

Compiler-Enabled Adaptive Security Monitoring on Networked Embedded Systems



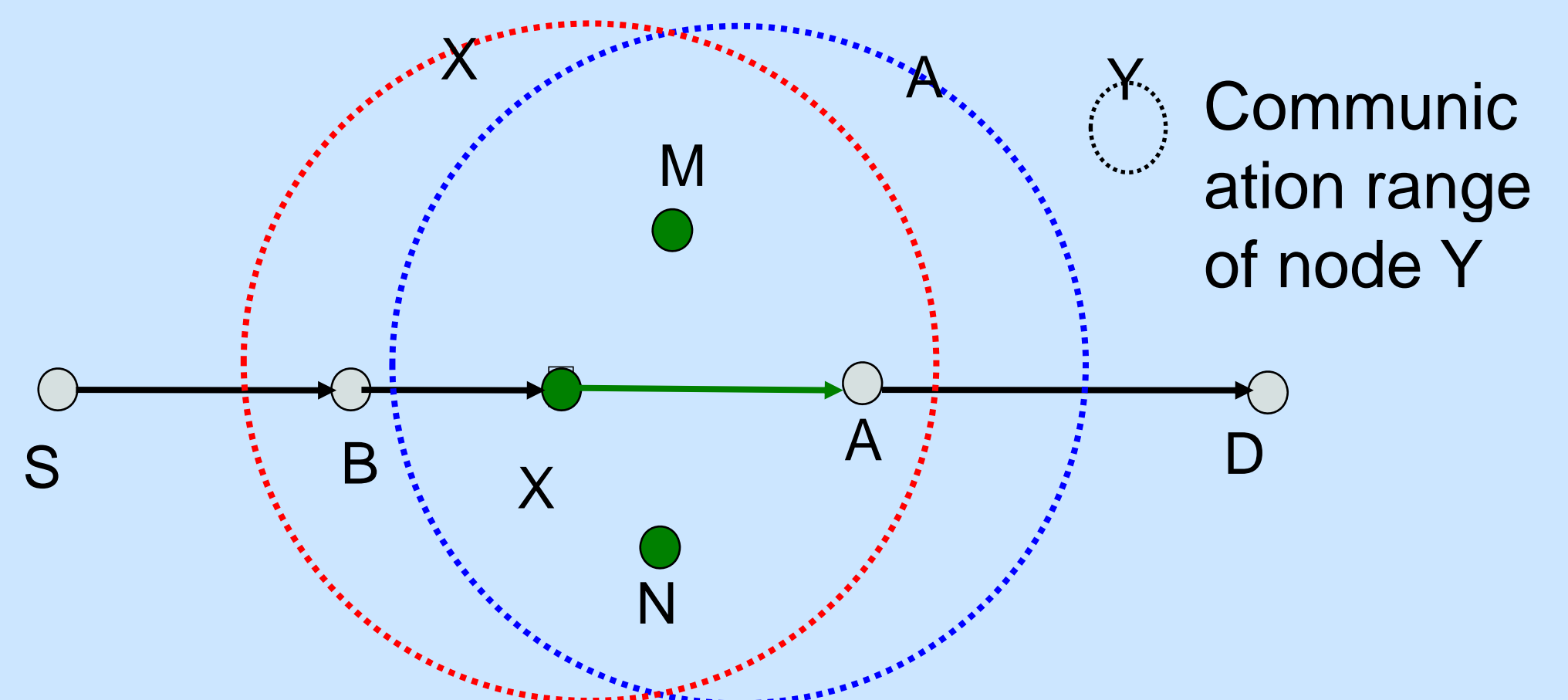
Saurabh Bagchi, Zhiyuan Li, Yung-Hsiang Lu, Purdue University
www.ece.purdue.edu/~sendor

Problem

Pervasive computing systems are open to tampering and security attacks. We need to find accurate and low resource demanding techniques for detecting successful attacks. They need to be easy to embed in applications and distributed in nature.

Approach

Monitoring mechanism whereby nodes oversee neighboring communication with their normal functionality. The monitoring is made adaptive to failure conditions and resource constraints. Distributed decision-making eliminates effect of compromised internal nodes.



M, N, and X act as guards of A for the communication X→A on the route from S to D

Approach and Impact

New approach

- Reaction to current security condition
- Security sensitive to resource availability
- High-level security directives

Research Impact

- Open but secure deployments of wireless networks
- Security through leveraging characteristics of wireless channel

Triggers for Activation of Levels of Security Protection

- Identify necessary conditions for successful security attacks
- Security attacks include data and control traffic attacks and physical compromise of node
- Necessary conditions act as triggers for more intensive monitoring

Compiler Tool for Embedding Security

- Declarative security specs from user
- Compiled into the functional code
- Multi-grade monitoring and defense operations are enabled
- Optimizes type and placement of monitoring operations
- Uses a repository of detection and defense mechanisms

