USMA 6th Network Science Workshop
April 23, 2012
West Point, NY

U.S. Army Research, Development and Engineering Command

A Composite Trust based Public Key Management in MANETs

TECHNOLOGY DRIVEN. WARFIGHTER FOCUSED.

Jin-Hee Cho and Kevin Chan

Computational and Information Sciences Directorate

U.S. Army Research Laboratory, Adelphi, MD

Motivation

- **Traditional key management solutions**:
  - Incur high resource consumption (i.e., communication and computation overhead) upon high network dynamics (i.e., frequent key assignment);
  - Require centralized trusted certificate authorities (CA); and
  - Have conflicting goals of efficiency and security
- **Characteristics of MANETs**:
  - Lack of resources (e.g., memory, energy, bandwidth);
  - No trusted third party allowed; and
  - Unreliable wireless medium

Goal

Take a soft security approach by applying the concept of trust in order to meet security requirements while maximizing performance:

- Propose a composite trust based public key management to meeting the conflicting goals (security and performance) without relying on a trusted third party such as CA
- Develop the public key management protocol aiming to be:
  - resilient against selfish or malicious nodes;
  - available in service provision; and
  - efficient in minimizing communication overhead

Related Work: Public Key Management

- **Certificate-based** (Capkun03, Dahshan10)
- **ID-based** (Yu10)
- **Threshold cryptography** (Zhu99, Dahshan09)
- **Certificateless** (Sattam03)
- **Hybrid**
  - ID-based plus threshold cryptography (Sun09)
  - Certificateless plus threshold cryptography (Li11)

- **Limitations:**
  - Need a centralized trusted third party;
  - High communication overhead;
  - Improper solution for dynamic/distributed networks

Contributions

- Soft security approach
- Composite trust metric
- Fully distributed algorithm
- Protocol design methodology

Main Design Features

- Modeling of heterogeneous nodes in MANETs (e.g., speed, energy, monitoring capability membership, and trustworthy behaviors);
- No trusted third party is required; hence there are no single points of failure;
- Resilience with high survivability in the presence of hostile entities;
- Secure key revocation (i.e., minimum delay to revoke a compromised node); and
- Scalability with low communication overhead for obtaining a valid public key

Trust Metric (1/2)

- **Trust Components**
  - **Competence (C):** An entity's capability to serve received requests in terms of a node's cooperativeness and availability

    ➔ Public keys needs to be distributed without being dropped
  - **Integrity (I):** Honesty of an entity in terms of network attack behaviors

    ➔ A node should be able to obtain correct public keys
  - **Social Connection (SC):** Social aspect of an entity in terms of the number of contacts over all nodes in the network

    ➔ Public keys may be distributed quickly via social connection based trust

Trust Metric (2/2)

- **Trust Aggregation** (Cho10)
  - Consider both direct observations plus recommendations

$$\text{if } (|R_j| > 0)$$

$$T_{i,j}^{X}(t) = \alpha T_{i,j}^{D-X}(t) + (1-\alpha) T_{i,j}^{ID-X}(t)$$

$$\text{else } T_{i,j}^{X}(t) = \gamma T_{i,j}^{X}(t - \Delta t)$$

  - Rely on past experience upon unavailability of direct observations
  - Decay trust upon no direct interactions

Key Generation & Certificate Issuance

- **Key Generation**
  - Each node generates its own public and private key pairs
- **Certificate Issuance**
  - A node selects a trustworthy certifier (TC) among 1-hop neighbors to issue the certificate of its public key;
  - TC decides to issue the certificate depending on the requestor's trust; and
  - Untrustworthy nodes are not able to obtain the certificate

Key Distribution

- Disseminate a public key with the certificate to trustworthy 1-hop neighbors
- Determines trustworthiness based on a threshold for each trust property X = competence (C), integrity (I), and social connection (SC)
- Dissemination of a public key by node i:

$$\left[\left(C^{TC\,(i)}_{K_{i,public}}\right)_{K_{i,private}}, K_{i,public}\right]$$

: TC(i): TC of node i, $K_{i,\ public}$: public key of node i, $K_{i,\ private}$: private key of node I

- Request a public key of a remote node:
  - Return the public key: $\left[\left(\left(C^{TC\,(TN)}_{K_{TN,public}}\right)_{K_{TN,private}}, K_{TN,public}, ID_{m1}\right)_{K_{i,public}}\right]$
  - Delegate the request: $\left[\left(\left(C^{TC\,(i)}_{K_{i,public}}\right)_{K_{i,private}}, K_{i,public}, ID_{TN}, ID_{pre(m1)}\right)_{K_{m1,public}}\right]$

Key Revocation

- **Implicit key revocation** based on the expiration date of a public key in its certificate;
- **Explicit key revocation** based on the detection of compromised nodes by their 1-hop neighbors

Attack Model

- **Packet dropping:** A node may drop a packet received due to the natures of selfishness or maliciousness;
- **Message modification or forgery:** A node may modify or forge a message received;
- **Fake identity:** A node may use a fake identity or multiple identities (i.e., Sybil attack); and
- **Good or bad mouthing:** A node may give a bad recommendation for a good node while giving a good recommendation for a bad node

Metrics

- **Mean Time To Security Failure (MTTSF)**: Average time elapsed before either security failure condition is met, where the security failure conditions (SFCs) are:
  - **SFC1:** When a private key has been compromised without key revocation and update for a certain time period
  - **SFC2:** When the fraction of the average number of incorrect public keys over the total number of public keys kept in each node exceeds a certain threshold
- **Mean Time To Service Availability (MTTSA)**: Average time elapsed until a node obtains a valid public key of a target node
- **Communication Overhead (CO)**: Communication overhead caused by the proposed key management scheme per time unit

Risk Analysis

- Risk may occur upon all decision makings based on perceived trust
- Node i's average risk probability by trusting node j per time unit is computed as:

$$r_{i,j}(t) = \sum_{d \in D} e^{-\alpha \frac{T_{i,j}(t)}{T_{i,th}}} I_d \text{ where } \sum_{d \in D} I_d = 1$$

I_d: Importance of a decision
D: A set of decisions d's

Conclusions & Future Work

- **Conclusions:**
  - Proposed a fully distributed trust-based public key management scheme for MANETs using the concept of trust as a soft security approach;
  - Aimed to maximize performance while meeting an acceptable risk level;
  - Employed the composite trust metric and trust-based public key management strategies where composite trust derives from communication, information and social networks; and
  - Suggested key metrics to reflect resilience, availability, and scalability along with risk analysis
- **Future work:**
  - Plan to conduct simulation experiments to validate the performance of the proposed public key management scheme

Thank you !

Any questions?

Contact us at:

Jin-Hee Cho
U.S. Army Research Laboratory (USARL)
2800 Powder Mill Rd, Adelphi, MD 20783
Phone: 301-394-0492
jinhee.cho@us.army.mil