mecanismo de mitigação de pacotes falsos, gerados por atacantes *jamming*.

Uma análise a respeito da defesa de ataques *jamming* baseada no aumento da potência de transmissão dos nós legítimos é apresentada em [Xu 2007]. Nesta análise, os

autores utilizam nós do tipo Mica2 para a análise da taxa de entrega de pacotes legítimos sob um ataque *jamming*. Embora a taxa de entrega de pacotes tenha sido avaliada, nós do tipo Mica2 operam com o rádio CC1000, que possui uma baixa capacidade de transmissão de dados. Além disso, este rádio opera com a decodificação contínua de *bits*, que é uma abordagem bastante distinta da utilizada pelos rádios de nós sensores mais modernos.

Desta forma, mesmo o ataque *jamming* sendo um tópico alvo de muitas pesquisas, as análises experimentais encontradas atualmente focam na análise de desempenho de modificações do ataque *jamming* ou na proposta de mitigação desse ataque. Este artigo visa expor uma análise experimental do impacto causado por um ataque *jamming* proativo simples, sem modificações que possam tirar a generalidade dos resultados. Por fim, os resultados serão analisados e comparados com resultados de simulações da mesma implementação de ataque utilizada para a experimentação.

3. Fundamentos

Esta seção apresenta a base de fundamentos necessária para o entendimento do restante do artigo. Inicialmente, o nó MicaZ é apresentado. Em sequência, o sistema operacional para sensores TinyOS é descrito e, por fim, a implementação do rádio CC2420, utilizado pelo sensor MicaZ, é detalhada.

3.1. MicaZ

Os sensores (nós) do tipo MicaZ [MicaZ] se comunicam na frequência de 2.4GHz, através do protocolo IEEE 802.15.4. Tais sensores foram desenvolvidos visando a compatibilidade com a especificação ZigBee, que considera a comunicação de baixo custo para a comunicação sem fio entre dispositivos de pouca energia, sendo mais simples do que o padrão BlueTooth, por exemplo. Este padrão foi especificado com a intenção de ser integrado como um dos componentes principais para redes ubíquas e é mantido pela *ZigBee Alliance*. Construído acima das camadas física e de enlace definidos pelo padrão IEEE 802.15.4, o ZigBee adiciona componentes para a comunicação sem fio de banda pequena com baixos custos de energia.

Utilizados para monitoramento de dados escalares, os nós MicaZ permitem expansão para conectores que incorporam sensores para medição de temperatura, pressão atmosférica, aceleração, acústica, magnetismo, entre outros. Em [Werner-Allen et al. 2006], por exemplo, uma rede de nós MicaZ é utilizada para o monitoramento de vulcões. Tais nós foram desenvolvidos especificamente para uso em redes de sensores densas, onde qualquer nó pode atuar como um roteador e retransmitir o tráfego recebido.

3.1.1. Rádio CC2420

Os nós MicaZ utilizam como rádio para a sua comunicação o CC2420 [CC2420 2007], que atua na frequência de 2.4GHz por meio do padrão IEEE 802.15.4, tendo também compatibilidade com a especificação ZigBee. O rádio CC2420 possui consumo de energia pequeno, de no máximo $17.4mA$ para transmissão e $18.8mA$ enquanto em modo de recepção. Este rádio, além de permite o cálculo do RSSI e LQI digitais, critérios para estimar distância ou qualidade de sinal, também permite a variação da potência de transmissão utilizada.

No TinyOS [Levis et al. 2004], a pilha de protocolos que coordena o rádio consiste de diversas camadas entre a aplicação e o *hardware*. Enquanto as camadas superiores modificam os dados e os cabeçalhos dos pacotes, por exemplo, as camadas mais baixas determinam o comportamento dos envios e recebimentos de mensagens. A camada mais alta desta pilha corresponde à componente *CC2420ActiveMessageC*, que é ilustrada na Figura 1. Na figura, os retângulos representam componentes e as elipses representam interfaces que as componentes indicadas pela seta provém. Uma seta entre duas componentes quer dizer que a componente na origem da seta faz uso de alguma interface provida pela componente no fim da seta.

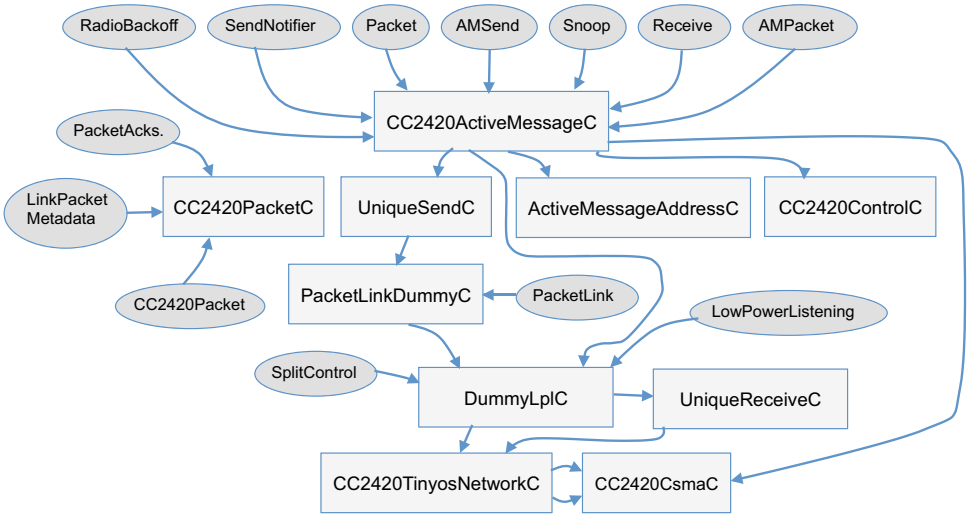

Figura 1. Implementação da comunicação pelo rádio CC2420

Nesta camada ilustrada na figura, a componente *CC2420ActiveMessageP* provém diretamente as interfaces *RadioBackoff*, *SendNotifier*, *Packet*, *AMSend*, *Snoop*, *Receive* e *AMPacket*. Nestes, a interface *AMSend* provém, dentre outros, o método *Send*, para o envio de mensagem em alto nível, assim como o evento *SendDone*, que a aplicação deve implementar a fim de que a interface *AMSend* possa comunicá-la sobre o término de um envio de mensagem. A interface *RadioBackoff* provém métodos e eventos que possibilitam a estipulação do valor do *backoff* das mensagens enviadas, assim como as consultas sobre estes valores.

4. Implementação do Ataque Jamming

Ataques *Jamming* são caracterizados por ignorar o controle de acesso ao meio sem fio, ou seja, o atacante transmitirá independente de outras transmissões ocorrendo no meio. Desta maneira, a subcamada de *Carrier Sense Multiple Access* implementada para o rádio CC2420 deve ser modificada a fim de permitir que o nó atacante possa realizar transmissões em um meio ocupado. Esta subcamada provém as interfaces *Send*, para envio de dados em baixo nível, e *RadioBackoff*, que determina o tempo que deve ser esperado entre tentativas de acesso ao meio, caso ocupado.

Um método importante no *Carrier Sense Multiple Access* é o *Clear Channell Assessment* (CCA), que realiza a verificação de meio ocupado antes da transmissão. Desta forma, para um atacante *jamming* ser bem sucedido, esta operação será completamente

desabilitada. Ademais, existem diversos tempos de *backoff*, para o caso de se detectar o meio como ocupado antes de transmitir, ou de ocorrer uma colisão durante uma transmissão. Desta maneira, estes tempos de *backoff* serão alterados para zero, a fim de possibilitar a transmissão de dados contínua mesmo em caso de colisão.

Realizadas as modificações apontadas, a implementação do *jamming* consiste no envio contínuo de dados para o meio sem fio. Como o TinyOS é um sistema baseado em eventos, existe um comando para o envio de determinado pacote, e um evento que indica o término de tal envio. Desta forma, o atacante *jamming* poderá chamar um novo método de envio quando o evento que indica o final do envio anterior, ou mesmo tentar realizar transmissões continuamente, independente do resultado da transmissão anterior. Na implementação utilizada, o evento indicativo de fim de transmissão foi ignorado, sendo que diversas chamadas de envio são chamadas continuamente.

Na tentativa de prover uma generalização dos resultados, a implementação do ataque *jamming* é a mais simples possível. O pacote a ser enviado continuamente para o meio sem fio é fixo, isto é, não depende de qualquer leitura do meio ou geração de números aleatórios. Além disso, a implementação permitirá ao atacante a variação da potência de transmissão, de acordo com os parâmetros do rádio CC2420.

5. Experimentos

Serão realizados experimentos considerando a comunicação entre sensores (nós) do tipo MicaZ.A potência de transmissão dos nós atacantes será variada, sendo que a dos nós legítimos será fixa. Pretende-se determinar não só o impacto causado pelo ataque *jamming*, variando-se a potência de transmissão utilizada. Tal cenário de teste é similar ao apresentado na Figura 2. São considerados apenas dois nós legítimos e um atacante para que se possa isolar o impacto do atacante na comunicação legítima.

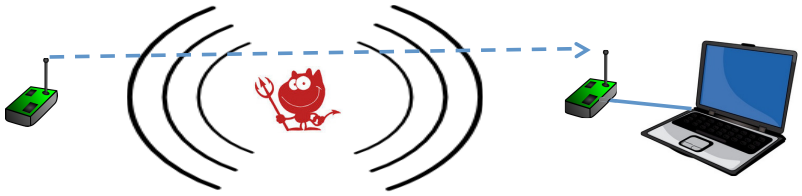

Figura 2. Cenário de experimentação

A aplicação legítima implementada para a experimentação no cenário apresentado consiste no envio de uma mensagem em *broadcast* a cada intervalo de $50ms$. Junto ao envio, os nós se manterão ouvindo o meio. Caso uma mensagem seja recebida, ela será computada, e os leds de interface do sensor MicaZ serão incrementados. A coleta dos dados é realizada através de uma placa de programação MIB510, que possui uma interface USB para a conexão com o computador. Desta forma, a cada mensagem recebida ou enviada, será possível calcular a taxa de entrega de pacotes, dado que a taxa de transmissão de ambos os sensores é a mesma.

Como cenário, foram consideradas posições fixas para os nós legítimos, espaçados a 70cms um do outro, havendo um nó atacante exatamente no meio deles. Tal posicionamento foi considerado levando em consideração o baixo alcance na comunicação destes

nós, que é evidente em aplicações pervasivas em redes corporais. A potência de transmissão dos nós legítimos foi fixada em -20dBm, enquanto a potência do nó atacante varia[1]. Para avaliar o impacto de ataques *jamming*, serão coletados valores para as métricas **taxa de entrega de pacotes** e **latência** dos pacotes entregues. Por fim, o resultados são verificados e comparados através do simulador Avrora [Avrora 2008], que pode utilizar a mesma implementação da experimentação, como será descrito adiante.

5.1. Resultados dos experimentos

Esta subseção apresenta os resultados obtidos experimentalmente nos cenários descritos. Inicialmente, é mostrada a taxa de entrega dos dados e, por fim, a latência das transmissões.

5.1.1. Taxa de entrega dos dados

A taxa de entrega dos pacotes é uma métrica importante, pois reflete diretamente a qualidade da comunicação pelo meio sem fio. Esta métrica consiste da quantidade de pacotes entregues com sucesso ao destino durante o tempo de experimentação, dividido pelo número total de pacotes enviados na origem de tráfego. O gráfico ilustrado na Figura 3 apresenta a variação da taxa de entrega dos pacotes direcionados ao nó conectado no computador de acordo com a variação da potência de transmissão utilizada pelo nó atacante.

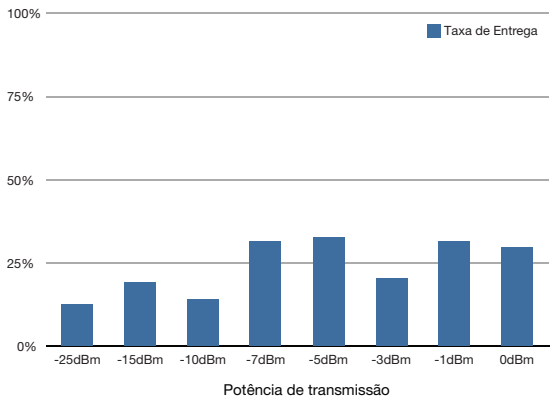

Figura 3. Taxa de entrega com relação à potência utilizada pelo atacante

Observando o gráfico, pode-se notar que a variação da potência de transmissão do nó atacante não estabelece uma variação padrão na taxa de entrega dos dados, isto é, no nosso cenário, elas são independentes. Devido ao fato de se utilizar um sensor do tipo MicaZ não só como nó legítimo mas também como nó atacante, não existe diferença no poder computacional entre eles. Desta forma, como a taxa de transmissão do nó MicaZ não é alta, dado que ele é um dispositivo para uso focado na coleta de dados e transmissões a baixas taxas de transferência, a potência de transmissão utilizada não é tão importante quanto o fator de sincronia entre os envios de mensagens dos nós legítimos e do nó atacante. Assim, basta que a potência do nó atacante seja o bastante para que ele consiga atingir os nós legítimos para causar impacto na rede. O mesmo comportamento foi percebido no trabalho de Hussain e Saqib [Hussain and Saqib 2011].

[1]Note que as potências consideradas pelos gráficos são aquelas mapeadas no *datasheet* do rádio CC2420.

Por fim, embora o impacto causado seja o bastante para denegrir significantemente a comunicação no meio sem fio, ele ainda não é tão severo quanto seria caso o atacante pudesse mandar suas mensagens em um intervalo de tempo menor. Para ilustração, enquanto os sensores do tipo MicaZ podem operar, por padrão, com *Timers* com precisão na ordem de até milisegundos, sensores mais poderosos como o Iris podem atingir a ordem de precisão dos microsegundos. Esta ordem de grandeza é fruto da potência computacional dos dispositivos, que juntamente com o rádio utilizado, influenciam no intervalo de tempo mínimo entre as mensagens enviadas.

5.1.2. Latência

A latência é uma métrica de grande importância em aplicações de *streaming* multimídia em tempo real e em aplicações de coleta de dados que envolvam riscos e a capacidade de resposta rápida a estes. Esta métrica corresponde ao tempo que um pacote enviado demora para chegar da sua origem ao seu destino. O gráfico apresentado na Figura 4 mostra a latência observada nas transmissões legítimas que atingem o nó conectado ao computador.

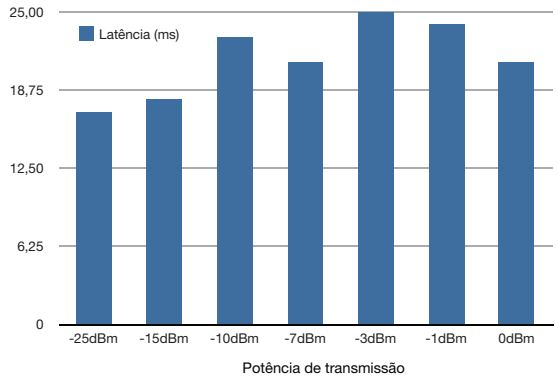

Figura 4. Latência na entrega com relação à potência utilizada pelo atacante

Observa-se que a latência também não apresenta um comportamento padrão no cenário avaliado. Da mesma forma que a sincronia afeta a taxa de entrega, a latência varia de acordo com a interferência e colisões no meio sem fio. Como o nó atacante não possui uma maior capacidade computacional do que os nós legítimos, a latência se comporta de acordo com a sincronia entre os envios de mensagens dos dispositivos.

5.2. Verificação e comparação dos resultados

A verificação dos resultados consistirá da prova através de simulação de que a sincronia entre os dispositivos computacionais é importante quando o nó atacante possui os mesmos recursos que os nós legítimos. Ou seja, enquanto uma maior capacidade computacional e de rádio garantiria que o nó atacante pudesse enviar mais pacotes ao meio em menor intervalo de tempo, causando mais colisões, a sincronia no envio das mensagens pode impactar igualmente o meio sem fio, no caso de dispositivos de mesma capacidade. Para isso, o simulador Avrora [Avrora 2008] foi utilizado.

O Avrora é um simulador baseado em emulação que utiliza o arquivo binário gerado pela compilação do código NesC, aquele que seria utilizado pelos nós sensores, de

fato. Desta forma, será utilizado mesmo o binário que foi criado para a experimentação, garantindo assim que o programa simulado é exatamente igual ao que foi utilizado na seção anterior. Assim, este simulador possui precisão em nível de instruções.

O código binário executado nos nós será também executado pelo Avrora instrução-a-instrução, garantindo com isso a sincronia perfeita entre os dispositivos sem fio. Com isso, espera-se mostrar que em um ambiente com sincronia entre os dispositivos sem fio, um nó atacante com capacidade computacional baixa e similar aos nós legítimos é capaz de impactar significativamente a rede, dado que as mensagens serão transmitidas em instantes de tempo iguais e o cálculo das colisões será afetado por isto.

5.2.1. Taxa de entrega dos dados

Esta seção apresenta a verificação da taxa de entrega de dados referente às simulações realizadas. A Figura 5 mostra os resultados obtidos e, como esperado, observa-se que a taxa de entrega de pacotes foi inferior para todas as potências utilizadas pelo nó atacante.

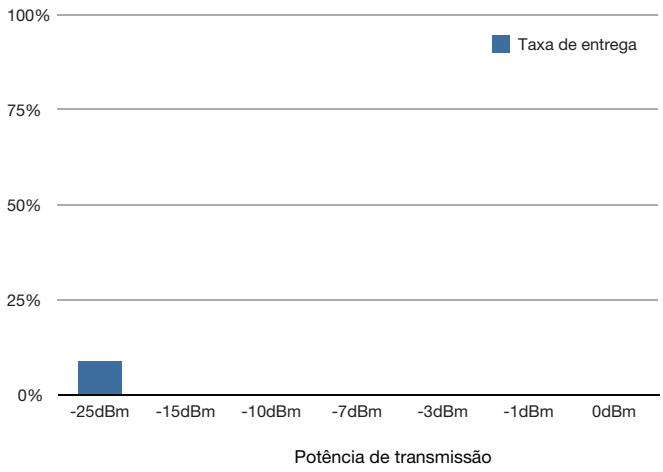

Figura 5. Taxa de entrega com relação à potência utilizada pelo atacante

A única ocasião na qual a taxa de entrega é superior a 0% é quando a potência de transmissão utilizada pelo atacante é inferior à potência utilizada pelos nós legítimos. Neste caso, o atacante se comunica com a potência de -25dBm, enquanto os nós legítimos se comunicam com a potência fixa de -20dBm. Ainda assim, é observado que a comunicação entre os nós legítimos é muito denegrida devido ao fator da sincronia entre eles e o atacante.

A Figura 6 consiste de parte da saída da execução do simulador e ilustra o impacto das colisões e interferências. Nesta figura, estão ilustrados os recebimentos de mensagens legítimas nos nós legítimos. A primeira coluna indica o índice do nó recebendo a mensagem. A segunda coluna indica o instante em que a mensagem foi recebida. A quarta coluna apresenta a mensagem recebida em hexadecimal e, por fim, a quinta coluna informa a latência da transmissão.

O conjunto de pares hexadecimais em vermelho claro correspondem aqueles da-

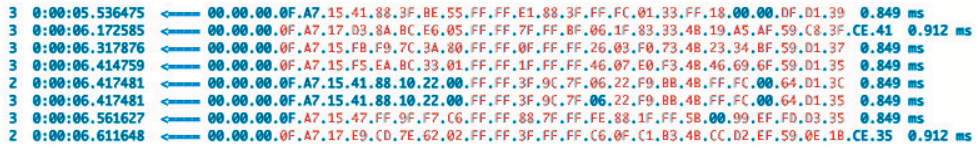

Figura 6. Pacotes corrompidos durante simulação no Avrora

dos que sofreram colisões e, desta forma, foram corrompidos. Neste caso, todos os pacotes recebidos, tanto pelo nó 2 quanto pelo nó 3, foram corrompidos. Isto leva à uma taxa de entrega de dados de 0% neste cenário. Deve-se notar que esta taxa é fruto da natureza do simulador, que executa todas instruções em nós sensores diferentes de maneira síncrona.

Além disso, como se pode ver nesta saída da execução do Avrora, o tempo de latência na entrega dos pacotes varia pouco. Isto acontece também devido à sincronia com a qual o Avrora executa o código binário. Devido a este aspecto temporal, não foi realizada a verificação de desempenho quanto à latência, pois seus resultados seriam irreais e análogos aos obtidos para a taxa de entrega dos pacotes.

5.2.2. Discussão

Através do que foi apresentado nas seções anteriores, verifica-se que os resultados da simulação foram fortemente influenciados pela sincronia entre os relógios dos nós. Esta sincronia em ambientes reais, por sua vez, dependeria do momento em que os nós são ligados e das consequentes variações naturais entre os relógios destes nós. Por isso, os resultados obtidos na experimentação não seguiram um padrão esperado - eles foram influenciados pela sincronia com a qual os nós foram ligados.

A simulação realizada demonstrou que em ambientes de sincronia perfeita, um nó atacante *jamming*, mesmo que de baixa capacidade computacional, é capaz de causar um grande impacto na rede sem fio. Desta forma, é possível que o comportamento de diversos ataques *jamming* proativos realizados em simulações não sejam condizentes com o comportamento que ocorreria na prática. Este fator de sincronia é de importância crítica quando são considerados atacantes com baixas capacidades computacionais e de transmissão. Assim, para ataques proativos, nós de baixa capacidade computacional podem falsamente aparentar comprometer a rede de maneira mais severa nas simulações do que aconteceria na realidade. Por isso, é essencial que trabalhos envolvendo ataques desta natureza considerem a variação de relógio nos nós.

6. Conclusão

Este artigo apresenta uma visão geral sobre a implementação de ataques *jamming* compostos por nós do tipo MicaZ, que se comunicam através padrão ZigBee, muito utilizado em ambientes pervasivos. Inicialmente, foram descritas a plataforma MicaZ e as componentes necessárias ao seu rádio CC2420 e à implementação do ataque *jamming*. Assim, foram indicadas as alterações que devem ser realizadas para que o nó consiga sobrecarregar o meio sem fio com pacotes, se comportando como um atacante.

Na experimentação, a taxa de entrega e a latência observadas não seguiram um padrão esperado. Concluiu-se que em plataformas com baixa capacidade de transferência,

um nó atacante não causará grandes danos caso seu poder computacional não seja superior ao dos nós legítimos. Neste caso, o fato de sincronia de envios entre os nós atacante e legítimo é um fator que compromete muito mais a taxa de entrega do que a potência de transmissão utilizada pelo nó atacante. Por fim, o simulador Avrora foi utilizado para verificar e confirmar a hipótese de que a sincronia entre os envios é um fator mais importante do que a potência de transmissão utilizada pelo nó atacante.

Desta forma, futuros trabalhos que venham a considerar ataques *jamming* em redes de sensores sem fio devem ser cautelosos para que seus resultados sejam coerentes com o mundo real. Muitos simuladores operam com uma síncrona irreal, como é o caso do Avrora. Nestes, os resultados podem ser deteriorados pelas colisões de mensagens mais frequentes do que o comum.

Referências

Avrora (2008). http://compilers.cs.ucla.edu/avrora/. acesso: 10/03/2012.

CC2420 (2007). http://www.tinyos.net/tinyos-2.x/doc/html/tep126.html. acesso: 10/03/2012.

Chiang, J. T. and Hu, Y.-C. (2011). Cross-layer jamming detection and mitigation in wireless broadcast networks. *IEEE/ACM Trans. Netw.*, 19(1):286–298.

Hussain, A. and Saqib, N. A. (2011). Protocol aware shot-noise based radio frequency jamming method in 802.11 networks. In *IEEE WOCN*, pages 1–6.

Levis, P., Madden, S., Polastre, J., Szewczyk, R., Woo, A., Gay, D., Hill, J., Welsh, M., Brewer, E., and Culler, D. (2004). Tinyos: An operating system for sensor networks. In *in Ambient Intelligence*. Springer Verlag.

Martinovic, I., Pichota, P., and Schmitt, J. B. (2009). *Jamming for good: a fresh approach to authentic communication in WSNs*, pages 161–168. Proceedings of the Second ACM Conference on Wireless Network Security.

MicaZ. http://www.openautomation.net/uploadsproductos/micaz_datasheet.pdf. acesso: 10/03/2012.

Mpitziopoulos, A., Gavalas, D., Konstantopoulos, C., and Pantziou, G. (2009). A survey on jamming attacks and countermeasures in wsns. *IEEE Communications Surveys & Tutorials*, 11(4):42 – 56.

Ramya, C., Shanmugaraj, M., and Prabakaran, R. (2011). Study on zigbee technology. *3rd International Conference on Electronics Computer Technology (ICECT)*, 6:297 – 301.

Sang, L. and Arora, A. (2009). Capabilities of low-power wireless jammers. In *IEEE INFOCOM*, pages 2551–2555.

Werner-Allen, G., Lorincz, K., Johnson, J., Lees, J., and Welsh, M. (2006). Fidelity and yield in a volcano monitoring sensor network. In *Proceedings of the 7th symposium on Operating systems design and implementation*, OSDI '06, pages 381–396, Berkeley, CA, USA. USENIX Association.

Xu, W. (2007). On adjusting power to defend wireless networks from jamming. In *Proceedings of the 2007 Fourth Annual International Conference on Mobile and Ubiquitous Systems: Networking&Services (MobiQuitous)*, MOBIQUITOUS '07, pages 1–6, Washington, DC, USA. IEEE Computer Society.

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*, MobiHoc '05, pages 46–57, New York, NY, USA. ACM.