Um Sistema de Detecção de Ataques Sinkhole sobre 6LoWPAN para Internet das Coisas

AUTORES:CHRISTIAN CERVANTES, DIEGO POPLADE, MICHELE NOGUEIRA, ALDRI SANTOS

APRESENTADOR:MÁRCIO LUÍS PETRY

Introdução

A IoT e uma rede híbrida, aberta e heterogênea que integra dispositivos inteligentes chamados de coisas (things);

Estes dispositivos compartilham informações, que expõem diversas vulnerabilidades na comunicação por apresentar uma infraestrutura variável e recursos computacionais limitados;

Introdução

A vulnerabilidade se apresenta em diversas formas sendo o *sinkhole*, um dos ataques de roteamento mais destrutivos para as redes sem fio;

Um dispositivo atacante *sinkhole* tem o objetivo de atrair a maior quantidade de trafego de uma certa área prejudicando um ponto de coleta de receber os dados enviados pelos nós.

Objetivo

Este trabalho propõe um sistema para identificar a presença de ataques *sinkhole* dentro do serviço de roteamento da IoT, chamado de **INTI** (Sistema de detecção de **I**ntrução de ataques *Si**N**khole* sobre 6LoWPAN para a Interne**T** das Co**I**sas).

O INTI visa prevenir, detectar e isolar os efeitos do ataque *sinkhole* no serviço de roteamento, e ao mesmo tempo mitigar os efeitos adversos.

Objetivo

O sistema combina o uso de *watchdog* com reputação e confiança dos nós, para a detectar ataques, por meio da analise do comportamento de cada nó.

Trabalhos relacionados

Diversas técnicas e mecanismos tem sido utilizados para detectar ataques *sinkhole*.

Esses **s**istemas de **d**etecção de **i**ntrusão (IDS) atenderem a maioria das características da IoT, mas

- não consideram a mobilidade e são muito restritos na análise do comportamento dos nós;
- possuem elevadas taxas de consumo de recursos e baixo desempenho.

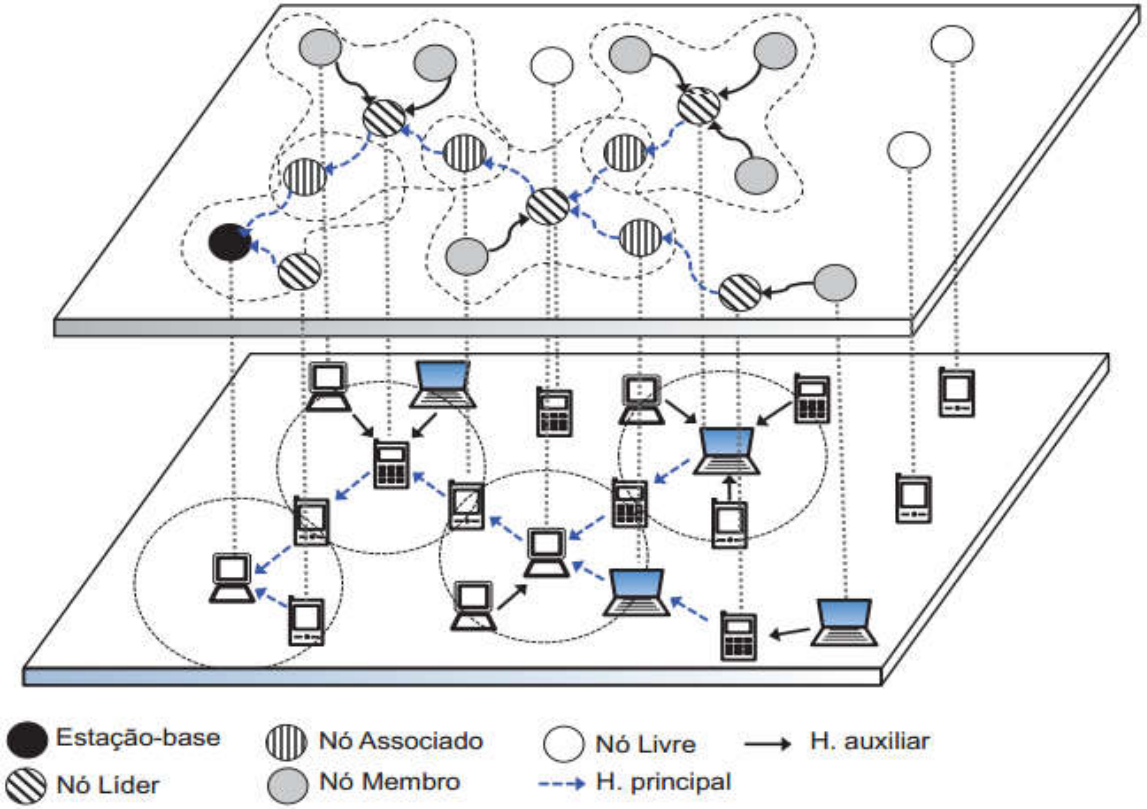
Modelo da IoT para o Sistema INTI

A **hierarquia principal** é a estrutura que permitira a comunicação entre os diferentes agrupamentos, nesta hierarquia só intervém os nós líderes, os nós associados e a estação-base como alvo.

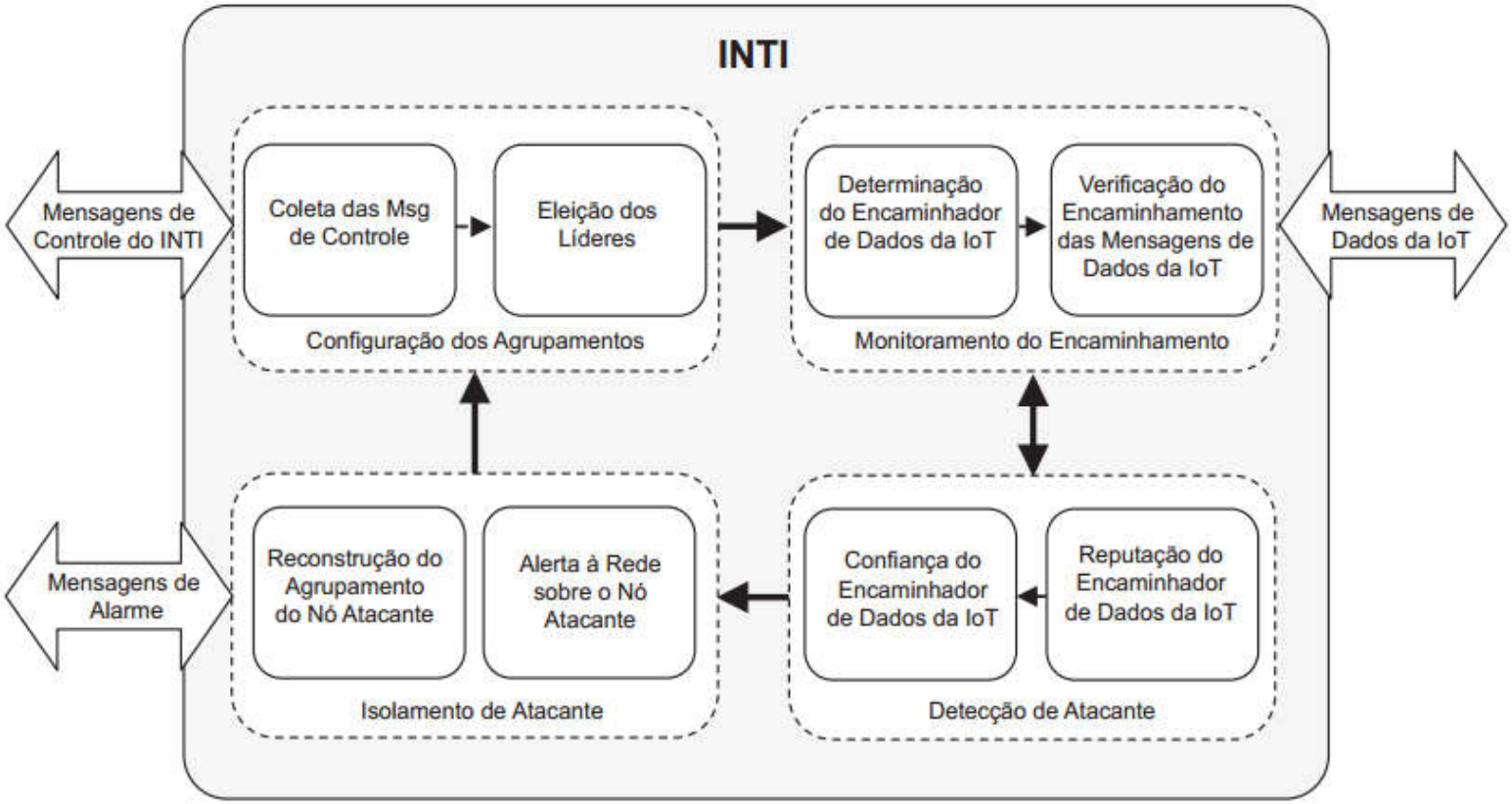
A **hierarquia auxiliar** compreende a comunicação de cada agrupamento realizado pelo nó líder e seus nós membros.

Modelo da IoT para o Sistema INTI

Os nós da rede são classificados como: nós membros, nós associados e líderes, conforme Figura:



Arquitetura do Sistema INTI



Arquitetura do Sistema INTI
Formação e restauração dos agrupamentos

- Inicialmente todos os nos da rede começam livres transmitindo e coletando dados de controle;
- Mensagem via *broadcast* estimam a quantidade de nós vizinhos para eleger os líderes.
- Os nós livres são classificados como nós líderes quando estes possuem a maior quantidade de nós vizinhos em relação aos outros. Após a eleição dos líderes, são definidos os agrupamentos.

Arquitetura do Sistema INTI
Formação e restauração dos agrupamentos

- A restauração do agrupamento acontece quando um dos nós falha, abandona o agrupamento ou quando ocorre um ataque *sinkhole*;
- Se um nó líder é afetado efetua-se uma nova eleição ou os nós membros afetados reagrupam-se em agrupamentos vizinhos.
- Se um nó associado é afetado existe a possibilidade de escolher outro no associado.

Arquitetura do Sistema INTI
Monitoramento do encaminhamento de dados

- Princípios de *watchdog* monitoram o numero de transições de entrada e saída realizadas por um nó;
- Se a quantidade de transmissões de entrada são iguais ao número de transmissões de saída o nó é considerado bom.
- Caso contrario, o componente assume que está acontecendo algum desvio do seu funcionamento normal.

Arquitetura do Sistema INTI
Detecção de ataque Sinkhole

A identidade do nó atacante é revelada realizando avaliações da reputação e confiança dos nós;

São calculas três predições: **i**ncerteza (i), **c**rença (c) **d**escrença (d) a partir de modelos matemáticos para representar a reputação.

Cada nó propaga seu status (St) sobre seu comportamento na transmissão de mensagens para o cálculo de sua reputação.

A reputação é um valor continuo dentro dos limites R[0,1], se o valor de um nó é maior ou igual 0,5 considera-se como um nó bom, caso contrario, é considerado um nó atacante.

Arquitetura do Sistema INTI
Isolamento do atacante

O módulo de isolamento faz com que o nó detectado seja isolado da rede.

Uma mensagem de alarme em *broadcast* com o ID do nó atacante é colocando na *blacklist* da estação-base.

O nó que detectou o ataque promove o isolamento do atacante enviando uma mensagem de restauração para seus vizinhos.

Arquitetura do Sistema INTI
Isolamento do atacante

Existem três formas de isolar um *sinkhole*:

(i) quando um nó *sinkhole* é um nó membro: este será isolado pelo nó líder;

(ii) quando o *sinkhole* assume a função de líder: os nós membros isolam o nó *sinkhole* ou caso exista um no associado este isola o *sinkhole*;

(iii) quando o nó *sinkhole* assume a função de nó associado, este será isolado pelo líder.

Avaliação do INTI

O sistema INTI foi implementado no simulador Cooja, SO de código aberto para sistemas embarcados e redes de sensores sem fio.

Para comparação também foi implementado o IDS SVELTE neste simulador. Para avaliar a eficácia e a eficiência dos sistemas .

O cenário é composto por 50 nós, alguns fixos e outros moveis, como celulares, PDAs, notebooks, que se movimentam em uma área delimitada.

Avaliação do INTI

Os resultados apresentados são a média de 35 simulações
As métricas utilizadas pelo sistema INTI são:

Taxa de detecção do ataque contabiliza os ataques identificados corretamente.

Taxa de falsos negativos indica a quantidade de vezes que o nó atacante foi considerado como confiável.

Taxa de falsos positivos determina a quantidade de vezes que o sistema detectou um ataque *sinkhole* sendo este negativo.

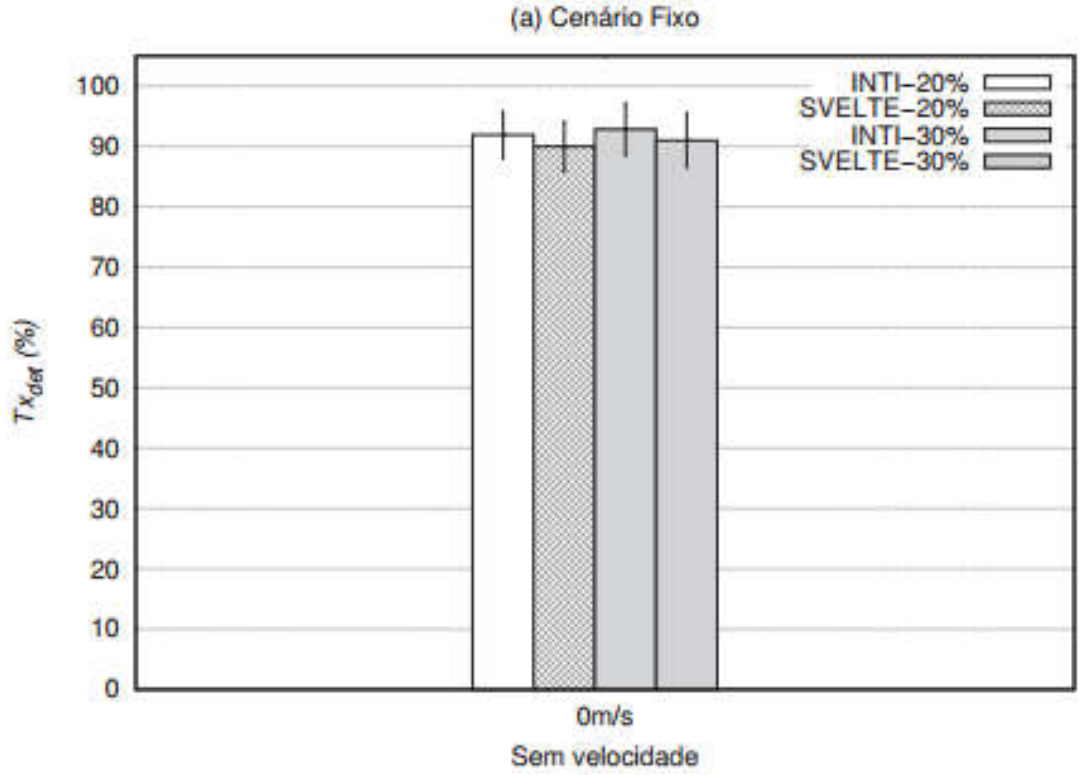
Consumo de energia indica o total do consumo de energia dos nós da rede durante a simulação.

Taxa de entrega de pacotes determina o total de pacotes de dados recebidos com sucesso.

Avaliação do INTI

Eficácia

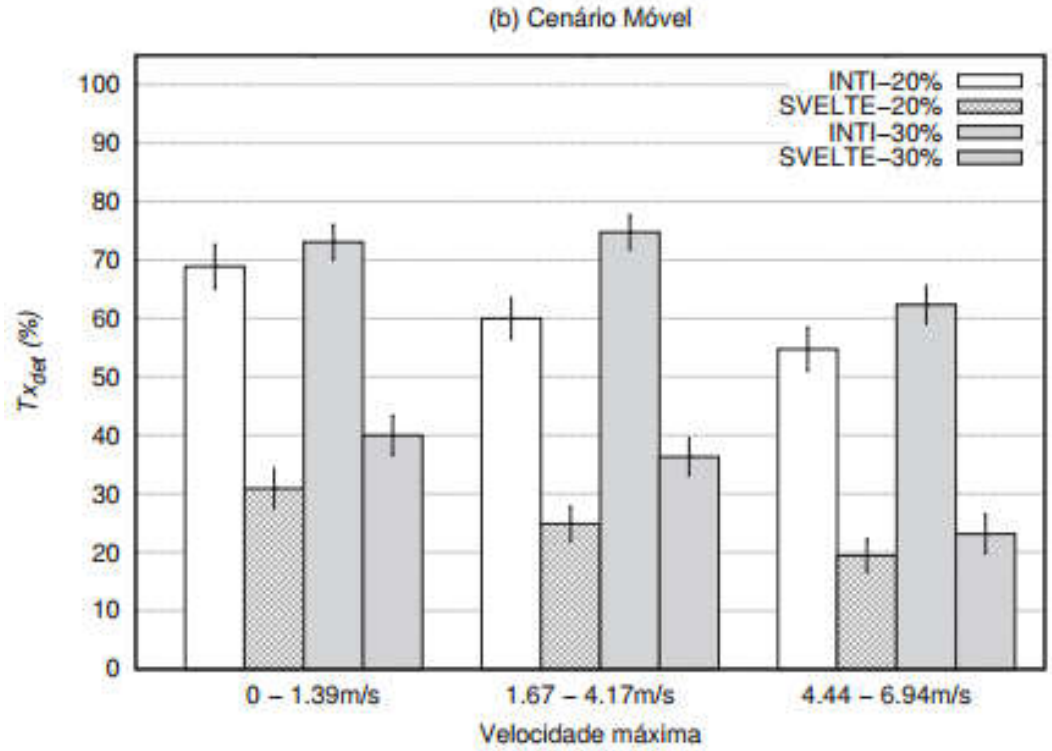
No cenário fixo, o INTI e o SVELTE apresentam praticamente uma igualdade (92% e 90% respetivamente) na detecção de ataques.



Avaliação do INTI

Eficácia

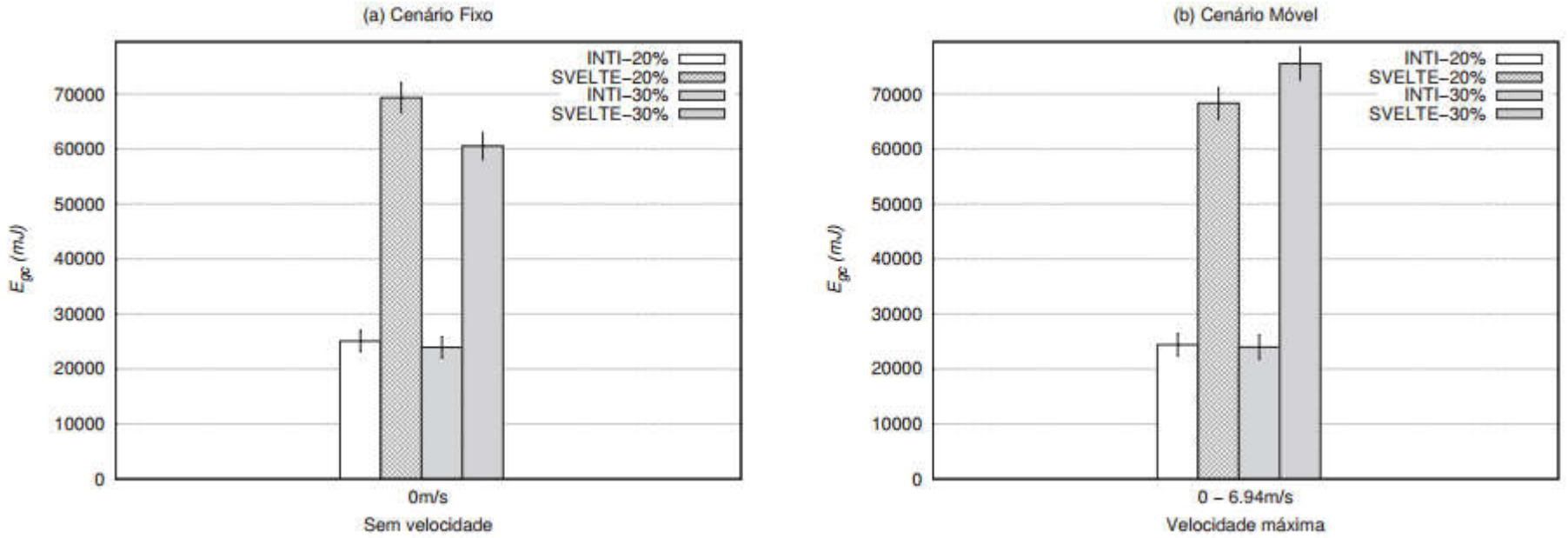
No cenário móvel a taxa de detecção do SVELTE diminuiu para 24% e a da INTI é superior a 70% por considerar a mobilidade dos nós.



Avaliação do INTI

Eficiência

As métricas da eficiência verificam o desempenho de acordo com o consumo de energia. O INTI permite a formação de agrupamentos para diminuir o consumo.



Conclusão

O INTI foi avaliado em um cenário realístico para o uso da IoT, alcançando uma taxa de detecção de ataques *sinkhole* de até 92% em um cenário com nós fixos e de 75% em um cenário com nós móveis.

Além disso, o INTI apresentou um baixo consumo de energia e uma baixa taxa de falsos positivos e negativos em relação ao SVELTE.

Como trabalhos futuros, pode se avaliar a eficácia do INTI na detecção de outros tipos de ataques que acontecem na IoT.

Referências

Atzori, L., Iera, A., and Morabito, G. (2010). The internet of things: A survey. volume 54, páginas 2787–2805, Catania, Italia. Elservier Science Publishers B. V.
Bannack, A., da Silva, E., Lima, M. N., dos Santos, A. L., and Albini, L. C. P. (2008). Segurança em redes ad hoc. Anais do XXVI Simpósio Brasileiro de Telecomunicações (SBRT), paginas 19–20.
Bellavista, P., Cardone, G., Corradi, A., and Foschini, L. (2013). Convergence of MANET and WSN in IoT urban scenarios. volume 13, paginas 3558–3567. IEEE.
Dunkels, A., Gronvall, B., and Voigt, T. (2004). Contiki-a lightweight and flexible operating system for tiny networked sensors. paginas 455–462. IEEE.
Gaddour, O. and Koubaa, A. (2012). RPL in a nutshell: A survey. páginas 3163–3178. Elsevier.
Ganeriwal, S., Balzano, L. K., and Srivastava, M. B. (2008). Reputation-based framework for high integrity sensor networks. ACM Transactions on Sensor Networks (TOSN), 4(3):15.
Jin Qi, Tang Hong, K. X. L. Q. (2012). Detection and defence of sinkhole attack in wireless sensor network. In ICCT-2012, paginas 809–813, Chengdu, China. IEEE Security.