Institute of Operating Systems
and Computer Networks

Technische
Universität
Braunschweig

Forward Secure Delay-Tolerant Networking

Signe Rüsch, Dominik Schürmann, Rüdiger Kapitza, Lars Wolf

October 20, 2017

Motivation

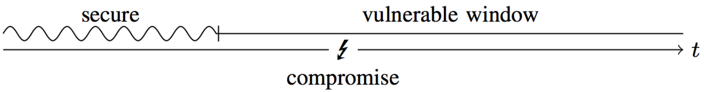
Delay-Tolerant Networks

- Communication for different kinds of environments
- Use store-carry-forward approach
- Bundle Protocol (BP):
  - End-to-end message-oriented overlay
- Bundle Security Protocol (BSP):
  - Defines bundle types for end-to-end and hop-to-hop security
  - Offers confidentiality, integrity, authenticity

Motivation

Forward Secrecy

- DTN communication vulnerable to attack:
  - Eavesdropping adversary records encrypted bundles
  - When key is leaked, then she can decrypt them
- Leakage highly probable due to exploits, design flaws, . . .
- FS provides protection of past communication up to certain time
- Difficult to achieve in asynchronous communication



(Unger et al., 2015)

Motivation

Forward Secrecy

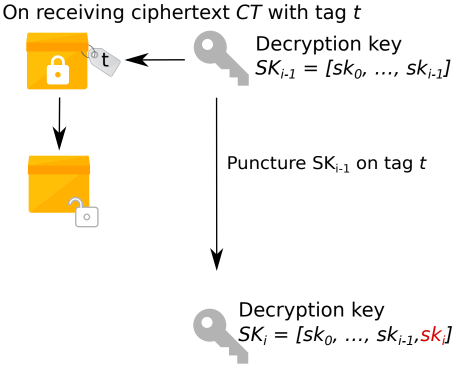
- Naïve countermeasure:
  - Encrypt each message with different ephemeral key
  - No common key for bundles
- But: complex key management, e. g. highly available infrastructure
- DTN includes highly mobile nodes, ad-hoc connections, . . .
- Proposed solution: use *Puncturable Encryption (FSE) Scheme*
  - M. D. Green and I. Miers, "Forward Secure Asynchronous Messaging from Puncturable Encryption", 2015

Puncturable Encryption

Approach

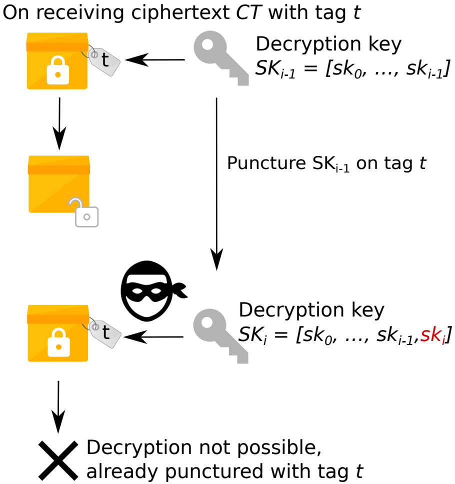
- Asymmetric encryption scheme
- Messages are encrypted with a *tag* and a *time interval* value
- Update private key:
  - Revoke decryption capabilities for certain messages
  - Based on tag or time value
  - No new key exchange required

Puncturing



Tags

Puncturing

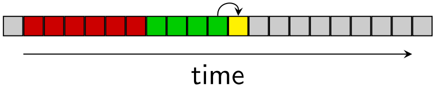


Tags

Puncturable Encryption

Key Forwarding *Time*

- Key lifetime is divided into time intervals
- Deriving new private key for a new interval
- Deleting interval key: remove decryption capabilities for this interval
- Buffer period: store keys for certain duration for late arrivals



Puncturable Encryption

Key Forwarding

- Decryption time and key storage cost (Green & Miers, 2015):
  - Grows with puncturing during interval
  - Linearly in number of messages received within time period
- Performed at start of each interval to “reset” the private key
- Duration of interval optimal with one message per interval

Forward Secure DTNs

Bundle Security Protocol

- No changes to bundle types
- Integrate FSE scheme as alternative cipher suite

Tags

- Every bundle should be unique in tag
- Decrypted only once by receiver, then punctured

→ Highest level of forward secrecy

- Hash of node's EID, timestamp, timestamp sequence number

Forward Secure DTNs

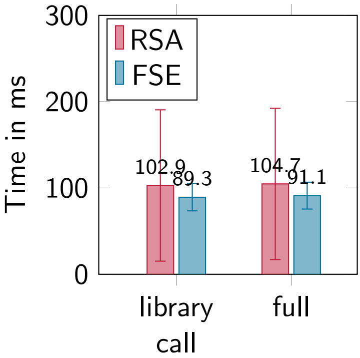
Parameters

- *n*: time interval length
- *d*: amount of time intervals
  - 2^{31} intervals supported by library (Green & Miers, 2015)
  - After this, new keys have to be exchanged
- *N*: interval keys *N* for buffer period

Microbenchmarks: Key Generation

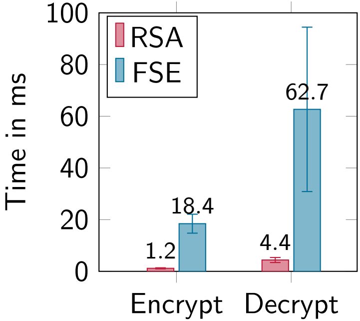
Evaluation

- `IBR-DTN:` `www.ibr.cs.tu-bs.de/projects/ibr-dtn`
- Dell OptiPlex 7010 Desktop-PC
- Intel Core i7-2770 CPU @ 4(8) x 3.4 GHz
- 16 GB RAM
- Ubuntu 14.04 LTS



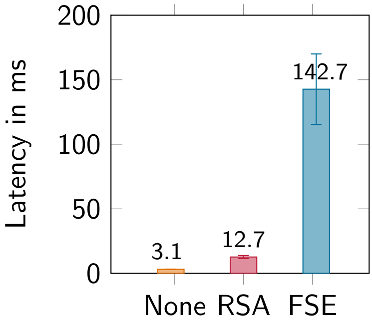
Microbenchmarks: Cryptographic Operations

- Puncturing included in decryption (18.6 ms)

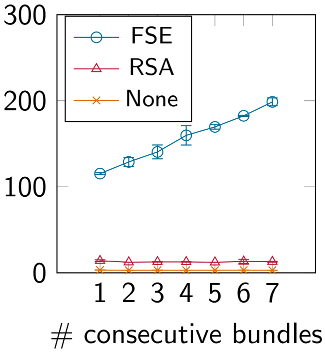


Microbenchmarks: Latency

- `dtnping`



(a) Latency introduced by FSE



(b) Latency during interval progression

FSE Parameters

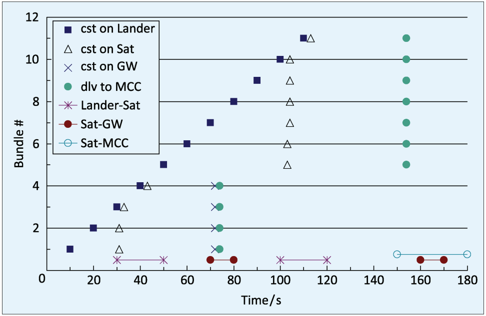
Scenarios

- Choice of parameters for FSE scheme in DTNs:
  - InterPlanetary network (Apollonio et al., 2013)
  - Rural village (Grasic & Lindgren, 2014)
  - Vehicular network (Doering et al., 2010)
- Chosen for varying delays and traffic loads
- Interval duration n: typically mean transmission time
- Buffer period: $N = \lceil \text{Max}/\text{Mean} \rceil + 1$

FSE Parameters

InterPlanetary Network

- Streaming scenario
- Moon lander sends bundles to Earth via multiple hops
- 5 kB bundles every 10 s
- Fully known contact plan of nodes
- Transmission time: mean ~ 124 s, max ~ 153 s



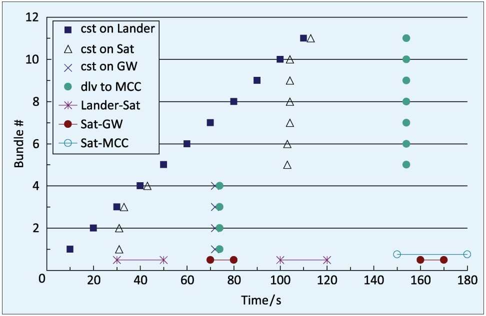
(Apollonio et al., 2013)

FSE Parameters

InterPlanetary Network

- Interval length $n = 124\,\mathrm{s}$
- $N = \lceil 153/124 \rceil + 1 = 3$
- $\sim 5 - 11$ bundles/interval

$\rightarrow$ decryption time
$\sim 170 - 250\mathrm{ms}/\mathrm{bundle}$

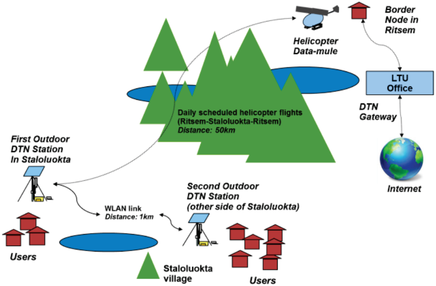


(Apollonio et al., 2013)

FSE Parameters

Rural Village

- Communication services to remote village
- Provided via data mule helicopter
- Direct connection to DTN Facebook, messaging
- 13 end-user nodes

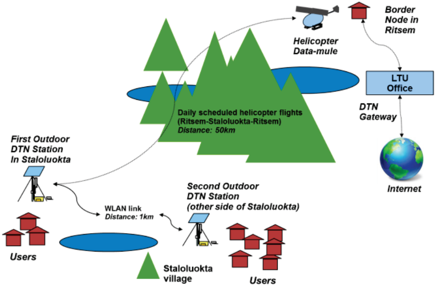


(Grasic & Lindgren, 2014)

FSE Parameters

Rural Village

- 115 bundles/day
  $\rightarrow$ 9 bundles/day/device
- Transmission time: mean $\sim$ 1 day, max $\sim$ 2 days
- Parameters:
  - $n = 1$ day
  - $N = \lceil 2/1 \rceil + 1 = 3$
- Decryption time $\sim$ 225 ms
  $\rightarrow$ acceptable performance

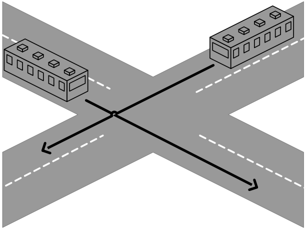


(Grasic & Lindgren, 2014)

FSE Parameters

Vehicular Networks

- Public transportation system
- 54 bus stops, 28 vehicles
- Vehicle positions, traffic information: ~ 2 bundles/s
- Routing algorithm RUTS: fixed network with high traffic
- Transmission time: mean $\sim 13\,\text{min}$, max $\sim 98\,\text{min}$

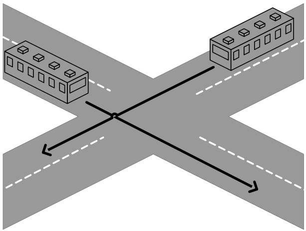


(Doering et al., 2010)

FSE Parameters

Vehicular Networks

- Parameters:
  - $n = 13\,\text{min}$
  - $N = \lceil 98/13 \rceil + 1 = 9$
  - 1560 bundles/interval
  - Decryption time $\sim 21.6\,\text{s}$

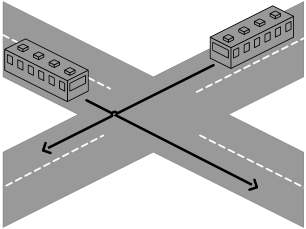


(Doering et al., 2010)

FSE Parameters

Vehicular Networks

- Parameters:
  - $n = 13\,\text{min}$
  - $N = \lceil 98/13 \rceil + 1 = 9$
  - 1560 bundles/interval
  - Decryption time $\sim 21.6\,\text{s}$
- Alternative parameters:
  - $n = 1\,\text{min}$
  - $N = 99$
  - 120 bundles/interval
  - Decryption time $\sim 1.8\,\text{s}$
- Trade-off: performance vs. memory usage → impractical!



(Doering et al., 2010)

Conclusion

Forward Secure Delay-Tolerant Networking

- DTN communication previously not forward secure
- Integrate FSE scheme by Green and Miers into `IBR-DTN`
- Ensures forward secrecy of bundles using puncturing
- Acceptable performance overhead, but high latency
- Remedy with suitable parameters, analyze scenario requirements

Conclusion

Forward Secure Delay-Tolerant Networking

- DTN communication previously not forward secure
- Integrate FSE scheme by Green and Miers into `IBR-DTN`
- Ensures forward secrecy of bundles using puncturing
- Acceptable performance overhead, but high latency
- Remedy with suitable parameters, analyze scenario requirements

Questions?

References I

P. Apollonio, C. Caini, and V. Fiore. "From the Far Side of the Moon: Delay/Disruption-Tolerant Networking Communications via Lunar". In: *China Communications* 10.10 (Oct. 2013), pp. 12–25. ISSN: 1673-5447.

R. Canetti, S. Halevi, and J. Katz. "A Forward-Secure Public-Key Encryption Scheme". In: *Advances in Cryptology — EUROCRYPT 2003. Proceedings*. Ed. by Eli Biham. Berlin, Heidelberg: Springer, 2003, pp. 255–271. ISBN: 978-3-540-39200-2.

References II

- M. Doering, T. Pögel, and L. Wolf. “DTN Routing in Urban Public Transport Systems”. In: *Proceedings of the 5th ACM Workshop on Challenged Networks*. CHANTS '10. Chicago, Illinois, USA: ACM, 2010, pp. 55–62. ISBN: 978-1-4503-0139-8.
- S. Grasic and A. Lindgren. “Revisiting a Remote Village Scenario and its DTN Routing Objective”. In: *Computer Communications* 48 (2014), pp. 133–140. ISSN: 0140-3664.
- M. D. Green and I. Miers. “Forward Secure Asynchronous Messaging from Puncturable Encryption”. In: *2015 IEEE Symposium on Security and Privacy*. May 2015, pp. 305–320.

References III

- F. Günther et al. "0-RTT Key Exchange with Full Forward Secrecy". In: *Advances in Cryptology - EUROCRYPT 2017. Proceedings, Part III*. Ed. by Jean-Sébastien Coron and Jesper Buus Nielsen. Cham: Springer, 2017, pp. 519–548. ISBN: 978-3-319-56617-7.
- I. Miers. *Libforwardsec. Forward Secure Encryption for Asynchronous Messaging*. 2015. URL: https://github.com/imichaelmiers/libforwardsec.
- R. Ostrovsky, A. Sahai, and B. Waters. "Attribute-Based Encryption with Non-Monotonic Access Structures". In: *ACM CCS '07*. 2007, pp. 195–203.

References IV

E. Rescorla. *The Transport Layer Security (TLS) Protocol Version 1.3*. https://tools.ietf.org/html/draft-ietf-tls-tls13-18. Mar. 2016.

S. Schildt et al. "IBR-DTN: A Lightweight, Modular and Highly Portable Bundle Protocol Implementation". In: *Electronic Communications of the EASST* 37 (Jan. 2011), pp. 1–11.

N. Unger et al. "SoK: Secure Messaging". In: *IEEE Symposium on Security and Privacy*. May 2015, pp. 232–249.

Backup Slides

Puncturable Encryption

Algorithms of FSE Scheme

- $KeyGen(1^d, k) \rightarrow (PK, SK_0)$
- $Encrypt(PK, M, t_1, \ldots, t_k) \rightarrow$ ciphertext CT
- $Decrypt(PK, SK_i, CT, t_1, \ldots, t_k) \rightarrow \{M\} \cup \{\perp\}$
- $Puncture(PK, SK_{i-1}, t) \rightarrow SK_i$
- $NextInterval(SK_n)$
- No signing or signature verification

Puncturable Encryption

Utilized Schemes

- FSE scheme combines two schemes:
  - PKE scheme with forward secrecy by Canetti, Halevi, and Katz
  - Non-Monotonic Attribute Based Encryption by Ostrovsky, Sahai, and Waters
- Private keys of both schemes cryptographically bound to each other

Puncturable Encryption

Synchronous Communication

- Online and interacting partners:
  - Use authenticated key exchange protocol (Diffie-Hellman)
  - Create new ephemeral keys for every connection
  - Used by OTR, TextSecure, ...
- Other naïve approach for asynchronous communication (Signal):
  - Key server for ephemeral pre-keys

Puncturable Encryption

Performance (Green & Miers, 2015)

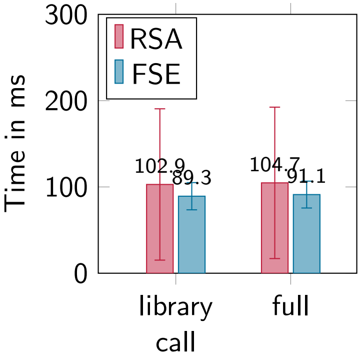
- Assume one message per interval for best performance
- Only encrypt symmetric key (AES256) $\rightarrow$ max. message size 32 B
- Puncture: 15.6 ms (initial), 9.8 ms (subsequent)
- Key forwarding: 50 ms
- Decryption: 13.8 ms
- Encryption: 5.49 ms
- Private key size: 14 kB – 890 kB, normally $<$ 50 kB

Puncturable Encryption

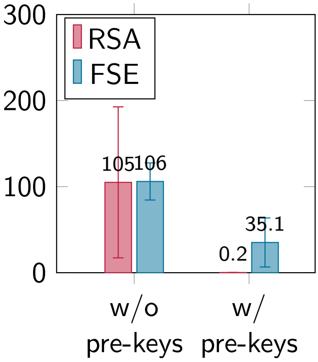
Puncturing & Key Forwarding

- Puncture: 18.6 ms
- Key forwarding: 15.5 ms

Microbenchmarks: Key Generation



(a) Key Generation



(b) Start-up time of `SecurityKeyManager`

FS-DTN

Buffer Period

- Assume bundles are delayed or dropped by attacker
- Corresponding decryption key is deleted after buffer period has passed

→ Forward secrecy is still provided

Related Work

- “0-RTT Key Exchange with Full Forward Secrecy” (Günther et al., 2017):
  - Reduce number of messages necessary for TLS key exchange
  - Uses puncturable encryption to provide forward secrecy to first RTT message