

Utilização de Redes de Confiança para Detecção de Anomalias em RSSF

**Beatriz de A. Campos, Claudio M. de Farias e Luiz
Fernando R. da C. Carmo**
PPGI / UFRJ



Sumário

- Cenário de RSSF.
- Detecção de anomalias.
- Redes de Confiança.
- Proposta.
- Conclusões.

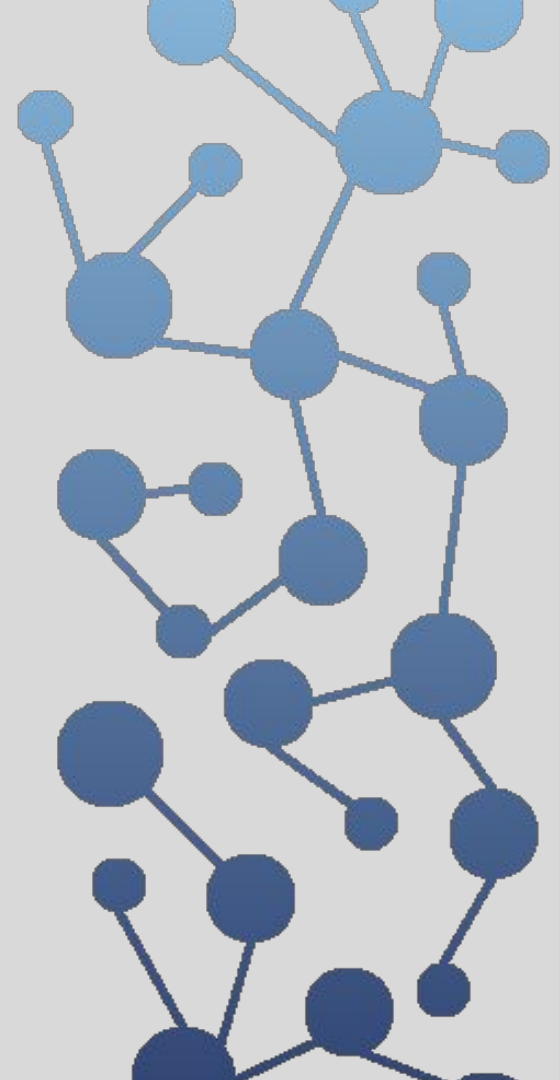
Redes de Sensores Sem Fio

- Uso médico e hospitalar.
- Monitoramento de ambientes.
- Aplicações em fazendas e indústrias.
- Uso em *Smart grids*.
- Etc.

Problemas relativos a RSSF

- Ataques maliciosos.
- Falta de energia, áreas de sombra.
- Fraudes.
- Problemas durante a medição.

Como saber
quando um nó
pode ser
considerado
comprometido?



Detecção de Anomalias

- Processo de identificação dos dados que:
 - Fogem do padrão esperado de coleta;
 - destoam do conjunto ao qual pertencem.

Causas de Anomalias

- Ataques maliciosos.
- Erros durante a medição.
- Eventos no ambiente, sejam eles temporários ou duradouros, previstos ou não.

Redes de Confiança

- São utilizadas para **expressar a relação entre duas partes** baseadas em **ocorrências positivas e negativas**.
 - + ocorrência **positiva** → + **confiança**
 - + ocorrência **negativa** → - **confiança**

Redes de Confiança

Gerenciamento de confiança pode ser utilizado para identificar comprometimento do nó.

Anomalias → **ocorrência negativa** → **queda de confiança**

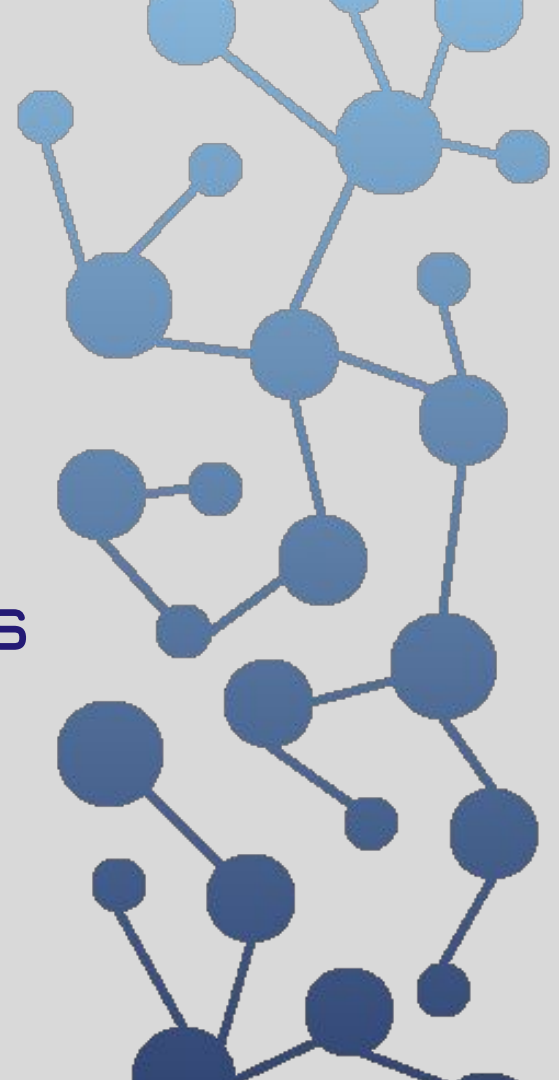
Lógica Subjetiva

- Lógica probabilística utilizada para calcular confiança entre duas partes, através de um valor de “**opinião**”.
- Uma opinião é uma quádrupla composta de: um valor para crença, um valor para descrença, um valor para incerteza e um valor de probabilidade de ocorrência.

Lógica Subjetiva

- Utiliza **ocorrências positivos e negativos** para calcular a opinião acerca dos nós.
- Possui um parâmetro de incerteza.
- **Possui uma proposta de consenso para unir duas “opiniões”.**

Propomos um método para
gerir a confiança dos nós de
uma RSSF, usando lógica
subjéctiva, baseado nos dados
provenientes destes nós.



Proposta

- Classificar os dados como anômalos ou não.
- Gerar uma opinião acerca dos dados recebidos.
- Agregar a opinião gerada com a opinião posterior.
- Enviar os dados dos nós, juntamente com suas respectivas opiniões, para outros pontos da rede (servidores).

Conclusão e trabalhos futuros

- O método deve ser implementado para fazer a validação do modelo proposto.
 - Ambiente simulado e real;
 - verificação do consumo de energia dispensado pelo nó.
- Espera-se que o valor da opinião expresse de forma coerente os tipos de ocorrências mais comuns do nó.
- A vantagem de utilizar redes de confiança juntamente com detecção de anomalias é agregar em um único valor a “memória” acerca de um dado nó.



Obrigada !



Contato

e-mail:

beatrizac@labnet.nce.ufrj.br

