CERIAS

the center for education and research in information assurance and security

On the Practicality of Cryptographic Defenses against Pollution Attacks in Wireless Network Coding

Andrew Newell, Jing Dong, Cristina Nita-Rotaru

Abstract

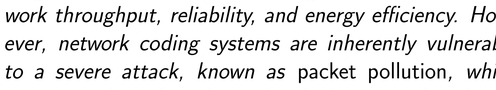
Network coding introduced a new paradigm for designing network protocols for multi-hop wireless networks. Numerous practical systems based on network coding have been proposed in recent years demonstrating the wide range of benefits of network coding such as increased network throughput, reliability, and energy efficiency. However, network coding systems are inherently vulnerable to a severe attack, known as packet pollution, *which presents a key obstacle to the deployment of such systems. Consequently, numerous schemes have been proposed to defend against pollution attacks. A major class of such defense mechanisms relies on cryptographic techniques.*

*We provide the first systematic evaluation of the existing cryptographic techniques for defending against pollution attacks. We first classify the cryptographic schemes based on their underlying cryptographic primitives (signature-based, hash-based, and MAC-based), security basis (DLP over a multiplicative group, DLP over an ECC group, and PRF), and security steps (*sign, verify, *and* combine*). Then, we define a unifying metric framework to compare the schemes. Lastly, we perform detailed analytical and experimental evaluations of a representative set of the schemes. Our results show that all of the schemes examined have serious limitations: They incur prohibitive computation overhead, high communication, or are insecure in the presence of multiple attackers. We conclude that while many cryptographic proposals for addressing pollution attacks exist, none of them are practical for use in wireless networks.*

1. Network Coding

Network coding:

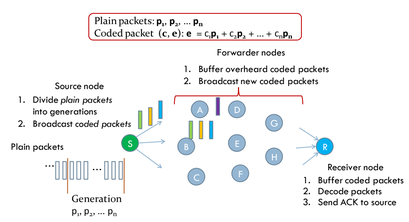
Traditionally forwarder nodes store-and-forward packets, but network coding allows these packets to be modified at forwarder nodes.



Tradional Network coding

Network coding in wireless:

The MORE protocol is an opportunistic routing protocol for wireless networks which utilizes intra-flow network coding.

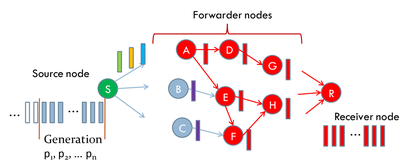


- Higher throughput
- Robustness
- Reliability
- Energy efficiency

2. Pollution Attacks

Pollution attack on MORE:

Node A is a byzantine adversary which injects invalid coded packets. Then, other honest nodes will mix their valid packets with the invalid packets and further pollute the network.



- Epidemic spreading
- Late discovery
- Cannot easily verify coded packets

3. Current Solutions

Taxonomy of cryptographic-based defense schemes:

These schemes supply forwarders with a verification mechanism.

Scheme	Type	Security basis
KFM[4]	Hash	DLP over $\mathbb{F}_p$
YWRG[6]	Signature	DLP over $\mathbb{F}_p$
ZKMH[7]	Signature	DLP over $\mathbb{F}_p$
LCL[5]	Signature	DLP over $\mathbb{F}_p$
CJL[3]	Signature	DLP over ECC
NCS_1[2]	Signature	DLP over ECC
HomoMac[1]	MAC	PRF

Homomorphic cryptography:

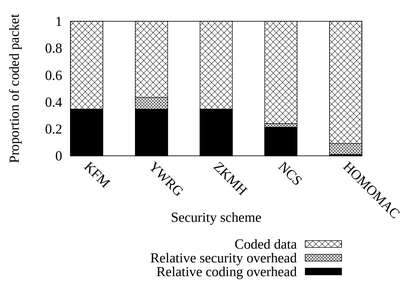
The cryptographic functions of these schemes are homomorphic to ensure coded packets can be verified.

$$\sigma(\alpha_1\mathbf{c}_1 + \alpha_2\mathbf{c}_2 +, ..., +\alpha_n\mathbf{c}_n) =$$
$$\alpha_1\sigma(\mathbf{c}_1) + \alpha_2\sigma(\mathbf{c}_2) + ... + \alpha_n\sigma(\mathbf{c}_n)$$

4. Analysis

Communication overhead:

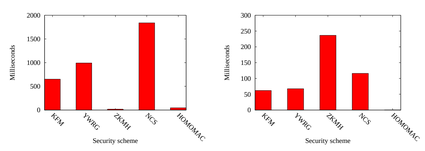
Defense schemes impose communication overhead through security payloads (hashes, signatures, or MACs) and large coding vectors.



- Large coding overhead
  - Upper-bounded coded packet size for wireless
  - Lower-bounded symbol size for security

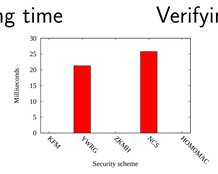
Computational overhead:

Additional computation required to compute security steps.



Signing time

Verifying time



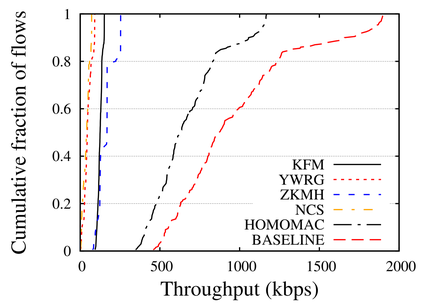
Combining time

- Large computational overhead
  - Modular exponentiations
  - ECC operations
  - Bilinear mappings

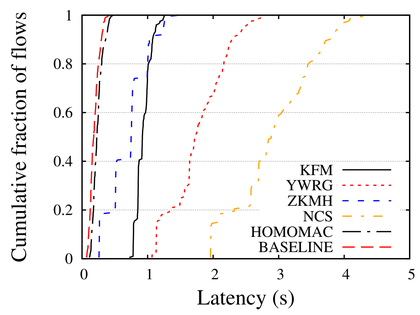
5. Evaluation

Simulations:

Simulation results under benign conditions of each security scheme applied to MORE along with a BASELINE case (no security scheme).



- HomoMac performs between 60%-75% of the baseline
- Other schemes perform less than 20% of the baseline



- Significantly higher latencies for schemes besides HomoMac

6. Multiple Byzantine Adversaries

Defense in the presence of multiple byzantine adversaries:

- HomoMac is the only scheme that is sensitive to multiple byzantine adversaries
  - Relies on special key-distribution
  - Number of adversaries must be known and bounded
  - Overhead increases drastically with more byzantine adversaries
- Other schemes provide same defense despite the number of byzantine adversaries

7. Conclusions

- Current cryptographic-based solutions are impractical in a wireless setting because they each have one of the following problems
  - High communication overhead due to large symbol sizes
  - High computational overhead due to costly operations
  - Poor security due to a weakness in the presence of multiple byzantine adversaries

References

[1] S. Agrawal and D. Boneh. Homomorphic macs: Mac-based integrity for network coding. In *ACNS*, 2009.

[2] D. Boneh, D. Freeman, J. Katz, and B. Waters. Signing a linear subspace: Signature schemes for network coding. In *Proc. of PKC '09*, 2009.

[3] D. Charles, Kamal Jain, and K. Lauter. Signatures for network coding. *40th Annual Conference on Information Sciences and Systems*, 2006.

[4] M. Krohn, M. Freedman, and D. Maziéres. On-the-fly verification of rateless erasure codes for efficient content distribution. In *SP'04*, 2004.

[5] Q. Li, D. Chiu, and J. Lui. On the practical and security issues of batch content distribution via network coding. In *ICNP*, 2006.

[6] Z. Yu, Y. Wei, B. Ramkumar, and Y. Guan. An efficient signature-based scheme for securing network coding against pollution attacks. In *IEEE INFOCOM*, 2008.

[7] F. Zhao, T. Kalker, M. Médard, and K. Han. Signatures of content distribution with network coding. In *IEEE*, 2007.

PURDUE UNIVERSITY

CERIAS

Discovery Park e-Enterprise Center