Attribute Based Encryption for Information Sharing on Tactical Mobile Networks

Jim Luo*, Qiuxiang Dong♯, Dijiang Huang♯, and Myong Kang*
♯Arizona State University, Tempe, AZ 85281, US
* Naval Research Lab, Washington DC, 20375, US
{qiuxiang.dong, dijiang}@asu.edu
{jim.luo, myong.kang}@nrl.navy.mil

***Abstract*—Security and access control for data in transit remains a challenge for the deployment of battlefield tactical mobile networks (TMN). Attribute based encryption (ABE) is a promising solution that inherently satisfies many of the security and functional requirements of the military in this context. We present a novel ABE cryptographic algorithm with added capabilities for revocation, delegation, and federation. It can serve as the foundation for a security infrastructure that allows effective and efficient information sharing on the TMN.**

***Index Terms*—Attribute-based Encryption, Tactical Mobile Network, access control**

I. INTRODUCTION

Large-scale tactical mobile networks (TMN) will revolutionize the future battlefield. Consumer smartphones are portable and cheap enough to equip every individual soldier. Information sharing at the lowest echelon can provide seamless communication and coordination for the fighting unit [1]–[4].Tactical applications on mobile devices can enable new capabilities for warfighting [5]. Pervasive sensor networks can saturate the battlefield to provide unprecedented situational awareness and make it available to individual soldiers [6], [7]. Smart devices and IoT concepts can provide even more capabilities [8], [9]. Autonomous systems for reconnaissance as well as offensive capabilities can be controlled by smartphones carried by individual soldiers [10]. In the future battlefield, information power will be as potent as firepower.

Smartphones, mobile devices, and applications rely on connectivity. The civilian cellular network model is incompatible with military and battlefield requirements. Facing near-peer adversaries, the network infrastructure will be the first target destroyed at the start of any conflict. Even if cellular and Wi-Fi technologies are deployed, the TMN must be able to fall back to fully distributed operations. Communication and coordination inside the fighting unit is a key mission of the TMN. Individual endpoints should be able to self-organize and fulfill this mission without relying on network infrastructure or other potential single points of failure. The military is currently investing in MANet [11] and tactical radio [12] technologies that are fully distributed, self-organizing, and highly survivable.

The particular challenge for the military is security of the TMN. Communications capabilities cannot be used if they cannot be secured. Tactical information is indeed fleeting. However, it does not go stale quickly enough. Highly sensitive information such as troop location, imagery, sensor readings and mission details can directly put lives in danger and turn the tide of battle. Considering the value of the tactical network traffic, near-peer adversaries will invest in the capabilities to capture, analyze, and disseminate tactical information in real-time. Data-in-transit on the TMN must be encrypted and protected. Access control is necessary to enforce need-to-know, classification levels, least privilege, risk of disclosure, etc. Mobile devices deployed to the battlefield are subject to capture. Moreover, insider threats are ever-present. Involvement of less trusted coalition forces, civilian contractors, and local allies further aggravate the problem. All-or-nothing access is unacceptable. Information needs to be shared widely for everyone authorized that needs it, while also restricted as much as possible such that the impact of compromise is minimized.

A. Traditional Approaches for TMN Security

Security and access control in the civilian cellular network is relatively simple. Communication between the edge nodes and the cellular tower is encrypted. Network traffic is always routed through the cell towers. Fine-grained access control is mediated by the centralized trusted servers. Trust is also managed by centralized servers on the network infrastructure. The need for distributed network operations in the TMN precludes the use of centralized access control points. Encryption, access control, and trust all have to be implemented at the edge devices. There are several approaches for accomplishing this in the tactical context using traditional cryptographic techniques.

Virtual private network (VPN) overlay establishes point-to-point encryption. This is the approach currently used for MANets. However, it creates significant inefficiencies as the size of the network increases. Much of the communication on the TMN will be group-based. Tactical applications, such as blue force tracking, send information to sizable community of interest (COI). Point-to-point channels will require rebroadcasts in the wireless medium and result in orders of magnitude increase in bandwidth utilization and power consumption. Frequent connection, disconnection and reconnection is the norm in the tactical context. The overhead to simply coordinating and maintaining the VPN network itself will be significant. There will also be significant overhead in terms of security management. Every data-sender will need to perform authentication and authorization for every data-recipient, and every data

978-1-5386-7185-6/18/$31.00 ©2018 IEEE

stream. This will quickly become untenable when thousands of endpoints and large number of applications are involved.

Using pre-shared keys would allow for secure-multicasting and take advantage of the wireless medium. This is the approach currently used for tactical radios. Secret keys are coordinated and distributed to the COI at manufacturing time or in the base. Access control is performed in the key distribution process by loading only the appropriate keys on devices. However, this approach is only appropriate for coarse-grained, all-or-nothing access control. There will be scalability problems with respect to the complexity of the access control policies where the number of pre-shared keys required grows exponentially with the number of attributes taken into account. The ability to segregate data becomes a choking point. Furthermore, with pre-shared keys, there is no way to establish or revoke trust outside the base. Devices captured by the enemy can compromise the entire network. Friendly units can unexpectedly move into the same area of operation and may not be able establish communications. Hierarchical multicasting schemes [13] can be used to manage trust. However, it does not address the problem with fine-grained segregation of data.

B. Military Requirements

The high-level requirements for secure information sharing in TMN are simple. We need to send data to the devices that are supposed to get it while keeping it away from others. The characteristics of the TMN and the tactical environment create specific security and functional requirements for the security solution:

- Support large-scale dynamic tactical networks. Efficiently hande connections and disconnections. Achieve scalability in terms of network size.
- Support fine-grained access control. Segregate access for COI and take into account large number of attributes. Achieve scalability in terms of complexity of the access control policy.
- Support unpredictable communication needs with the ability to establish trust in the field. The security layer should not prevent communications that otherwise should be able to take place.
- Support efficient group-based communications over the wireless medium. Wireless signals can be received by multiple recipients without additional cost to the sender. The security layer should preserve this advantage.
- Support distributed operations when disconnected from the network infrastructure. The security layer cannot rely on centralized control nodes. Isolated units should be able to communicate effectively in peer-to-peer mode.
- Asymmetry in sending and receiving data. Nodes with the privilege to send data to a COI may not necessarily have the privilege to receive data.
- Anonymity for recipients in the COI. Data senders should not be able to enumerate and identify recipients for their data.

We envision the TMN concept of operation to be where each data sender encrypts each data packet or data stream seperately for a group of recipients. Authentication and authorization is embedded in the encryption and enforced by the recipient's ability to decrypt. It does not rely on management nodes in the network. Access control policies are communicated in plaintext, and can be changed on the fly by the data sender. Every endpoint in the battlefield carries the secret keys necessary to communicate with everyone else. There is no handshake or overhead for connecting and disconnecting. Data senders do not need to keep track of the data recipients, they simply manage security at the access control policy level. Endpoints captured by the enemy will only compromise the minimal amount of data due to fine-grained access control. Revocation of captured endpoints can be done efficiently without having to rekey other endpoints. Revocation lists can be distributed in plaintext to data senders. Adversaries that capture and compromise multiple endpoints are not able to gain greater access than the individual endpoints are entitled to. Endpoints are able to encrypt data for an access policy, but should not be able to decrypt. For example, sensor nodes are able to encrypt data, but do not have to keys to decrypt data. Endpoints are also able to decrypt data anonymously. For example, special forces units should be able to access data they are entitled to without having to authenticate with the data sender and reveal their identity.

II. Attribute Based Encryption

Attribute Based Encryption (ABE) is a relatively new security primitive based on bilinear maps on elliptic curves [14], [15]. It will provide revolutionary capabilities that are especially suited for information sharing on the TMN.

Identity and access privileges are defined using a set of attributes, e.g. nationality, rank, unit, location, clearance level, mission, etc. Attributes are assigned by trust authorities. A single set of master public/private keys is used in the entire security domain. In essence, the entire system is under the same community of trust (COT) [16], [17]. Attribute private keys are calculated from the master private key. They are bound together with a personal identifier to prevent collusion. Attribute public keys are calculated from the master public key and they are the same for the entire domain. During encryption, the sender creates an access policy tree using attribute public keys and Boolean operators. Recipients will be able to decrypt the messages if and only if they have the attribute private keys to resolve the access policy tree. Since the attribute public keys, and therefore the ciphertext, are the same for the entire domain, the same encrypted message can be decrypted by multiple recipients. There is no need to specify individual recipients or perform handshakes. This bypasses much of the management overhead in keeping track of recipients. The sender can simply encrypt data according to the access policy, send it out to the network, and all the recipients who can satisfy the policy will be able to decrypt it. Different access policies can be attached to individual datagrams and achieve unlimited granularity. This is compatible with the Object Level Protection (OLP) concept [18], and the data-centric security paradigm. The sender can

also change the access policy dynamically without relying on the central authority.

The following is a summary of ABE characteristics that make it especially well-suited for secure information sharing on the military TMN:

- Connectionless operations. The secret share is universal for the entire system and distributed at setup time. Senders and recipients are automatically able to communicate using their version of the secret share. There is no need to coordinate secure connections. The scalability problem is fully addressed.
- Policy-based encryption. This allows for fine-grained policies and cryptographic enforcement of access control. The encryption and decryption costs increase linearly with the complexity of the access control policy. There is no need to resolve identities and perform authorization.
- Group-based communications. All recipients that satisfy the access policy tree will be able to decrypt.
- Distributed operations. There is no need for centralized coordination for security or control nodes to mediate access. Access control is cryptographically enforced through the ability to decrypt. Senders are free to setup and change the access policy on the fly.
- Asymmetry between sender and recipients. Data senders are not necessarily able to decrypt data for the community of interest of intended recipients.
- Anonymity of the recipients. Policy-based encryption and connectionless operations means the sender do not need to be aware of who is receiving data.

III. Our Contributions

A. Additional Capabilities for Military Requirements

Basic ABE characteristics are inherently a nice fit for the TMN. However, additional capabilities are needed to make it a practical security infrastructure solution.

- Revocation: The ability to revoke access is critical for public key infrastructures. Ideally, the revocation list should be distributed in plaintext and data senders can amend the access policy tree to remove access for those users.
- Delegation: Delegation makes it much easier to manage the security infrastructure by allowing for hierarchical trust authorities that follow the organizational structure of the military. It would also allow for forward-deployed limited trust authorities that are necessary for dynamic attributes such as location.
- Federated operations: Coalition operations are important for modern warfare. Coalition partners should be able to interoperate without having to share their root of trust. Encryption can be performed such that attributes private keys derived from different master private keys can be used to decrypt.

IV. Algorithm Construction

We developed a novel ABE algorithm that incorporates these capabilities.

A. Federated Setup and Key Generation

Assume there is a trusted coalition TC= $\{TC_1, \cdots, TC_N\}$ (N is the number of members in TC) who will run the setup protocol of the ABE scheme to generate their shares of the master secret key and the public parameters and then generate the system-wide master secret key and public parameters by running a secure multiple party computation protocol.

Protocol 1 Federation Setup

INPUTS:

Each TC_i has inputs of security parameter λ, attribute set U, a prime-order group $\mathbb{G}$, the generator g of $\mathbb{G}$, random elements $\{h_x\}_{x\in U}$ selected from $\mathbb{G}$.

PROCEDURE:

(a). TC_i generates $\alpha_i, b_i, s_i \in \mathbb{Z}_p$;

(b). TC_i computes $b_i^2, e(g,g)^{\alpha_i}, b_i^{-1}, s_{ij}^{-1}$, where s_{ij} is equal to $ID_j^{s_i}$ and $ID_j \in \mathcal{RI}$ (the set of identities of the root authorities).

(b.1) If $i = 1$, TC_1 will calculate PK_1 as shown below and send it to TC_2.

$$\{g^{b_1}, g^{b_1^2}, e(g,g)^{\alpha_1}, \{h_x^{b_1}, h_x^{b_1^2}\}_{x\in U}, \{g^{b_1 s_{1j}^{-1}}, g^{s_{1j}^{-1}}\}_{ID_j\in\mathcal{RI}}\}$$

(b.2) If $i \neq 1$, TC_i will receive public parameters from TC_{i-1} in the format of PK_{i-1} and calculate PK_i.

$$PK_{i-1} = \{pk_1, pk_2, pk_3, \{pk_{x1}, pk_{x_2}\}_{x\in U}, \{pk_{ID_j1}, pk_{ID_j2}\}_{j\in\mathcal{I}}\}$$

$$PK_i = \{pk_1^{b_i}, pk_2^{b_i^2}, pk_3 \cdot e(g,g)^{\alpha_i}, \{pk_{x1}^{b_i}, pk_{x_2}^{b_i^2}\}_{x\in U}, \{pk_{ID_j1}^{b_i s_{ij}^{-1}}\}, \{pk_{ID_j2}^{s_{ij}^{-1}}\}_{ID_j\in\mathcal{RI}}\}$$

(b.2.1) If $i \neq N$, TC_i calculates PK_i and sends it to TC_{i+1}.

(b.2.2) If $i = N$, TC_N calculates $PK = PK_N$ and then publishes it to the public.

Fig. 1 Federation Setup.

*1) **Federation Setup**:* Each TC member performs computation and communication as described in **Protocol** 1. The master secret key and public parameters are as follows

$$MSK = (\alpha, b, s)$$

$$PK = \left(g, g^b, g^{b^2}, e(g,g)^\alpha, \{h_x^b, h_x^{b^2}\}_{x\in U}, \{g^{bs_{ID_j}^{-1}}, g^{s_{ID_j}^{-1}}\}_{ID_j\in\mathcal{RI}}\right)$$

where $\alpha = \sum_{i=1}^N \alpha_i, b = \prod_{i=1}^N b_i, s = \sum_{i=1}^N s_i, s_{ID_j} = \prod_{i=1}^N s_{ij}$ and $\mathcal{RI}$ denotes the set of identities of the root authorities (or organizations).

*2) **Federated Key Generation**:* As shown in **Protocol** 2, the trusted coalition members generate a private key SK for the root authority of an organization ID with attributes U_{ID}.

$$SK = (g^\alpha g^{b^2 t}, g^{-t}, (g^{bs_{ID}} h_x^b)^t, g^{bs_{ID}}, h_x, g^{bt}, h_x^t, h_x^{bt}, s_{ID})_{x\in U_{ID}},$$

where $t = \sum_{i=1}^N t_i$, $b = \prod_{i=1}^N b_i$, $s_{ID} = ID^s, s = \prod_{i=1}^N s_i$ and x is in the set of attributes managed by organization ID. With the private component s_{ID}, each root authority generates private components for the domain authorities with the rule $s_{child} = (ID_{child})^{s_{parent}}$. $g^{bs_{child}^{-1}}$ and $g^{s_{child}^{-1}}$ are part of the system public parameters.

Protocol 2 Federated Key Generation

INPUTS:

Each TC_i has public parameters, the secret share α_i, b_i, s_i, and the identity ID of the organization.

PROCEDURE:

(a). TC_i with α_i, b_i, s_i generates $t_i \in \mathbb{Z}_p$;

(b). TC_i calculates ID^{s_i}, g^{α_i}, $(g^{b^2})^{t_i}, g^{-t_i}, (g^b)^{t_i}$, and $\{h_x^{t_i}, h_x^{bt_i}\}_{x \in U_{ID}}$.

(b.1). If $i = 1$, TC_1 calculates $ID_1 = ID^{s_1}, g^{\alpha_1}$, $(g^{b^2})^{t_1}, g^{-t_1}, (g^b)^{t_1}, \{h_x^{t_1}, h_x^{bt_1}\}_{x \in U_{ID}}$ and sends it to TC_2.

(b.2). Instead, if $i \neq 1$, TC_i obtains $(c_1, c_2, c_3, c_4, \{c_5, c_6\}_{x \in U_{ID}})$ from TC_{i-1} and calculates $((c_1)^{s_i}, c_2 \cdot g^{\alpha_i}, c_3 \cdot (g^{b^2})^{t_i}, c_4 \cdot g^{-t_i}, \{c_5 \cdot h_x^{t_i}, c_6 \cdot h_x^{bt_i}\}_{x \in U_{ID}})$.

(b.2.1). Instead, if $i \neq N$, TC_i sends the generated components to TC_{i+1}.

(b.2.2). If $i = N$, TC_N sends the generated private key SK to the root authority of organization ID.

Fig. 2 Federated Key Generation.

Protocol 3 Delegation-Internal

INPUTS:

Parent DA has private key SK_{ia} shown below.

$$SK_{ia} = \Big(g^{\alpha} g^{b^2 t_{ia}}, g^{s_{ja}^{-1} t_{ia}}, g^{-t_{ia}}, (g^{bs_{ja}} h_x^b)^{t_{ia}}, g^{bs_{ja}}, h_x, g^{bt_{ia}}, h_x^{t_{ia}}, h_x^{bt_{ia}}, s_{ia}\Big)_{j \in ANC_i \cup i}^{x \in S_{ia}}.$$

PROCEDURE:

(a). Parent DA sends $SK_{ia \to (i+1)a}$ below to Child DA.

$$SK_{ia \to (i+1)a} = \Big(g^{\alpha} g^{b^2 t_{ia}}, g^{s_{ja}^{-1} t_{ia}}, g^{-t_{ia}}, (g^{bs_{ja}} h_x^b)^{t_{ia}}, g^{bs_{ja}}, h_x, g^{bt_{ia}}, h_x^{t_{ia}}, h_x^{bt_{ia}}, s_{(i+1)a}\Big)_{j \in ANC_{(i+1)a}}^{x \in S_{(i+1)a}}.$$

(b). Child DA obtains the private key $SK_{(i+1)a}$.

$$SK_{(i+1)a} = \Big(g^{\alpha} g^{b^2 t_{(i+1)a}}, g^{s_{ja}^{-1} t_{(i+1)a}}, g^{-t_{(i+1)a}}, (g^{bs_{ja}} h_x^b)^{t_{(i+1)a}}, g^{bs_{ja}}, h_x, g^{bt_{(i+1)a}}, h_x^{t_{(i+1)a}}, h_x^{bt_{(i+1)a}}, s_{(i+1)a}\Big)_{j \in ANC_{(i+1)a} \cup (i+1)}^{x \in S_{(i+1)a}},$$

Fig. 3 Internal Key Generation Delegation.

B. Key Generation Delegation

At the inner-organization level, the hierarchical structure reflects the internal organizations' authority and responsibility. For the internal nodes in an organizational structure, the key generation delegation privilege of the parent domain authority could be distributed to the child domain authority. For the external nodes (individual users) in an organizational structure, it is the internal nodes which are the parent of the external nodes to generate the private key for them.

1) ***Delegation-Internal****:* **Protocol** 3 is run between a parent domain authority ID_{ia} and a child domain authority $ID_{(i+1)a}$ to generate the private key for $ID_{(i+1)a}$ based on that of the parent domain authority on level i. ANC_a denotes the ancestor nodes of a in the organization structure.

The components in the private key of the child domain authority are updated in the following way. The integer t' is a random integer selected by the child authority.

$$g^{\alpha} g^{b^2 t_{(i+1)a}} = g^{\alpha} g^{b^2 t_{ia}} \cdot (g^{b^2})^{t'}, g^{s_{ja}^{-1} t_{(i+1)a}} = g^{s_{ja}^{-1} t_{ia}} \cdot (g^{s_{ja}^{-1}})^{t'},$$

$$(g^{bs_{ja}} h_x^b)^{t_{(i+1)a}} = (g^{bs_{ja}} h_x^b)^{t_{ia}} \cdot (g^{bs_{ja}} \cdot h_x^b)^{t'}, g^{-t_{(i+1)a}} = g^{-t_{ia}} \cdot g^{-t'},$$

$$(g^{bs_{(i+1)a}} h_x^b)^{t_{(i+1)a}} = (g^{bt_{ia}} \cdot g^{bt'})^{s_{(i+1)a}} \cdot h_x^{bt_{ia}} \cdot h_x^{bt'},$$

$$g^{bs_{(i+1)a}} = (g^b)^{s_{(i+1)a}}, g^{bt_{(i+1)a}} = g^{bt_{ia}} \cdot g^{bt'},$$

$$h_x^{t_{(i+1)a}} = h_x^{t_{ia}} \cdot h_x^{t'}, h_x^{bt_{(i+1)a}} = h_x^{bt_{ia}} \cdot (h_x^b)^{t'}.$$

Protocol 4 Delegation External

INPUTS:

Domain authority with identity ID_a has private key SK_a.

$$SK_a = \Big(g^{\alpha} g^{b^2 t_a}, g^{s_{ja}^{-1} t_a}, g^{-t_a}, (g^{bs_{ja}} h_x^b)^{t_a}, g^{bs_{ja}}, h_x, g^{bt_a}, h_x^{t_a}, h_x^{bt_a}, sa\Big)_{j \in ANC_a \cup d}^{x \in U_{IDa}}.$$

PROCEDURE:

(a). A user sends private key request to the domain authority.

(b). The domain authority sends the private key SK to the user with identity ID.

$$SK = \Big(K = g^{\alpha} g^{b^2 tu}, \{L_a = g^{s_{ja}^{-1} tu}\}_{j \in ANC_u}, L_u = g^{-tu},$$

$$\{K'_{xa} = (g^{b \cdot sja} h_x^b)^{tu}\}_{j \in ANC_u}^{\forall x \in U_{IDu}}, \{K_{xu}{}' = (g^{b \cdot ID} h_x)^{tu}\}_{\forall x \in U_{IDu}}\Big),$$

where $t_u = t_a + t'$.

Fig. 4 External Key Generation Delegation.

2) ***Delegation-External****:* **Protocol** 4 is run by a domain authority to generate a private key for a user. The components in the private key of the domain authority are updated as follows where t' is a random integer.

$$g^{\alpha} g^{b^2 t_u} = g^{\alpha} g^{b^2 t_a} \cdot (g^{b^2})^{t'}, g^{s_{ja}^{-1} t_u} = g^{s_{ja}^{-1} t_a} \cdot (g^{s_{ja}^{-1}})^{t'},$$

$$(g^{bs_{ja}} h_x^b)^{t_u} = (g^{bs_{ja}} h_x^b)^{t_a} \cdot (g^{bs_{ja}} \cdot h_x^b)^{t'}, g^{-t_u} = g^{-t_a} \cdot g^{-t'},$$

$$g^{bt_u} = g^{bt_a} \cdot g^{bt'}, \; h_x^{t_u} = h_x^{t_a} \cdot h_x^{t'},$$

C. Data Distribution and Access

The revocation is enforced directly during the encryption phase. The data owner would first construct an attribute-based access policy tree and then kick out the undesired data consumers by adding their identities into a revocation identity set. Takeing as inputs of the access policy, revoked identity set as well as the plaintext data, the encryption algorithm outputs the ciphertext to be distributed. In this way, only data consumers whose attributes satisfy the access policy and are not revoked by the data owner can decrypt the ciphertext by running the decryption algorithm described below.

1) $\mathbf{Encrypt}(\mathrm{PK}, (M, \rho), \mathcal{M}, \mathbf{ID})$*:* This is an algorithm that revokes both multiple users and multiple domain authorities. The *Encrypt* algorithm takes as inputs an access infrastructure (M, ρ), where M is an $l \times n$ matrix and the function ρ associates each row of M to corresponding attributes. $\mathbf{ID} = \mathbf{ID}_a \cup \mathbf{ID}_u$ and $|\mathbf{ID}_a| + |\mathbf{ID}_u| = r_a + r_u = r$. Denote the set of revoked domain authority identities as $\mathbf{ID}_a = \{(ID'_{a,j}, h_{a,j})\}_{j \in [1, r_a]}$. The set of revoked user identities is denoted by $\mathbf{ID}_u = \{(ID'_{a,j}, ID'_{u,j}, h_{u,j})\}_{j \in [1, r_u]}$, where $ID'_{u,j}$ is managed by domain authority $ID'_{a,j}$. The *Encrypt* algorithm first chooses a random vector $v = (s, y_2, \cdots, y_n) \in \mathbb{Z}_p^n$. For $x \in [1, l]$, it calculates $\lambda_x = v \cdot M_x$. The *Encrypt* algorithm

chooses random $s \in \mathbb{Z}_p$. The algorithm chooses random μ_a, μ_u such that $\mu = \mu_a + \mu_u$, and $\mu_1, \cdots, \mu_{r_a}, \mu'_1, \cdots, \mu'_{r_u} \in \mathbb{Z}_p$ such that $\mu_a = \mu_1 + \cdots + \mu_{r_a}$ and $\mu_u = \mu'_1 + \cdots + \mu'_{r_u}$. The ciphertext is $CT = (C, C_0, \hat{C}_a, \hat{C}_u, \hat{C_a}', \mathbf{ID})$, where

$$C = \mathcal{M}e(g,g)^{\alpha s\mu},\ C_0 = g^{s\mu},$$

$$\hat{C}_a = \left(C^*_{akj} = g^{bs_i^{-1}\lambda_k u'_j},\ C'_{ak} = (h^b_{\rho(k)})^{\lambda_k u'_j}\right)^{i\in\mathcal{I}_{nr}}_{k\in[1,l],j\in[1,r_a]}$$

$$\hat{C}_u = \Big(\{C^*_{ukj} = g^{b\lambda_k u'_j}\}_{k\in[1,l],j\in[1,r_u]},$$

$$\{C'_{ukj} = (g^{b^2\cdot ID_{u,j}} h^b_{\rho(k)})^{\lambda_k u'_j}\}_{k\in[1,l],j\in[1,r_u]}\Big)$$

$$\hat{C_a}' = \left(C^*_{akj} = g^{bs_i^{-1}\lambda_k \mu_j},\ C'_{akj} = (h^b_{\rho(k)})^{\lambda_k \mu_j}\right)^{i\in\mathcal{I}_{nr}}_{k\in[1,l],j\in[1,r_a]}$$

2) $\mathbf{Decrypt}(\mathrm{CT}, \mathrm{SK})$*:* *CT* is the ciphertext with an access structure and *SK* is a private key for a set $\mathbf{S}$. Suppose that $\mathbf{S}$ satisfies the access structure and let $\mathbf{I} \subset [1, l]$ be defined as $\mathbf{I} = \{i : \rho(i) \in \mathbf{S}\}$. Let $\{\omega_i \in \mathbb{Z}_p\}_{i\in\mathbf{I}}$ be a set of constants such that if $\{\lambda_i\}$ are valid shares of any secret s according to the access structure, then $\Sigma_{i\in\mathbf{I}}\omega_i\lambda_i = s$. For the j^{th} revoked user identity, denote the identity of the non-revoked domain authority administrating ID_u by $ID_{a,j}$, then calculate $e(g,g)^{b^2ts\mu'_j}$ as follows:

$$\begin{cases} (\prod_{i\in\mathbf{I}}[e(K_{\rho(i)u}, C^*_{uij})\cdot e(L_u, C'_{uij})]^{\omega_i})^{\frac{1}{(ID_u - ID_j)}}, ID_{u,j} \neq ID'_{u,j}, \\ \prod_{i\in\mathbf{I}}[e(K'_{\rho(i)aj}, C^*_{aij})\cdot e(L_{aj}, C'_{aij})]^{\omega_i}, ID_{a,j} \neq ID'_{a,j}. \end{cases} \tag{1}$$

Then we can get $e(g,g)^{b^2ts\mu_u}$ in the following way:

$$e(g,g)^{b^2ts\mu_u} = \prod_{j\in[1,r_u]} e(g,g)^{b^2ts\mu'_j}.$$

For the j^{th} revoked domain authority, denote the identity of the domain authority on the ${h_j}^{th}$ layer managing ID_u by $ID_{a,j}$. The decryption algorithm evaluates $e(g,g)^{b^2tsu_j}$ as follows:

$$e(g,g)^{b^2tsu_j} = \prod_{i\in\mathbf{I}}[e(K'_{a\rho(i)j}, C^*_{aij})\cdot e(L_{aj}, C'_{aij})]^{\omega_i}.$$

Then we can get $e(g,g)^{b^2ts\mu_a}$ in the following way:

$$e(g,g)^{b^2ts\mu_a} = \prod_{j\in[1,r_a]} e(g,g)^{b^2ts\mu_j}.$$

If *SK*'s holder is not managed by any revoked domain authority and is not among the revoked users, then we can get $e(g,g)^{\alpha s\mu} = \frac{e(C_0,K)}{e(g,g)^{b^2ts\mu_u}\cdot e(g,g)^{b^2ts\mu_a}}$. Finally get the message $\mathcal{M}$ by evaluating $\frac{C}{e(g,g)^{\alpha s\mu}}$.

D. Security Model

Our scheme should be resistant against two types of unauthorized access. The first one is unauthorized access from a single user. In particular, the user without attributes satisfying the access policy embedded in the ciphertext. The second one is collusion attack. Two users might collude together to gain more access privileges. Our scheme can be proven to be secure against both types of unauthorized access using the same proof as baseline ABE [14], [15].

E. Complexity Analysis

The complexity analysis is summarized in **Table** I of the designed scheme. There are four types of time-consuming operations: pairing, exponentiation, multiplication and inversion, included in the schemes. Among them, the pairing and exponentiation operations are the dominant costs. Therefore, we utilize the number of pairing and exponentiation operations as metrics for computation complexity of each scheme. The main storage overhead comes from the setup algorithm and key generation algorithm. Since the setup of the master secret key and system public parameters is performed by the Trust Coalition, we show the computation complexity for each of the TC members. Each member will perform one pairing and $2|\mathcal{RI}| + |U| + 2|$ exponents. Since each member will send the intermediate result to the next member, there will be $2|\mathcal{RI}| + 2|U| + 3|$ elements transmitted from one member to another. All the TC members will store both the public parameters and the share of the master secret key. The total storage complexity will be $2|U| + 2|\mathcal{RI}| + 7$.

There are two types of key generation. Generating delegation private keys for the domain authorities occures rarely and we exclude it here. The computation complexity of each TC when generating a private key is $2|U_{ID}| + 5$, where $|U_{ID}|$ is the number of attributes of the root authority. We assume that the height of the identity structure tree is 2, *i.e.*, $H = 1$. The complexity of generating a private key for a user is $2|U_{ID_u}|+4$, where U_{ID_u} is the set of attributes assigned to the user.

One pairing computation is performed during the encryption. The number of exponents is $x((|\mathcal{I}_{nr}| + 2)r_u l + r_u + 2) + y((|\mathcal{I}_{nr}| + 1)l + 2)$. If only multiple users are revoked then $x = 1, y = 0$; if only multiple domain authorities are revoked then $x = 0, y = 1$; if there are both multiple users and multiple domain authorities revoked then $x = 1, y = 1$. The communication complexity of the encryption algorithm is $x(2r_u + lr_u|\mathcal{I}_{nr}| + 2lr_u) + y(r_g + l|\mathcal{I}_{nr}|) + 2$, where x and y is the same as above. The computation cost of decryption consists of $2|\mathbf{I}|(r_u + 1)$ pairings and $x(|\mathbf{I}|r_u) + y|\mathbf{I}|$ exponents.

Fig. 5 shows the experimental performance evaluation of the algorithms. The algorithms are implemented in C using PBC library [19] on Ubuntu 14.04 operating system. We set the number of revoked identities to 1 and evaluate the relationship between the number of attributes and the computation time. We are able to achieve reasonable computation time in the 100ms order of magnitude for practical numbers of attributes. .

V. CONCLUSION AND FUTURE WORK

The basic operational characteristics of ABE are inherently compatible with the TMN. We develop a novel ABE algorithm with additional combined capabilities for revocation, delegation, and federation. It can serve as the foundation for a practical TMN information sharing security infrastructure for the military. We intend to further develop the ABE algorithm with additional capabilities, including fine-grained attribute expiration, comparable attributes, and hierarchical attributes. These capabilities will ease management, improve

TABLE I Complexity Analysis.

Overhead	Setup	KeyGen-RA	KeyGen-U	Encrypt	Decrypt
Computation (Pairing)	1	0	0	1	$2\|\mathbf{I}\|(r_u+1)$
Computation(Exponent)	$2\|\mathcal{RI}\|+2\|U\|+2$	$2\|U_{ID_a}\|+5$	$2\|U_{ID_u}\|+3$	$x((\|\mathcal{I}_{nr}\|+2)r_u l+r_u+2)$ + $y((\|\mathcal{I}_{nr}\|+1)l+2)$	$x(\|\mathbf{I}\|r_u)+y\|\mathbf{I}\|$ $x(\|\mathbf{I}\|r_u)+y\|\mathbf{I}\|$
Communication	$2\|\mathcal{RI}\|+2\|U\|+3$	$2\|U_{ID_a}\|+5$	$2\|U_{ID_u}\|+3$	$x(2r_u+lr_u\|\mathcal{I}_{nr}\|+2lr_u)$ + $y(r_g+l\|\mathcal{I}_{nr}\|)+2$	0
Storage	$2\|\mathcal{RI}\|+2\|U\|+7$	$2\|U_{ID_a}\|+5$	$2\|U_{ID_u}\|+3$	0	0

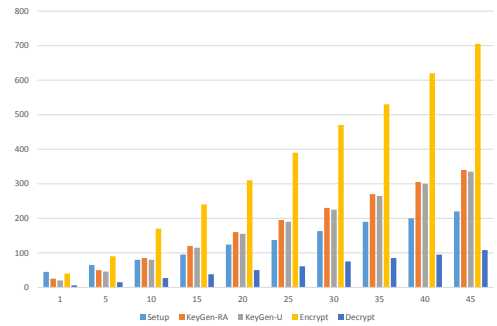

Fig. 5 Relationship between the number of attributes and the computation time for each operation in milliseconds

expressiveness, and enable new modes of operation. Another challenge is in establishing the access control policy model. Existing and new access control policies has to be translated into ABE access trees. Integration with the application and network layer is another challenge. We envision ABE to provide security at the application layer to provide fine-grained security, and interoperate with a pre-shared key scheme at the network layer providing coarse-grained security.Performance and computational complexity is a basic short-coming of ABE. We are able to achieve somewhat acceptable performance with the current implementation. We intend to develop a high performance implementation and protocols for caching and pre-computation that can further alleviate the computation load. We have demonstrated the feasibility of our enhanced ABE algorithm in sending data. The next step is to apply it to a real-world application and network.

REFERENCES

[1] B. A. Weiss, L. Fronczek, E. Morse, Z. Kootbally, and C. Schlenoff, "Performance assessments of android-powered military applications operating on tactical handheld devices," in *Mobile Multimedia/Image Processing, Security, and Applications 2013*, vol. 8755. International Society for Optics and Photonics, 2013, p. 875504.

[2] B. J. Ewy, M. T. Swink, S. G. Pennington, J. B. Evans, J. M. Kim, C. Ling, S. L. Earp, and M. Maeda, "Tigr in iraq and afghanistan: Network-adaptive distribution of media rich tactical data," in *Military Communications Conference, 2009. MILCOM 2009. IEEE*. IEEE, 2009, pp. 1–7.

[3] J. B. Evans, B. J. Ewy, M. T. Swink, S. G. Pennington, D. J. Siquieros, and S. L. Earp, "Tigr: the tactical ground reporting system," *IEEE Communications Magazine*, vol. 51, no. 10, pp. 42–49, 2013.

[4] M. R. Brannsten, T. H. Bloebaum, F. T. Johnsen, and B. K. Reitan, "Kings eye: Platform independent situational awareness," in *Military Communications and Information Systems (ICMCIS), 2017 International Conference on*. IEEE, 2017, pp. 1–5.

[5] W. Mitchell, "Project kitae part i battlespace agility in helmand: Network vs. hierarchy c2," 2011.

[6] S. H. Lee, S. Lee, H. Song, and H. S. Lee, "Wireless sensor network design for tactical military applications: Remote large-scale environments," in *Military communications conference, 2009. MILCOM 2009. IEEE*. IEEE, 2009, pp. 1–7.

[7] M. P. DJurišić, Z. Tafa, G. Dimić, and V. Milutinović, "A survey of military applications of wireless sensor networks," in *Embedded Computing (MECO), 2012 Mediterranean Conference on*. IEEE, 2012, pp. 196–199.

[8] D. Singh, G. Tripathi, A. M. Alberti, and A. Jara, "Semantic edge computing and iot architecture for military health services in battlefield," in *Consumer Communications & Networking Conference (CCNC), 2017 14th IEEE Annual*. IEEE, 2017, pp. 185–190.

[9] A. Raglin, S. Metu, S. Russell, and P. Budulas, "Implementing internet of things in a military command and control environment," in *Next-Generation Analyst V*, vol. 10207. International Society for Optics and Photonics, 2017, p. 1020708.

[10] L. Young and M. Ishii, "One force tactical communications system: Connecting the tactical edge at aewe spiral g," in *MILITARY COMMUNICATIONS CONFERENCE, 2012-MILCOM 2012*. IEEE, 2012, pp. 1–4.

[11] A. Blair, T. Brown, K. M. Chugg, and M. Johnson, "Tactical mobile mesh network system design," in *Military Communications Conference, 2007. MILCOM 2007. IEEE*. IEEE, 2007, pp. 1–7.

[12] G. Henderson, W. Pase *et al.*, "Emerging radio and manet technology study: Research support for a survey of state-of-the-art commercial and military hardware/software for mobile ad hoc networks," Bell Canada Ottawa, Ontario Canada, Tech. Rep., 2014.

[13] Y. Sun and K. R. Liu, "Hierarchical group access control for secure multicast communications," *IEEE/ACM Transactions on Networking*, vol. 15, no. 6, pp. 1514–1526, 2007.

[14] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proceedings of the 13th ACM conference on Computer and communications security*. Acm, 2006, pp. 89–98.

[15] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Security and Privacy, 2007. SP'07. IEEE Symposium on*. IEEE, 2007, pp. 321–334.

[16] A. Fongen and M. Salmanian, "Communities of trust in tactical coalition networks," in *Military Communications Conference (MILCOM), 2014 IEEE*. IEEE, 2014, pp. 67–73.

[17] M. Salmanian, J. D. Brown, S. Watson, R. Song, H. Tang, and D. Simmelink, "An architecture for secure interoperability between coalition tactical manets," in *Military Communications Conference, MILCOM 2015-2015 IEEE*. IEEE, 2015, pp. 37–42.

[18] A. Armando, M. Grasso, S. Oudkerk, S. Ranise, and K. Wrona, "Content-based information protection and release in nato operations," in *Proceedings of the 18th ACM symposium on Access control models and technologies*. ACM, 2013, pp. 261–264.

[19] B. Lynn *et al.*, "Pbc: The pairing-based cryptography library," *http://crypto. stanford. edu/pbc*, 2011.