Problem Statement

Design a secure and efficient Non-Interactive, Hierarchical, Identity-based Key Agreement scheme for Mobile Ad-hoc Networks which is fully Resilient at each level against arbitrary number of node compromises.

Jargons

- **MANET**: An infrastructure-less and wireless network composed of mobile nodes
- **Key Agreement Protocol**: Allows two or more parties to agree on a shared secret key

Ad-hoc Networks

- MANETs find application in establishing Tactical Networks for Military
- Communication in disaster hit areas
- MANET nodes are constrained in:
  - Computational capabilities
  - Communication capabilities
- The nodes are usually mobile and have limited battery supply

HH-KAS

- Hybrid Hierarchical scheme (HH-KAS) was introduced for key agreement in MANETs by Gennaro et al. in 2008
- HH-KAS scheme comprises:
  - A one linear hierarchical key agreement scheme given by Sakai et al. at leaf level.
  - HH-KAS is fully resilient at leaf level and resilient up to a threshold at non-leaf levels

Tools

- Let $G_1, G_2, G_t$ be cyclic prime order groups then, pairing is an efficiently computable map $e: G_1 \times G_2 \rightarrow G_t$ which satisfies:
  - Bilinearity: $\forall a, b \in F_r, \forall P \in G_1, \forall Q \in G_2: e(PQ) = e(P, Q)^{ab}$
  - Non-degeneracy: $e(P, Q) \neq 1$
- Basic Id One way function scheme (BIOS) is a deterministic key pre-distribution (KPD) scheme introduced by Lee and Stinson
- BIOS achieves perfect resiliency and complete connectivity with fewer keys/node when compared to randomized KPD schemes.

References


BIOS-SOK Key Agreement Scheme

- **PKG** runs following three algorithms:
  1. Setup: Takes security parameter as input and outputs public parameters (params) and master secret key (msk)
  2. Extract: Uses msk and identities of nodes. PKG generates their secret keys
  3. Shared Key: Uses params, its own secret key and peer's identity. Node computes a shared key with the peer

Basic Id One-way Function Scheme

- $e(P, Q) \neq 1$
- $h$ is a one-way hash function
- $\mathbf{SOK}$
- $\mathbf{BIOS}$

SOK Key Agreement Scheme

Comparison of BIOS-SOK and HH-KAS

- **Non-Interactive**: Any two nodes can compute a shared secret key without any interaction
- **Identity-based**: To compute the shared secret key, a node only needs its own secret key and peer's identity
- **Hierarchical**: Intermediate nodes in the hierarchy can derive the secret keys for their children
- **Resilient**: The scheme is fully resilient against compromise of arbitrary number of nodes at each level
- **Efficient**: Compared to HH-KAS, BIOS-SOK is better in terms of computation time, space requirement and scalability

Properties

Problem Statement

Design a secure and efficient Non-Interactive, Hierarchical, Identity-based Key Agreement scheme for Mobile Ad-hoc Networks which is fully Resilient at each level against arbitrary number of node compromises.

Jargons

- **MANET**: An infrastructure-less and wireless network composed of mobile nodes
- **Key Agreement Protocol**: Allows two or more parties to agree on a shared secret key

Ad-hoc Networks

- MANETs find application in establishing Tactical Networks for Military
- Communication in disaster hit areas
- MANET nodes are constrained in:
  - Computational capabilities
  - Communication capabilities
- The nodes are usually mobile and have limited battery supply

HH-KAS

- Hybrid Hierarchical scheme (HH-KAS) was introduced for key agreement in MANETs by Gennaro et al. in 2008
- HH-KAS scheme comprises:
  - A linear hierarchical key agreement scheme given by Sakai et al. at leaf level.
  - HH-KAS is fully resilient at leaf level and resilient up to a threshold at non-leaf levels

Tools

- Let $G_1, G_2, G_t$ be cyclic prime order groups then, pairing is an efficiently computable map $e: G_1 \times G_2 \rightarrow G_t$ which satisfies:
  - Bilinearity: $\forall a, b \in F_r, \forall P \in G_1, \forall Q \in G_2: e(PQ) = e(P, Q)^{ab}$
  - Non-degeneracy: $e(P, Q) \neq 1$
- Basic Id One way function scheme (BIOS) is a deterministic key pre-distribution (KPD) scheme introduced by Lee and Stinson
- BIOS achieves perfect resiliency and complete connectivity with fewer keys/node when compared to randomized KPD schemes.

References


BIOS-SOK Key Agreement Scheme

- **PKG** runs following three algorithms:
  1. Setup: Takes security parameter as input and outputs public parameters (params) and master secret key (msk)
  2. Extract: Uses msk and identities of nodes. PKG generates their secret keys
  3. Shared Key: Uses params, its own secret key and peer's identity. Node computes its shared key with the peer

Basic Id One-way Function Scheme

- $e(P, Q) \neq 1$
- $h$ is a one-way hash function
- $\mathbf{SOK}$
- $\mathbf{BIOS}$

SOK Key Agreement Scheme

Comparison of BIOS-SOK and HH-KAS

- **Non-Interactive**: Any two nodes can compute a shared secret key without any interaction
- **Identity-based**: To compute the shared secret key, a node only needs its own secret key and peer's identity
- **Hierarchical**: Intermediate nodes in the hierarchy can derive the secret keys for their children
- **Resilient**: The scheme is fully resilient against compromise of arbitrary number of nodes at each level
- **Efficient**: Compared to HH-KAS, BIOS-SOK is better in terms of computation time, space requirement and scalability

Properties

Problem Statement

Design a secure and efficient Non-Interactive, Hierarchical, Identity-based Key Agreement scheme for Mobile Ad-hoc Networks which is fully Resilient at each level against arbitrary number of node compromises.

Jargons

- **MANET**: An infrastructure-less and wireless network composed of mobile nodes
- **Key Agreement Protocol**: Allows two or more parties to agree on a shared secret key

Ad-hoc Networks

- MANETs find application in establishing Tactical Networks for Military
- Communication in disaster hit areas
- MANET nodes are constrained in:
  - Computational capabilities
  - Communication capabilities
- The nodes are usually mobile and have limited battery supply

HH-KAS

- Hybrid Hierarchical scheme (HH-KAS) was introduced for key agreement in MANETs by Gennaro et al. in 2008
- HH-KAS scheme comprises:
  - A linear hierarchical key agreement scheme given by Sakai et al. at leaf level.
  - HH-KAS is fully resilient at leaf level and resilient up to a threshold at non-leaf levels

Tools

- Let $G_1, G_2, G_t$ be cyclic prime order groups then, pairing is an efficiently computable map $e: G_1 \times G_2 \rightarrow G_t$ which satisfies:
  - Bilinearity: $\forall a, b \in F_r, \forall P \in G_1, \forall Q \in G_2: e(PQ) = e(P, Q)^{ab}$
  - Non-degeneracy: $e(P, Q) \neq 1$
- Basic Id One way function scheme (BIOS) is a deterministic key pre-distribution (KPD) scheme introduced by Lee and Stinson
- BIOS achieves perfect resiliency and complete connectivity with fewer keys/node when compared to randomized KPD schemes.

References