# *Non-Interactive Hierarchical Id-based Key Agreement in MANETs*

Mayank Tiwari and Sanjit Chatterjee
Contact : [mayank.tiwari , sanjit]@csa.iisc.ernet.in
Information Security Lab
Department of Computer Science and Automation , IISc , Bangalore

## *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* : is 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
  - ➢ Communicational 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 at non-leaf levels, and
  - ➢ *SOK* key agreement scheme given by Sakai et al. at leaf level.
- HH-KAS is fully resilient at leaf level and resilient upto a threshold at non-leaf levels

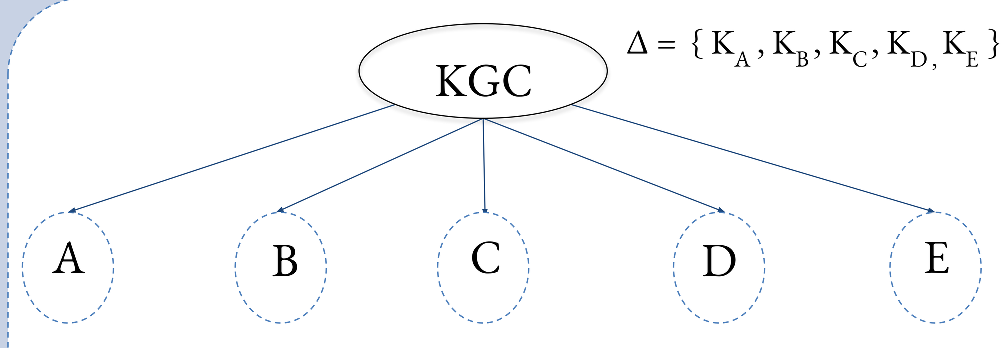
## *Tools*

- Let $G_1$ , $G_2$, $G_T$ be cyclic prime order groups then, *pairing* is a efficiently computable map $e : G_1 \times G_2 \rightarrow G_T$ which satisfies :
  - ➢ Bilinearity : $\forall a, b \in F_q^*, \forall P \in G_1, \forall Q \in G_2 : e(aP, bQ) = e(P, Q)^{ab}$
  - ➢ 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*


- Gennaro R., Halevi S., Krawczyk H., Rabin T., Reidt S. , Wolthusen S.D.: Strongly-Resilient and Non-interactive Hierarchical Key-Agreement in MANETs, ESORICS, 2008
- Lee J., and Stinson D.R., Deterministic Key Predistribution Schemes for Distributed Sensor Networks, SAC, 2004
- Sakai R., Ohgishi K., Kasahara M.: Cryptosystems based on pairing. Cryptography and Information Security, 2000
- Chatterjee S., Hankerson D., Knapp E., Menezes A.: Comparing two pairing-based aggregate signature schemes. Designs, Codes and Cryptography, 2010


## *BIOS-SOK Key Agreement Scheme*

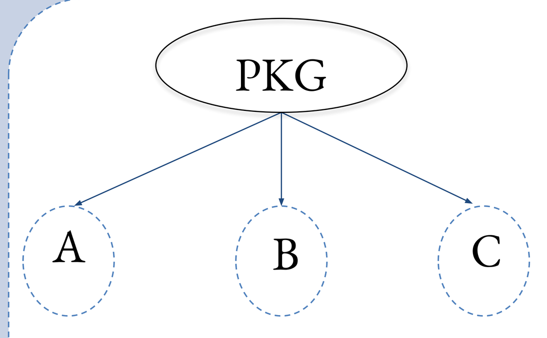



| Id | Secret Keys |
|---|---|
| A | $K_A, h(K_E \| Id_A), h(K_D \| Id_A)$ |
| B | $K_B, h(K_A \| Id_B), h(K_E \| Id_B)$ |
| C | $K_C, h(K_B \| Id_C), h(K_A \| Id_C)$ |
| D | $K_D, h(K_C \| Id_D), h(K_B \| Id_D)$ |
| E | $K_E, h(K_D \| Id_E), h(K_C \| Id_E)$ |

- h is a one-way hash function
- Shared secret key of A and B is $s_{AB} = h(K_A \| Id_B)$ which is possessed by B and can be computed by A

# of keys/ node = $\lceil \frac{n-1}{2} \rceil + 1$

*Basic Id One-way Function Scheme*




| Id | Secret Keys |
|---|---|
| A | $s . H . (Id_A)$ |
| B | $s . H . (Id_B)$ |
| C | $s . H . (Id_C)$ |

Shared Key between A and B :
$K_{AB} = e(s. H(ID_A), H(ID_B)) = e( H(ID_A), s. H(ID_B)) = K_{BA}$

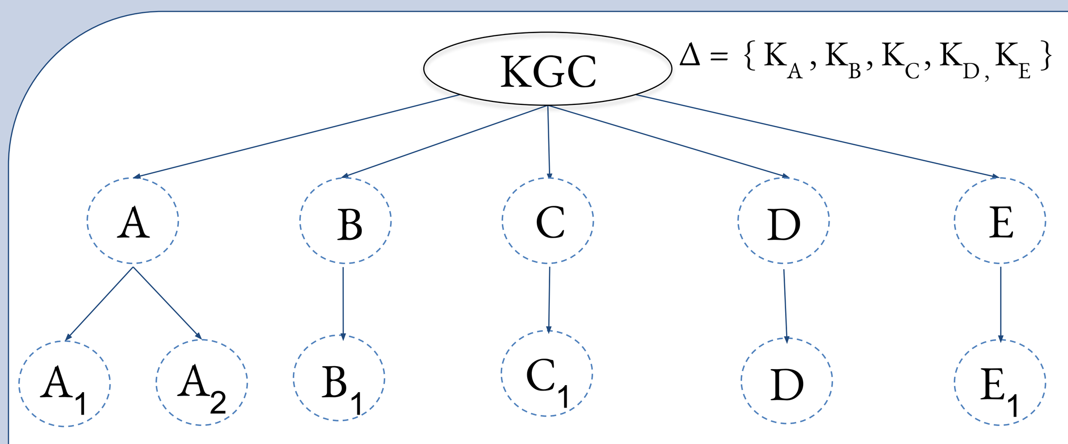
PKG runs following three algorithms :

1) *Setup* : takes security parameter as input and outputs public parameters (params) and master secret key (msk)
2) *Extract* : using msk and identities of nodes, PKG generates their secret keys
3) *Shared Key* : using params, its own secret key and peer's identity, a node computes its shared key with the peer

*SOK Key Agreement Scheme*

At Level 1

Beyond Level 1




Secret Keys at Level 1

| Id | Secret Keys |
|---|---|
| A | $K_A, h(K_E \| Id_A), h(K_D \| Id_A)$ |
| B | $K_B, h(K_A \| Id_B), h(K_E \| Id_B)$ |
| C | $K_C, h(K_B \| Id_C), h(K_A \| Id_C)$ |
| D | $K_D, h(K_C \| Id_D), h(K_B \| Id_D)$ |
| E | $K_E, h(K_D \| Id_E), h(K_C \| Id_E)$ |

Shared Keys at Level 1 for Node A

$s_{AB} = h(K_A \| Id_B) = s_{BA}$
$s_{AC} = h(K_A \| Id_C) = s_{CA}$
$s_{AD} = h(K_D \| Id_A) = s_{DA}$
$s_{AE} = h(K_E \| Id_A) = s_{EA}$
$s_{AA} = h(K_A \| Id_A)$

Secret Keys at Level 2

| Id | Secret Keys |
|---|---|
| $A_1$ | $s_{AA}. H(A_1) , s_{AB}. H(A_1) , s_{AC}. H(A_1) , s_{AD}. H(A_1) , s_{AE}. H(A_1)$ |
| $A_2$ | $s_{AA}. H(A_2), s_{AB}. H(A_2), s_{AC}. H(A_2), s_{AD}. H(A_2), s_{AE}. H(A_2)$ |
| $B_1$ | $s_{BA}. H(B_1) , s_{BB}. H(B_1), s_{BC}. H(B_1), s_{BD}. H(B_1) , s_{BE}. H(B_1)$ |
| $C_1$ | $s_{CA}. H(C_1) , s_{CB}. H(C_1) , s_{CC}. H(C_1), s_{CD}. H(C_1), s_{CE}. H(C_1)$ |
| $D_1$ | $s_{DA}. H(D_1), s_{DB}. H(D_1), s_{DC}. H(D_1), s_{DD}. H(D_1), s_{DE}. H(D_1)$ |
| $E_1$ | $s_{EA}. H(E_1), s_{EB}. H(E_1), s_{EC}. H(E_1), s_{ED}. H(E_1), s_{EE}. H(E_1)$ |

Shared Keys at Level 2 for Node $A_1$

$s_{A1A2} = e(s_{AA}.H(A_1), H(A_2)) = e(H(A_1), s_{AA}.H(A_2)) = s_{A2A1}$
$s_{A1B1} = e(s_{AB}.H(A_1), H(B_1)) = e(H(A_1), s_{BA}.H(B_1)) = s_{B1A1}$
$s_{A1C1} = e(s_{AC}.H(A_1), H(C_1)) = e(H(A_1), s_{CA}.H(C_1)) = s_{C1A1}$
$s_{A1D1} = e(s_{AD}.H(A_1), H(D_1)) = e(H(A_1), s_{DA}.H(D_1)) = s_{D1A1}$
$s_{A1E1} = e(s_{AE}.H(A_1), H(E_1)) = e(H(A_1), s_{EA}.H(E_1)) = s_{E1A1}$

*BIOS - SOK Key Agreement Scheme*

## Comparison of BIOS-SOK and HH-KAS

| Scheme : | Polynomial based HH-KAS | | Subset based HH-KAS | | BIOS-SOK KAS | |
|---|---|---|---|---|---|---|
| Thresholds : | $t_1 = t_2 = 3$ | $t_1 = 7, t_2 = 31$ | $t_1 = t_2 = 3$ | $t_1 = 7, t_2 = 31$ | $n_1 = n_2 = 4$ | $n_1 = 8, n_2 = 32$ |
| Key-Size (# of group elements) | Root : 100<br>Leaves : 16 | Root : 19008<br>Leaves : 256 | Root : 28768<br>Leaves : 1800 | Root : 8930800<br>Leaves : 35000 | Root : 4<br>Level 1 : 3<br>Level 2 : 4<br>Leaves : 4 | Root: 8<br>Level 1 : 6<br>Level 2: 8<br>Leaves: 32 |
| Shared Key Computation | 1 pairing<br>16 EC mult's | 1 pairing<br>256 EC mult's | 1 pairing<br>450 EC add's<br>1800 hashing | 1 pairing<br>11000 EC add's<br>35000 hashing | 3 pairings<br>6 hashing | 3 pairings<br>6 hashing |
| Shared Key Computation (in terms of field mult's) | 39703 m | 407623 m | 587125 m | 11052275 m | 47415 m | 47415 m |

## *Properties*

- *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