School of
Engineering and Computing Sciences

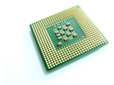
Implementation of GF(2^8) Operations and Multi-variate Key Pre-distribution Scheme

REU fellow(s): Cory Pruce[1], Faculty mentor: Dr. Farshid Delgosha[2], Affiliation: 1. Pitzer College, Claremont Consortium, Claremont, CA, 91711 2. School of Engineering and Computing Sciences, NYIT
School of Engineering and Computing Sciences, New York Institute of Technology, New York, NY 10023
Contact: cpruce@students.pitzer.edu, fdelgosh@nyit.edu

Abstract

• Mobile/temporary devices contain a myriad of advantages:
  • Efficiency doubles every ~18 months
  • Cost decreases overtime
  • Able to create a wireless network
  • Used ubiquitously for everyday tasks

01010111 01101001 01101011
01101001 01110000 01100101
01100100 01101001 01100001



• Disadvantages do exist, however:
  • Memory and network bandwidth constraints
  • Incapable of performing costly computations
  • Limited amount of energy
  • Large bit-size encryption implausible

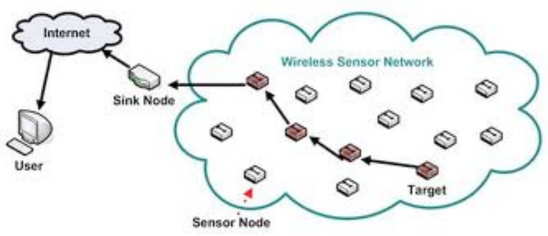
Introduction

• Hardware is more efficient/cheaper (<$50/GB of DDR3)
• Inexpensive, specialized devices becoming more pragmatic
• Innovations and breakthroughs have opened the doors to many possibilities for wireless networks

Galois Field(256)

• Elements of the finite field can conveniently be represented in a single byte:
  • Different implementations pertaining to hardware setup
  • Operations use either full-lookup tables, log tables, composite fields or a combination among the set
  • Unsigned char datatype is optimal because 1 byte is allocated as opposed to 4 bytes in the latest edition of the C language
  • Additionally, being unsigned, the span of the datatype is exactly GF(256)

Wireless Sensor Networks (WSN's)



• Used to observe and respond to environmental stimuli
• Applications include monitoring temperature, motion, sound, chemicals, illumination, etc.
• Often sensor nodes are required to be disposable and/or built on a micro-scale, forcing limitations and vulnerabilities

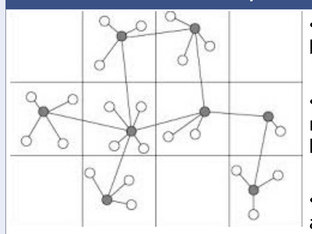
The Problem

• Security
  • Cryptosystems such as RSA too expensive
  • Easy to capture
  • Except for those not in the network, nodes have some indirect connection to sink
  • Leaks information about neighboring nodes
  • Can be masqueraded

• Limitations
  • Major computations processed by sink
  • Nodes designed for monitoring and communicating
  • Security is inversely proportional to performance
  • Only able to directly interact with neighbors

• Complete prevention of node capture is impractical, especially in a cost/size-conscious program:
  • Threshold secure
  • Dependent on ability to compromise polynomial shares

Multi-variate Key Pre-distribution Scheme



• Designed for network formed by resource limited devices

• Concept similar to "onion routing" in which each node has a layer of security

• Sink is relayed messages and applies appropriate response

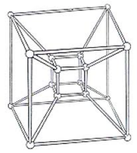
• Less storage and processing expense

• Provides verification among nodes

• Difficult to replicate

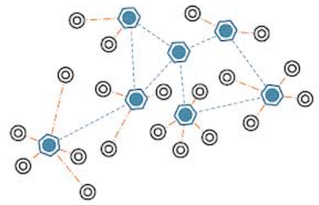
• Challenges
  • Security under constraints
  • Well-connected network
  • Uncovered areas
• Two phases of the protocol:
  • Setup phase
    • Computed in sink and distributed upon completion
  • Link-key Establishment phase
    • Performed between neighboring nodes

Setup Phase



• Sink generates d-dimensional hypercube:
1. Points are unique ID's
2. Distributed randomly among nodes

• ID's form network:
1. Each broadcasts ID
2. Nodes connect with those that are close in locality and identifier



• Sink also creates a set of symmetric d-variate polynomials:
1. Used in establishing link-keys
2. Most exponents pseudo-randomly generated

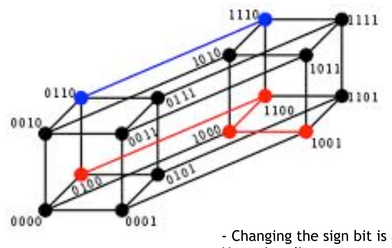
Link-Key Establishment Phase

• Nodes create a set of d univariate polynomials unique to its own ID

• Nodes having ID's with Hamming-distance one and are within communication range form a link-key

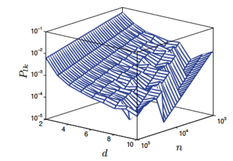
• Link-key established by evaluating d-variate polynomials

1	1	0	1	1	1	0	1
1	1	0	1	0	1	0	1
1	1	1	1	0	0	0	1
0	0	0	0	0	0	0	1
1	1	1	1	0	1	0	1
0	0	0	1	0	1	0	1
1	1	1	1	0	0	0	1
1	1	1	1	0	1	1	1



- Changing the sign bit is a conversion of Hamming-distance one

Network Connectivity

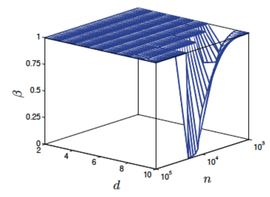


(a) Average probability of the link-key establishment.

• Optimal dimension d_{opt} of hypercube exists for n nodes

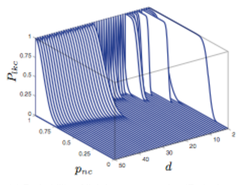
• Probability of link-key establishment decides approximate size of network

• Isolated nodes may exist



(b) Size of the largest component in the network normalized to the network size.

Resilience



(c) Probability of link-key compromise (P_{kc}) when n = 10, 000 and t = floor(50/(d-1)).

• Large threshold of captures required for link-key compromise

• Dependent on ability to recover polynomials from captured nodes

Conclusions

• Protocol is useful in networks of resource limited devices:
  • Practical
  • Small amount of captures won't compromise whole network
  • Node costs remain low
• Approach intentionally more appropriate to networks with simple detection and communication purposes

Acknowledgement

• Thanks to Dr. Ziqian Dong, Dr. Farshid Delgosha, REU Program Manager Dr. Marta Panero, NYIT Graduate Student Randy Espejo, and fellow REU participants for their helpful guidance and support. The project is funded by National Science Foundation Grant No.1263283 and New York Institute of Technology

References

[1] F. Delgosha: "Finite-field Arithmetic" Electrical Engineering and Computing Sciences New York Institute of Technology, 2009. New York NY.
[2] F. Delgosha, F. Fekri: "A Multivariate Key-Establishment Scheme for Wireless Sensor Networks." IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 8, NO. 4, APRIL 2009.