Bug Hunting in Sensor Network Applications

Raimondas Sasnauskas, Jó Ágila Bitsch Link, Muhammad Hamad Alizai, and Klaus Wehrle
The Need of WSN Application Testing

• Why is reliable WSN software difficult to create?
  ▶ Distributed and concurrent execution
  ▶ Faulty nodes
  ▶ Limited human interaction
  ▶ Severe resource constraints

• Issues with C language
  ▶ No dynamic type checking (type-unsafe)
  ▶ Misuse of union types
  ▶ Correct exception handling is a challenging task

Software bugs are difficult to avoid
Problems with wide-spread C checking tools

- Static code analysis only with limited C semantics
  - Poor code coverage
- Tight integration with the whole operating system
  - Tedious manual code modification before the actual testing
- No push-button technology with steep learning curve
  - In most cases, testing tools are not used at all

Fall back on manual code debugging techniques
Related Efforts

Main goal: memory safe executions at runtime

- **Safe TinyOS (SenSys’07)**
  - Limited automatic code instrumentation
  - Bug detection only eventually at runtime
  - Additional resource usage

- **2 papers at upcoming SenSys’08 conference**
  - *Declarative Tracepoints*: A Programmable and Application Independent Debugging System for Wireless Sensor Networks
  - *DustMiner*: Troubleshooting Interactive Complexity Bugs in Sensor Networks

Yet no solution for bug detection *before deployment*
KleeNet – bug detection *before deployment*

- **Klee (Cadar et al.)**
  - Symbolic execution tool for C programs
  - Symbolic input allowed to be “anything”
  - Detects memory reference errors
  - Automatic test case generation

```c
int main()
{
    unsigned i, t;
    unsigned a[4] = { 1, 3, 5, 2 };
    klee_make_symbolic(&i, sizeof(i));
    if(i >= 4)
        exit(0);
    char *p = (char*)a + i * 4;
    *p = *p - 1;
    t = a[*p];
}
```

```bash
$ klee test.o
KLEE: ERROR: memory error: out of bound pointer
```

```bash
$ BOutPrint.py klee-last/test000001.bout
-- klee-last/test000001.bout
Args: test.o
i[4]: '\x02'
```
Summary

- **Contribution**
  - Real bug detection tool for WSN applications before deployment
  - Prototype implementation for TinyOS

Goals achieved: usability, coverage, and integration

- **Ongoing work**
  - Extended implementation and evaluation
  - Addition of further useful checks in KleeNet
  - Integration into other OS’s
  - Distributed WSN testing
Thanks for your attention!