Naval Research Laboratory

Washington, DC 20375-5320

NRL/MR/5542--20-10,206

Information Security for the Tactical Mobile Network (TMN)

Jim Z. Luo

Center for High Assurance Computing Branch
Information Technology Division

February 9, 2021

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
09-02-2021	NRL Memorandum Report	10/01/2017 – 09/30/2020

4. TITLE AND SUBTITLE

Information Security for the Tactical Mobile Network (TMN)

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Jim Z. Luo

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER
6A93

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Naval Research Laboratory
4555 Overlook Avenue, SW
Washington, DC 20375-5320

8. PERFORMING ORGANIZATION REPORT NUMBER

NRL/MR/5542--20-10,206

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Office of Naval Research
One Liberty Center
875 N. Randolph Street, Suite 1425
Arlington, VA 22203-1995

10. SPONSOR / MONITOR'S ACRONYM(S)

ONR

11. SPONSOR / MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Create a novel Attributed Based Encryption (ABE) algorithm to secure data-in-transit and enforce fine-grained access control for the future battlefield tactical mobile network (TMN). Develop enhanced ABE capabilities to efficiently and effectively support user revocation, trust authority delegation, federated operations, attribute expiration, and improvement in real-world performance.

15. SUBJECT TERMS

Attribute based encryption
Access control
Network security
Tactical mobile network
Cryptography

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
					Jim Z. Luo
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**	Unclassified Unlimited	7	**19b. TELEPHONE NUMBER** *(include area code)*
Unclassified Unlimited	Unclassified Unlimited	Unclassified Unlimited			(202) 767-3381

This page intentionally left blank.

Project Objective

The objective of this project is to create a novel Attributed Based Encryption (ABE) algorithm to secure data-in-transit and enforce fine-grained access control for the future battlefield Tactical Mobile Network (TMN). We will develop enhanced ABE capabilities to efficiently and effectively support user revocation, trust authority delegation, federated operations, and attribute expiration.

Project Background and Motivation

The Tactical Mobile Network (TMN) is an important facet of the future battlefield. Advancements in peer-to-peer routing, mobile ad hoc networks (MANets), wireless networking, and heterogeneous networks are steadily improving the capabilities of the TMN. However, how to secure the TMN remains an open question.

The size of tactical networks, currently in the hundreds of nodes, will eventually grow to thousands if not millions of nodes when mobile devices, sensor networks, and Internet of Things (IoT) come into play. Scalability will become a severe problem for securing data-in-transit. Current point-to-point secure channels and pre-shared key schemes will not scale. The high-level requirement for secure information sharing in the TMN is simple. We need to send data to the devices that are supposed to get it while keeping it away from all others.

The specific requirements for a security solution are summarized as follows:

- Support large and dynamic battlefield networks. Efficiently handle connections and disconnections. Minimize the cost of nodes entering and leaving the network. Achieve scalability in terms of network size.
- Provide fine-grained access control. The security solution must segregate access for communities of interest and support advanced access control frameworks such as attribute-based access control. Achieve scalability in terms of complexity of the access control policy.
- Provide the ability to establish trust for the unpredictable communication needs of the battlefield. The security solution must not prevent communications that otherwise should be able to take place.
- Support efficient group-based communications over the wireless medium. Multiple recipients can receive wireless signals without additional cost to the sender. The security solution must preserve this advantage.
- Support distributed operations when disconnected from the network infrastructure. The security solution cannot rely on centralized control nodes. Secure communication needs to be established and maintained at the edge nodes. Isolated units must be able to communicate effectively in peer-to-peer mode.

Currently, symmetric key encryption and public key encryption are the only cryptographic primitives available in constructing security protocols. Satisfying TMN security and functional requirements with only these two primitives will be very difficult. The solution will invariably be overly complicated with

Manuscript approved January 29, 2021.

unacceptable overhead and management costs. A paradigm shift in cryptography is needed to create an effective security solution for the TMN.

Technical Approach

We propose to apply the Attribute-Based Encryption (ABE) concept to secure data-in-transit and perform access control for the TMN. ABE is a novel security primitive that provides a set of distinct operational characteristics that are especially well-suited for the TMN. Under ABE, identity and access privileges are defined using attributes. During encryption, the sender creates an access-policy tree using attribute public keys and Boolean operators. To decrypt, recipients can resolve the access-policy tree if and only if they possess the appropriate attribute private keys. Individualized attribute private keys are given to users by trust authorities at setup time. They are bound together with a personal identifier to prevent collusion. Attribute public keys are calculated from published parameters. A single master public private key pair is used in the entire system. Essentially, all users in the network possess secret shares that allow them to communicate, while the arrangement of the secret shares will enable them to define specific recipients according to the agreed-upon attribute semantics.

The following is a summary of ABE characteristics that make it especially well-suited for the TMN:

1. Connectionless operations: The secret share is universal and distributed at setup time. Senders and recipients are automatically able to communicate without handshakes. Network security management is bypassed.
2. Distributed operations: Direct cryptographic links are provided between all senders and recipients. There is no need for control nodes during operation.
3. Policy-based encryption: The encryption process itself supports fine-grained policies and cryptographic enforcement of access control. There is no need to resolve identities and perform authorization.
4. Group based communications: All recipients that satisfy the access policy tree will be able to decrypt messages.

The main technical challenge for this project is developing a more advanced ABE algorithm with additional capabilities for military TMN operations, as follows:

1. Revocation: The ability to revoke is critical and the most important capability we will add to ABE. Our strategy is to develop a tightly coupled two-layer solution. Users are assigned an additional identifier (ID). Our approach cleverly incorporates $1/(ID_{user} - ID_j)$ into the ciphertext where ID_j=revoked ID. Revoked users will not resolve $1/(ID_j - ID_j)$ and will not be to decrypt the ciphertext. We will also develop a hierarchical user ID structure supporting efficient group revocation among different echelons.
2. Delegation: The security infrastructure can be easier to manage by allowing hierarchical trust authorities that follow the organizational structure. It also provides for forward-deployed trust authorities that are necessary for dynamic attributes. Delegation is an existing capability in ABE. Our contribution is the ability to revoke delegated attributes when the delegated trust authority is revoked. Our approach is to attach trust authority ID (TID) to attributes and tightly couple them

in the ciphertext. Consequently, solving for $1/(ID - ID_j)(TID - TID_j)$ will fail if either the ID_j or the TID_j is revoked.

3. Federation: Federated operations are important for modern warfare and allow secure communication between coalition partners without having to share a root of trust. Federation is similar to delegation except with a master private key that is not known by any of the parties. Our approach is to create a multiparty secret sharing scheme to generate delegated master private keys for all parties without revealing the ultimate master private key.
4. Expiration: Simplistic expiration can be accomplished using time slices. However, this lacks granularity, where all attributes expire at the same time. Our approach is to attach comparable numerical values to individual user attributes where expiration can be precisely specified. This capability will enable dynamic attributes (e.g., location, mission, task) with short and varying lifetimes.

Extending the ABE paradigm with new algorithms and these additional capabilities to support a TMN security infrastructure is the primary effort of this project. Once the new ABE algorithms are designed, we will develop a native Android implementation and create a protocol for information sharing on the TMN. We will integrate ABE as a security library that can be directly leveraged by applications. It will interoperate without interfering with link-layer routing and the security mechanisms of the underlying network. We will also develop the information governance and security operations model for the TMN using realistic scenarios. There is not an existing body of attribute-based access control (ABAC) policies for the military. We will develop policy examples and templates, as well as the deployment model for trust authorities. We will create a simulation-based testbed to evaluate the effectiveness of ABE in the TMN context. We will focus on a hierarchical MANet with around 5000 nodes, which corresponds roughly to a maneuvering battalion with mobile devices, sensors, UAVs, and various smart devices. We will create sample applications and scenarios to generate realistic network traffic and demonstrate real-world performance. We will highlight the difference in security capabilities, performance, and scalability compared to traditional security protocols such as VPN, pre-shared keys, multicast schemes, and PKI.

Results

FY2018:

We developed two new constructions for the algorithm. The first construction focuses on identity-based user revocation. A special user ID is embedded into all the user attribute private keys. The sender can exclude a specified user from decrypting the access control tree with the user ID. During encryption, additional equations incorporating the revoked ID's are added ciphertext. During decryption, if the user ID is not in the set of revoked IDs, it will derive two *independent* equations that can be used to solve for the plaintext. If the user ID is revoked, it will derive two *dependent* equations that cannot resolve the plaintext. This scheme allows for the incorporation of multiple IDs for each user. This way, hierarchical revocation can be supported, e.g., multiple users who share the same group ID can be revoked at once. The second construction focuses on attribute expiration. We developed the concept of comparable attributes where user attribute private keys can be associated with a numerical range. Access policy trees can incorporate additional constraints on the numerical range. The numerical range can be used to denote time and support fine-grained expiration. Data senders can specify the valid time period for each attribute.

Only attribute private keys that are valid within that time period will be able to decrypt the access policy tree. The two constructions are not compatible. We created security proofs for both constructions, implemented the revocation scheme in C using the PBC library[1], and applied basic performance and complexity analysis to the resulting software. Encryption and decryption times of under one second can be achieved using standard mobile device hardware. It is important to note that the ABE encryption and decryption has to be performed only once per session of the data stream. This happens relatively infrequently, suggesting the amortized overhead to be relatively low.

FY2019

We developed generalized schemes to support delegation and federation that is compatible with both of our ABE constructions. Delegation is a common requirement for ABE. We developed both unconstrained delegation, where the delegated master key can generate any attribute, and constrained delegation, where the master key for generating specific attributes is delegated. Federation is a new concept in ABE. It is a unique requirement for the military with the need for distributed coalition operations. We developed a scheme based on Diffie-Hellman group key agreement. Coalition partners can agree on a single federated master public key that allows the individual country's master private keys to interoperate. For instance, ciphertext encrypted with the coalition wide attribute public key for "Sergeant" can be decrypted by all the sergeants in the coalition. However, no single country holds the top-level master private key, preventing one coalition entity from creating attributes for another coalition entity. For instance, a US node cannot create UK attributes. This scheme supports revoking a country from the coalition and encryption for a specific set of countries. We created a security proof for this scheme.

FY2020

The delegation and federation schemes were applied to the user revocation and attribute expiration construction using the charm-crypto library[2]. The user revocation and the attribute expiration construction are not compatible and cannot be combined. However, they are useful for different scenarios. The user revocation construction is applicable for general-purpose information sharing. The attribute expiration is suitable for short-lived tactical attributes. A mapping and blue force tracking mobile application were developed to demonstrate the ABE capabilities for information sharing and securing data-in-transit.

Associations and Outputs

Publications:

[1] https://crypto.stanford.edu/pbc/
[2] http://charm-crypto.io/

Dong, Q., Huang, D., Luo, J., & Kang, M. (2018, May). Achieving fine-grained access control with discretionary user revocation over cloud data. In *2018 IEEE Conference on Communications and Network Security (CNS)* (pp. 1-9). IEEE.

Luo, J., Dong, Q., Huang, D., & Kang, M. (2018, October). Attribute Based Encryption for Information Sharing on Tactical Mobile Networks. In *MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM)* (pp. 1-9). IEEE.

Huang, D., Chung, C. J., Dong, Q., Luo, J., & Kang, M. (2019, April). Building private blockchains over public blockchains (PoP) an attribute-based access control approach. In *Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing* (pp. 355-363).

Patents:

Huang, Dijiang, Jim Luo, Myong Hoon Kang, and Qiuxiang Dong. "Method and Apparatus for Achieving Fine-Grained Access Control with Discretionary User Revocation Over Cloud Data." U.S. Patent Application 16/728,724, filed October 8, 2020.