O Impacto do Ataque Hello no Protocolo de Roteamento RPL

Estefânia Pianoski, Jeferson Cotrim e João Henrique Kleinschmidt

***Resumo*— A Internet das Coisas (IoT) tem atraído a atenção nos últimos anos, tanto da área acadêmica quanto do mundo dos negócios. Porém para o funcionamento da IoT foi necessário o desenvolvimento de novos protocolos, dentre eles o protocolo de roteamento RPL. Este protocolo atende as demandas das redes de baixa potência e com perdas, sendo também, até o momento o único protocolo de roteamento padronizado para IoT. Apesar da grande aceitação do RPL, este ainda apresenta algumas deficiências que precisam ser sanadas, dentre elas diversas questões associadas à segurança da informação. O objetivo deste trabalho é avaliar o impacto de um ataque *Hello* no desempenho do RPL. Os testes foram realizados com o *Contiki/Cooja* e as métricas avaliadas foram o consumo de energia dos nós, a taxa de entrega e atraso de pacotes de dados. Com os resultados obtidos foi possível identificar que o ataque *Hello* no RPL pode gerar uma negação de serviço, seja pelo esgotamento da energia dos nós da rede ou pela diminuição da entrega de pacotes.**

***Palavras-Chave*— Internet das Coisas, RPL, Ataque *Hello*, Segurança da Informação.**

***Abstract*— The Internet of Things (IoT) has attracted attention in recent years, both in the academic area and in the business world. However, for the operation of IoT, it was necessary to develop new protocols, among them the RPL routing protocol. This protocol meets the demands of low power and lossy networks and is the only standardized routing protocol for IoT. Despite the great acceptance of RPL, it still presents some deficiencies that are needed to be solved, such as severall issues associated with information security. The objective of this work is to evaluate the impact of a Hello attack on RPL performance. The tests were performed using Contiki/Cooja and the metrics evaluated were the nodes energy consumption, the packet delivery rate and the delay of data packets. With the obtained results it was possible to identify that the Hello attack in the RPL can generate a denial of service, either by the depletion of the energy of the nodes or by the decrease of the packets delivery.**

***Keywords*— Internet of Things, RPL, Hello Attack, Information Security.**

I. INTRODUÇÃO

Com o surgimento da Internet das Coisas, IoT (do inglês *Internet of Things*), pesquisas relatam que até o ano de 2020 o número de dispositivos conectados chegará a 50 bilhões [1]. A IoT tem possibilidades de avanços em diversas áreas, que vão desde monitoramento e sensoriamento, transporte, saúde, militar, até uso social. Pensando nesse novo cenário, e nas limitações dos dispositivos que irão compor essas redes, diversos novos protocolos de comunicação foram desenvolvidos, dentre eles o RPL (*IPv6 Routing Protocol for Low-power and Lossy Network*). O RPL foi desenvolvido pelo IETF (*Internet Engineering Task Force*), para fazer o roteamento em uma rede de baixa potência e com perdas (LLNs, do inglês *Low power and Lossy Networks*) [2] [3].

Estefânia Pianoski, Jeferson Rodrigues Cotrim e João Henrique Kleinschmidt Centro de Engenharia, Modelagem e Ciências Sociais Aplicadas, Universidade Federal do ABC, Santo André - SP, Brasil, E-mails: estefania.pianoski@ufabc.edu.br, jeferson.cotrim@ufabc.edu.br, joao.kleinschmidt@ufabc.edu.br.

O RPL é um protocolo que poderá atender diversos cenários IoT, com isso é importante estudar as questões de segurança da informação para garantir a confidencialidade, integridade e disponibilidade das informações. Se tratando da camada de roteamento um ataque pode causar diversos danos a informação, entre eles uma negação de serviço, deixando as informações indisponíveis a quem é de direito. As características intrínsecas do RPL fazem com que protocolo apresente vulnerabilidades como, por exemplo, o ingresso de nós na rede sem autenticação, possibilitando diferentes tipos de ataques na camada de rede [4]. Diversos trabalhos estudam ataques ao RPL, como ataques de rank, *wormhole* ou *Sybil*, mas não fazem uma análise de ataques de inundação, como o ataque *Hello* [4] [5] [6] [7] [8].

Sendo assim, o objetivo deste trabalho é estudar o desempenho do RPL em um ataque *Hello*. Nesse tipo de ataque um nó malicioso inunda a rede com o envio sucessivo de mensagens, sejam estas mensagens de controle ou mesmo de dados [9]. No caso específico do RPL, o ataque *Hello* é feito com a utilização das mensagens de controle do protocolo[5]. As simulações para o desenvolvimento deste trabalho foram feitas no sistema operacional Contiki com a utilização do simulador COOJA [10]. As métricas avaliadas foram o consumo de energia dos nós, o atraso e a taxa de entrega de pacotes de dados. Essas métricas permitem avaliar o efeito do ataque no desempenho da rede, que por consequência permite o entendimento dos efeitos do ataque no que diz respeito a segurança da informação.

Este artigo está organizado da seguinte forma: na seção II é feita a descrição do RPL. A seção III mostra os possíveis ataques e as vulnerabilidades em uma rede RPL. A seção IV mostra os resultados dos testes realizados com ataque *Hello* e a última seção faz as conclusões do artigo.

II. RPL

O RPL é um protocolo de vetor de distância, projetado para redes de baixa potência e com perdas, baseado em teoria de grafos acíclicos direcionados formando uma DAG (*Directed Acyclic Graph*), mais especificamente uma DAG orientada a destino formando uma DODAG (*Destinatin-Oriented Directed Acyclic Graph*). Dessa forma os dados são direcionados para um nó específico da rede conhecido como nó raiz. As men-

sagens de controle utilizadas pelo RPL são descritas abaixo [3]:

- DIO (*DODAG Information Object*): É utilizada para definir e atualizar as rotas da rede. Esta mensagem carrega os parâmetros de configuração da rede, incluindo o *rank* e a OF, do inglês (do inglês *Objective Function*).
- DAO (*Destination Advertisement Object*): Esta mensagem é enviada para o nó raiz pelos demais nós da rede com o objetivo de informar ao nó raiz a posição de cada nó na rede. A mensagem DAO pode requisitar uma confirmação de recebimento, o DAO-ACK.
- DIS (*DOGAG Information Solicitation*): Esta mensagem é utilizada por um nó que deseja ingressar na rede. O nó que recebe uma mensagem DIS responde a ela com o DIO.

Para formar o DODAG, inicialmente o nó raiz envia uma mensagem DIO aos demais nós da rede, a qual é composta por diversas informação sendo as mais importantes o *rank* e a OF que será utilizada nesta rede. A OF é um algoritmo que, com base em métricas definidas pelo desenvolvedor da rede, irá definir o *rank* de cada nó dentro da rede. O *rank* representa a distância lógica entre um nó e o nó raiz, sendo assim o nó raiz sempre terá o menor valor de *rank* da rede. Um nó recebe diversas mensagens DIO dos seus vizinhos, e escolhe para si um ”pai preferido”, que é o nó que informou o menor valor de *rank* e que será utilizado para encaminhar os dados. Com base no *rank* do pai preferido e a OF, o nó calcula para si um valor de *rank* e difunde uma mensagem DIO [11]. Após todos os nós terem recebido e enviado as mensagens DIO, estes enviam para o nó raiz uma mensagem DAO, de modo a informar ao nó raiz a posição de cada nó na rede [12]. O tempo de atualização da rede é controlado pelo algoritmo *Trickle Timer*, que aumenta o intervalo entre mensagens de controle caso não haja nenhum evento na rede [13]. Caso a rede passe por alguma alteração o valor do *Trickle Timer* volta para o mínimo.

III. Seguranca no RPL

As características do protocolo RPL o torna vulnerável a ataques, seja de ataques já conhecidos em outros protocolos de roteamento, como *black hole*, *wormhole* ou *Sybil*, até ataques que exploram vulnerabilidades específicas do protocolo, como o ataque de *rank* [6] [4].

Ataques ao RPL podem gerar danos em uma rede, por exemplo, interceptar os pacotes da rede, monitorar as ações de um usuário e até gerar uma negação de serviço DoS (do inglês *Denial of Service*), tornando a rede inacessível. Em uma ataque *Sybil*, um nó ingressa na rede com identidade falsa e pode ser utilizado com outros ataques na mesma rede. Em [6] esse ataque foi testado em uma rede RPL com mobilidade. O nó malicioso se move na rede para analisar o impacto desse ataque no desempenho da rede. Os resultados mostraram que esse tipo de ataque pode facilmente derrubar a rede, assim como aumentar o consumo de energia, reduzir a taxa de entrega dos pacotes e aumentar as mensagens de controle. Outro ataque que ocorre na camada de rede é o *wormhole*, que faz com que uma grande quantidade de mensagens usem as rotas estabelecidas entre os nós atacantes. Este ataque foi analisado em [7], sendo proposta uma solução de autenticação dos nós baseado em árvore *Merkle*.

Em [8] foi analisado o impacto de um ataque de *rank*, o qual atribuiu aos nós maliciosos o maior valor de *rank*, em seguida analisou o desempenho da rede. O desempenho da rede foi prejudicado, sendo que o ataque é mais efetivo em determinados pontos da rede. Estas características de posição do ataque foram utilizadas para propor soluções de segurança, através de níveis de paramêtros e monitoramento da rede. Ainda no ataque de *rank*, um nó malicioso pode receber o menor valor de *rank* diante dos demais nós da rede, tornando se o pai preferido dos demais nós, podendo então decidir se envia ou não os pacotes transmitidos na rede. Logo, o ataque de *rank* pode causar um buraco negro na rede deixando de transmitir os pacotes que passam por um nó malicioso.

Os protocolos de roteamento podem usar uma mensagem de *Hello* para anunciar um novo nó na rede, que é enviada aos nós vizinhos [4] [9]. Um nó mal intencionado pode utilizar essa mensagem *Hello* para ingressar, formar uma nova rota, ou inundar a rede com mensagens. Esse ataque foi escolhido como objeto de estudo por ser um ataque comum em redes de sensores sem fio e IoT e não ter sido analisado para o protocolo RPL. No ataque proposto, será utilizada a mensagem DIO como o ataque *Hello*, em que um nó malicioso ingressa na rede e começa a enviar mensagens DIO a todo momento. O tempo de espera entre uma mensagem e outra é apenas o tempo de processamento. A implementação do ataque faz com que o nó malicioso mande mensagens DIO aos demais nós vizinhos sem respeitar o algoritmo *Trickle Timer*. Sempre que o nó malicioso enviar uma mensagem DIO irá receber uma mensagem de resposta dos nós vizinhos, causando uma sobrecarga de mensagens e inundando a rede. Isto pode causar uma negação de serviço e comprometer o desempenho da rede, aumentando o consumo de energia e diminuindo a taxa de entrega de pacotes.

IV. Cenário de testes

Para a avaliação do ataque *Hello* foi escolhido um cenário com os nós dispostos em forma de grade e espaçados em 40 metros, como pode ser visto na Fig 1. A rede é composta por 20 nós, mais um nó raiz posicionado no centro na topologia. Inicialmente, em cada cenário de teste, um dos nós assume o papel de nó malicioso. A escolha de qual nó seria o malicioso se baseou no número de saltos deste nó em relação ao nó raiz. Dessa maneira os nós escolhidos como nós maliciosos foram o 1, 2, 3 e 7, que possuem entre 1 e 4 saltos em relação ao nó raiz. Esses cenário com a presença de um único nó raiz tem como principal função a verificação do impacto da posição do nó malicioso no desempenho da rede. Posteriormente foram testados mais três cenários com um número maior de nós maliciosos. Dois cenários com dois nós maliciosos, sendo um com os nós 1 e 20, e outro com os nós 7 e 14. E o terceiro cenário com 5 nós maliciosos (1, 4, 9, 11 e 17).

As simulações foram feitas no COOJA, que é o simulador presente no sistema operacional Contiki [10]. Cada teste tem duração de 30 minutos e foi repetido 30 vezes. Os resultados

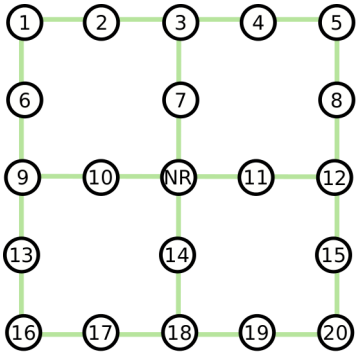

Fig. 1. Topologia de testes.

são apresentados com um intervalo de confiança de 95%. A taxa de transmissão dos nós é de um pacote de dados a cada 30 segundos e todos os nós enviam seus dados com destino ao nó raiz. O mote utilizado foi Sky mote, com *duty cycle* de 8 Hz.

O nó malicioso foi configurado para iniciar como um nó comum na rede e a partir de um determinado momento começar a agir de forma maliciosa. Isso faz com que o nó malicioso não interfira na criação do DODAG, mas somente após a formação da rede. A partir do momento que o nó malicioso inicia sua ação, o rádio deste fica ligado e ignora o *trickle timer*, fazendo com que o nó malicioso inunde a rede com menagens DIO.

V. Análise dos Resultados

A sessão de análise dos resultados será dividida pelas métricas que foram avaliadas. Em cada métrica serão apresentados separadamente os resultados para os ataques na presença de um nó malicioso e mais nós maliciosos. Serão apresentados também os resultados para uma rede sem a presença de nós maliciosos para comparação. Os resultados foram agrupados de acordo com o número de saltos de cada nó em relação ao nó raiz.

A. Taxa de Entrega de Pacotes

É possível observar pela Fig. 2 que sem a presença de nós maliciosos a taxa de entrega de pacotes, PDR (do inglês *Packet Delivery Ratio*), é de praticamente 100%. Conforme a posição do nó malicioso se aproxima do nó raiz o ataque fica mais eficiente, diminuindo a PDR dos nós mais afastados do nó raiz. Tomando como referência os dados do nó 7 atuando como malicioso, verifica-se que a PDR dos nós com mais de um salto em relação ao nó raiz cai para valores de até 50%. O nó malicioso impede que o nó atacado encaminhe as mensagens de dados dos demais nós, e as suas próprias, isto por que precisa processar as mensagens DIO enviadas pelo nó malicioso. Dessa forma, o nó malicioso tende a impedir o tráfego de todo o ramo que dependa dele para o encaminhamento de mensagens. Por conta da baixa PDR, a rede pode apresentar indisponibilidade aos usuários, prejudicando a segurança da informação. Além disso, as mensagens de controle também não são entregues e dessa forma um nó pode não receber resposta quando solicita seu ingresso na rede.

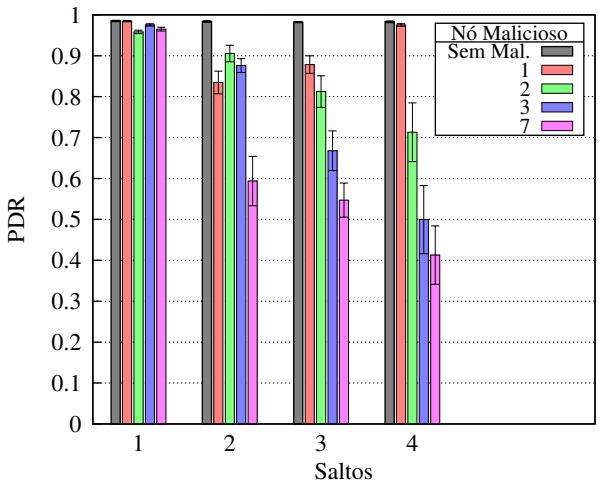

Fig. 2. PDR para um nó malicioso.

A Fig. 3 apresenta os resultados da PDR na presença de mais nós maliciosos. Para o ataque com os nós maliciosos 1 e 20, nas extremidades da rede, a perda passou a ser significativa a partir de 2 saltos com PDR de aproximadamente 65%. Os nós que estão a 4 saltos do nó raiz apresentam os piores valores de PDR com menos de 50% dos pacotes entregues, indicando assim que sofreram maior impacto em relação ao ataque. Quando o ataque é feito pelos nós 7 e 14, vizinhos ao nó raiz, a PDR dos nós mais afastados do nó raiz é praticamente nula, o que pode ser considerado um DoS. O aumento da quantidade de nós maliciosos na rede, também pode afetar a PDR, como foi visto com a presença de 5 nós maliciosos. Neste caso, apenas os nós com 1 salto do nó raiz obtiveram um valor satisfatório para a PDR, mas ainda sim muito baixo (30%), o que pode prejudicar aplicações mais sensíveis.

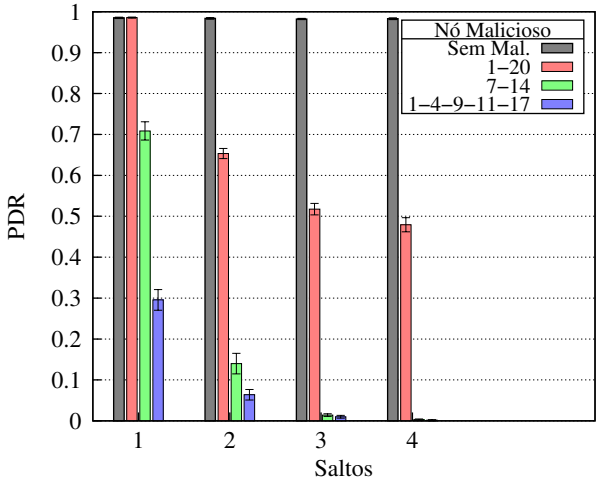

Fig. 3. PDR para vários nós maliciosos.

B. Atraso

A Fig. 4 mostra o atraso dos pacotes de dados, na presença de um nó malicioso. O resultado do cenário com nó malicioso, comparado a um cenário sem nó malicioso, mostrou que

a rede sofreu um atraso significativo, podendo levar a uma indisponibilidade da informação. O atraso aumenta conforme o nó malicioso está posicionado mais próximo ao nó raiz. O nó malicioso impede que seus vizinhos encaminhem os pacotes, já que estes precisam processar os pacotes DIO. Dessa forma, os nós diretamente atacados mantém consigo os pacotes de dados, aumentando assim o atraso. No pior cenário, o atraso ultrapassou 2 segundos, o que pode ser significativo para algumas aplicações.

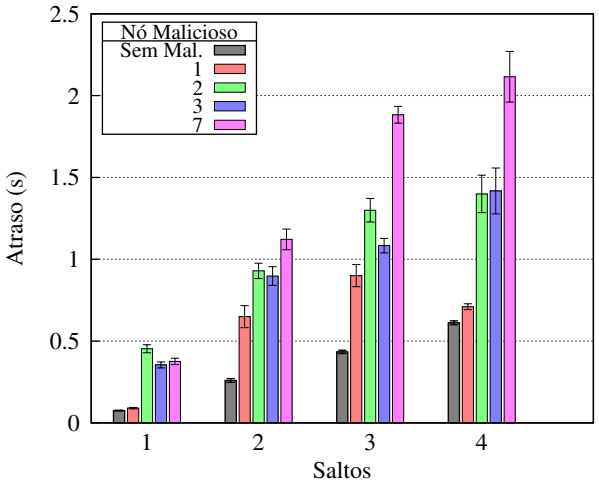

Fig. 4. Atraso para um nó malicioso.

A Fig. 5 mostra que aumentar a quantidade de nós maliciosos na rede, com posições próximas ao nó raiz, faz que o atraso aumente em até 10 vezes o seu valor em relação um cenário normal. Quando comparado o aumento da quantidade de nós maliciosos, com a posição que eles ocupam na rede, os resultados mostraram que o ataque dos nós 7 e 14 maliciosos afetam mais a rede do que o ataque com 5 nós maliciosos. Como pode ser visto, para 4 saltos tem o cenário mais crítico com um atraso maior que 10 segundos. Sendo assim a posição dos nós maliciosos influencia mais no atraso da rede do que a quantidade de nós maliciosos. Isto devido a rota percorrida pelos pacotes de dados até o nó raiz, ou seja, o nó malicioso associado ao nó raiz gera uma sobrecarga de mensagem naquele ramo da rede, aumentando o atraso quando comparado as outras posições ocupadas pelos nós maliciosos. Assim como ocorre com a PDR, mostrado na Fig. 3.

C. Consumo de Energia

A Fig. 6 apresenta o consumo de energia dos nós na presença de um nó malicioso. É possível observar que o nó malicioso faz com que seus vizinhos diretos consumam mais energia. Esse comportamento pode ser observado, por exemplo, em nós com 2 saltos, que apresentam elevado consumo de energia quando os nós maliciosos são o 2 e o 7. Apesar de os dados apresentados no gráfico estarem agrupados pelo número de saltos, o nó diretamente ligado ao nó malicioso é o que consome mais energia. É importante dizer também que a simples presença de um nó malicioso na rede eleva o consumo de energia de todos os nós, isso por conta do aumento do número de mensagens de controle trafegando na rede.

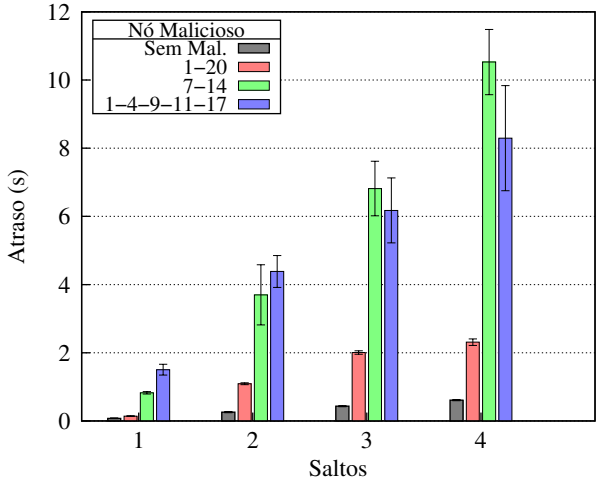

Fig. 5. Atraso para vários nós maliciosos.

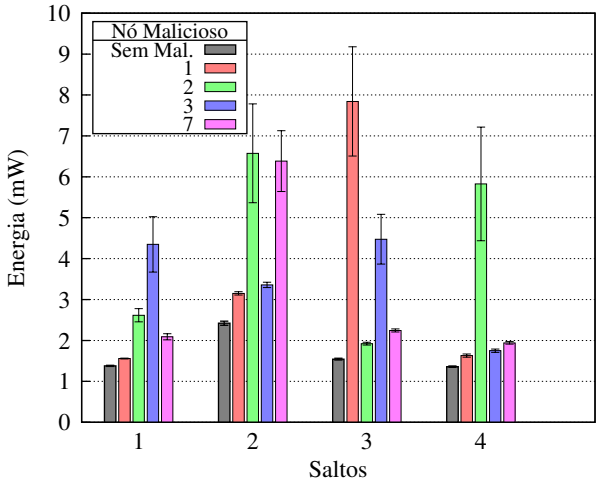

Fig. 6. Consumo de Energia para um nó malicioso.

A Fig. 7 mostra que, de maneira geral, um número maior de nós maliciosos na rede eleva o consumo de energia. Mas quando comparado um ataque com 2 nós maliciosos, a um ataque com 5 nós maliciosos, os resultados mostraram que 2 nós maliciosos em posições distintas para os casos com os nós de 3 e 4 saltos o consumo de energia foi superior ao ataque com 5 nós maliciosos.

D. Análise conjunta das métricas

TABELA I
TABELA COMPARATIVA ENTRE OS NÓS DIRETAMENTE E INDIRETAMENTE AFETADOS PELO NÓ MALICIOSO 7.

Métrica	**Nós**					
	2	**3**	**4**	**17**	**18**	**19**
Atraso (s)	3.13	0.67	1.54	1.57	1.37	1.58
PDR (%)	0.23	1.95	0.34	80.98	81.95	81.90
Energia (mW)	2.63	12.61	2.67	2.27	6.37	2.28

Para o ataque *Hello* os resultados mostram que o desempenho está diretamente relacionado a posição que o nó malicioso

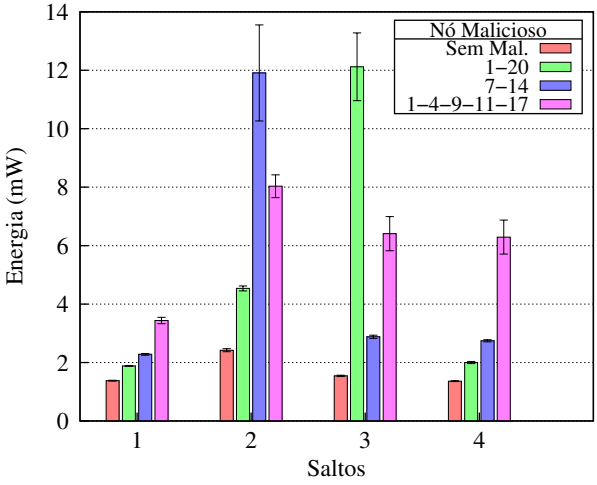

Fig. 7. Consumo de energia para vários nós maliciosos.

se encontra na topologia, como pode ser visto na Tabela I. Quando o nó malicioso está associado ao nó raiz e os demais nós o utilizam como rota para entrega dos pacotes, a PDR é prejudicada naquele determinado ramo da rede, como pode ser visto com os nós 2, 3 e 4, que utilizam o nó 7 malicioso como rota até o nó raiz. A PDR apresenta valores próximos a zero, causando assim um DoS, ou seja a sobrecarga das mensagens faz que pacotes de dados sejam perdidos. Tanto o atraso quanto o consumo de energia são em média maiores para o ramo onde o nó malicioso atua, porém, o ramo sem a atuação também é afetado, pois o nó raiz, neste caso, também está recebendo as mensagens DIO do nó malicioso. Dessa forma, o nó raiz está constantemente processando essas mensagens DIO, o que impede o recebimento imediato de mensagens dos demais nós. Isso aumenta o atraso e por consequência o consumo de energia, dado que os nós precisam manter seus rádios ligados mais tempo para que o nó raiz consiga receber essas mensagens.

VI. Conclusão

Neste artigo foi analisado o ataque *Hello* que explora algumas vulnerabilidades do protocolo RPL. Os resultados apresentados mostram como esse ataque pode prejudicar o desempenho da rede, podendo ser considerado um ataque DoS. Com nós posicionados em locais próximos ao nó raiz as chances de impactar de forma negativa as métricas de desempenho da rede aumentam. A inundação de pacotes DIO na rede pode fazer com que nós fiquem sobrecarregados, aumentando o atraso e diminuindo a entrega de pacotes. Além disso, o ataque faz com que os nós consumam mais energia, podendo levar a negação de serviço pelo esgotamento da bateria dos nós.

Com trabalhos futuros podem ser propostas soluções para minimizar os efeitos do ataque *Hello*, como mecanismos de autenticação e sistemas de detecção de intrusão (IDS). A autenticação pode ser usada para evitar que nós maliciosos ingressem na rede e um IDS pode identificar as ações de nós maliciosos, como a geração de tráfego acima de um determinado limiar.

Referências

[1] D. Evans, "The Internet of Things - How the Next Evolution of the Internet is Changing Everything," *CISCO white paper*, no. April, pp. 1–11, 2011.

[2] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497–1516, 2012.

[3] O. Gaddour and A. Koubâa, "RPL in a nutshell: A survey," *Computer Networks*, vol. 56, no. 14, pp. 3163–3178, 2012.

[4] P. Pongle and G. Chavan, "A survey: Attacks on RPL and 6LoWPAN in IoT," *2015 International Conference on Pervasive Computing: Advance Communication Technology and Application for Society, ICPC 2015*, vol. 00, no. c, pp. 0–5, 2015.

[5] L. Wallgren, S. Raza, and T. Voigt, "Routing Attacks and Countermeasures in the RPL-Based Internet of Things," *International Journal of Distributed Sensor Networks*, vol. 9, no. 8, p. 794326, aug 2013.

[6] F. Medjek, D. Tandjaoui, M. R. Abdmeziem, and N. Djedjig, "Analytical evaluation of the impacts of Sybil attacks against RPL under mobility," *12th International Symposium on Programming and Systems, ISPS 2015*, pp. 13–21, 2015.

[7] F. I. Khan, T. Shon, T. Lee, and K. Kim, "Wormhole attack prevention mechanism for RPL based LLN network," *International Conference on Ubiquitous and Future Networks, ICUFN*, pp. 149–154, 2013.

[8] A. Le, J. Loo, A. Lasebae, A. Vinel, Y. Chen, and M. Chai, "The impact of rank attack on network topology of routing protocol for low-power and lossy networks," *IEEE Sensors Journal*, vol. 13, no. 10, pp. 3685–3692, 2013.

[9] K. Saghar, D. Kendall, and A. Bouridane, "RAEED: A solution for hello flood attack," in *2015 12th International Bhurban Conference on Applied Sciences and Technology (IBCAST)*. IEEE, jan 2015, pp. 248–253.

[10] Sistema operacional contiki. [Online]. Available: www.contiki-os.org

[11] A. Dvir, T. Holczer, and L. Buttyan, "VeRA - Version number and rank authentication in RPL," *Proceedings - 8th IEEE International Conference on Mobile Ad-hoc and Sensor Systems, MASS 2011*, pp. 709–714, 2011.

[12] Q. Le, T. Ngo-Quynh, and T. Magedanz, "RPL-based multipath Routing Protocols for Internet of Things on Wireless Sensor Networks," *2014 International Conference on Advanced Technologies for Communications (ATC 2014)*, pp. 424–429, 2014.

[13] P. Levis, T. Clausen, J. Hui, O. Gnawali, and J. Ko, "RFC 6206 - The Trickle Algorithm," Tech. Rep., 2011.