Volume No:3, Issue No:6 (November-2017) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

An Efficient Data Retrieval for Decentralized Disruption-Tolerant Military Networks

A.V.V.S.Manoj
Department of Computer Science Technology
Sanketika Vidya Parishad Engineering College, Pothinamallayyapalem, Visakhapatnam - 530041, A.P, India.

R.Satya Ravindra Babu
Department of Computer Science Technology
Sanketika Vidya Parishad Engineering College, Pothinamallayyapalem, Visakhapatnam - 530041, A.P, India.

ABSTRACT:

Target Tracking is an important problem in sensor networks, where it dictates how accurate a targets position can be measured. In response to the recent surge of interest in mobile sensor applications, this paper studies the target tracking problem in a mobile sensor network (MSN), where it is believed that mobility can be exploited to improve the tracking resolution. This problem becomes particularly challenging given the mobility of both sensors and targets, in which the trajectories of sensors and targets need to be captured. We derive the inherent relationship between the tracking resolution and a set of crucial system parameters including sensor density, sensing range, sensor and target mobility. We investigate the correlations and sensitivity from a set of system parameters and we derive the minimum number of mobile sensors that are required to maintain the resolution for target tracking in an MSN. The simulation results demonstrate that the tracking performance can be improved by an order of magnitude with the same number of sensors when compared with that of the static sensor environment.

I. Introduction

The development of sensor network technology has enabled the possibility of target detection and tracking in a largescale environment. There has been an increased interest in the deployment of mobile sensors for target tracking, partly motivated by the demand of habitat monitoring and illegal hunting tracking for rare wild animals [1]. In this paper, we are primarily interested in target tracking by considering both moving targets and mobile sensors as shown in Figure 1. Specifically, we are interested in the spatial resolution for localizing a target's trajectory. The spatial resolution refers to how accurate a target's position can be measured by sensors, and defined as the worst-case deviation between the estimated and the actual paths in wireless sensor networks [2]. Our main objectives are to establish the theoretical framework for target tracking in mobile sensor networks, and quantitatively demonstrate how the mobility can be exploited to improve the tracking performance. Given an initial sensor deployment over a region and a sensor mobility pattern, targets are assumed to cross from one boundary of the region to another. We define the spatial resolution as the deviation between the estimated and the actual target traveling path, which can also be explained as the distance that a target is not covered by any mobile sensors.

Given the mobility of both targets and sensors mobility, it is particularly challenging to model such a stochastic problem for multiple moving objects. Furthermore, we are also interested in determining the minimum number of mobile sensors that needs to be deployed in order to provide the spatial resolution in mobile sensor networks. It turns out that our problem is very similar to the collision problem in classical kinetic theory of gas molecules in physics, which allows us to establish and derive the inherently dynamic relationship between moving targets and mobile sensors. The binary sensing model of tracking for wireless sensor networks has been studied in several prior works. The work in [3] showed that a network of binary sensors has geometric properties that can be used to develop a solution for tracking with binary sensors. Another work [4] also considered a binary sensing model. It employed piecewise linear path approximations computed using variants of a weighted centroid algorithm, and obtained good tracking performance if the trajectory is smooth enough.

Cite this article as: A.V.V.S.Manoj & R.Satya Ravindra Babu, "An Efficient Data Retrieval for Decentralized Disruption-Tolerant Military Networks", International Journal of Research in Advanced Computer Science Engineering, Volume 3 Issue 6, 2017, Page 30-38.

Volume No:3, Issue No:6 (November-2017) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

A follow-up work explored fundamental performance limits of tracking a target in a two-dimensional field of binary proximity sensors, and designed algorithms that attained those limits in [5]. Prior works in stationary wireless sensor networks have studied the fundamental limits of tracking performance in term of spatial resolution. Our focus in this paper is completely different from all prior works. There are two distinctive features of our work:

1) We try to identify and characterize the dynamic aspects of the target tracking that depend on both sensor and target mobility;

2) We consider tracking performance metrics: spatial resolution in a mobile sensor network. By leveraging the kinetic theory from physics, we model the dynamic problem, and examine its sensitivity under different network parameters and configurations. To the best of our knowledge, we believe this is a completely new study of target tracking in mobile sensor networks.

The rest of this paper is organized as follows. Section II describes the network and mobility model, as well as defining the target tracking problem in a mobile sensor network. Section III formulates the target tracking problem. Section IV examines the tracking performance sensitivity under different network parameters and configurations, and finally Section V concludes the paper.

II. Network Archetecture

In this section, we describe the DTN architecture and define the security model.

Fig: 1. Architecture of secure data retrieval in a disruption-tolerant military network.

System Description and Assumptions

Fig. 1 shows the architecture of the DTN. As shown in Fig 1,the architecture consists of the following system entities.

1) Key Authorities: They are key generation centers that generate public/secret parameters for CP-ABE. The key authorities consist of a central authority and multiple local authorities. We assume that there are secure and reliable communication channels between a central authority and each local authority during the initial key setup and generation phase. Each local authority manages different attributes and issues corresponding attribute keys to users. They grant differential access rights to individual users based on the users' attributes. The key authorities are assumed to be honest-but-curious. That is, they will honestly execute the assigned tasks in the system [6], however they would like to learn information of encrypted contents as much as possible.

2) Storage node: This is an entity that stores data from senders and provide corresponding access to users. It may be mobile or static [4], [5]. Similar to the previous schemes, we also assume the storage node to be semitrusted, that is honest-but-curious.

3) Sender: This is an entity who owns confidential messages or data (e.g., a commander) and wishes to store them into the external data storage node for ease of sharing or for reliable delivery to users in the extreme networking environments. A sender is responsible for defining (attribute based) access policy and enforcing it on its own data by encrypting the data under the policy before storing it to the storage node.

4) User: This is a mobile node who wants to access the data stored at the storage node (e.g., a soldier). If a user possesses a set of attributes satisfying the access policy of the encrypted data defined by the sender, and is not revoked in any of the attributes, then he will be able to decrypt the ciphertext and obtain the data.

Since the key authorities are semi-trusted, they should be deterred from accessing plaintext of the data in the storage node; meanwhile, they should be still able to issue secret keys to users. In order to realize this

Volume No:3, Issue No:6 (November-2017) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

somewhat contradictory requirement, the central authority and the local authorities engage in the arithmetic 2PC protocol with master secret keys of their own and issue independent key components to users during the key issuing phase. The 2PC protocol [7] prevents them from knowing each other's master secrets so that none of them can generate the whole set of secret keys of users individually. Thus, we take an assumption that the central authority does not collude with the local authorities (otherwise, they can guess the secret keys of every user by sharing their master secrets)

.

Threat Model and Security Requirements

1) Data confidentiality: Unauthorized users who do not have enough credentials satisfying the access policy should be deterred from accessing the plain data in the storage node. In addition, unauthorized access from the storage node or key authorities should be also prevented.

2) Collusion-resistance: If multiple users collude, they may be able to decrypt a ciphertext by combining their attributes even if each of the users cannot decrypt the ciphertext alone [1]–[3]. For example, suppose there exist a user with attributes {"Battalion 1", "Region 1"} and another user with attributes {"Battalion 2", "Region 2"}. They may succeed in decrypting a ciphertext encrypted under the access policy of ("Battalion 1" AND "Region 2"), even if each of them cannot decrypt it individually. We do not want these colluders to be able to decrypt the secret information by combining their attributes. We also consider collusion attack among curious local authorities to derive users' keys.

3) Backward and forward Secrecy: In the context of ABE, backward secrecy means that any user who comes to hold an attribute (that satisfies the access policy) should be pre-vented from accessing the plaintext of the previous data exchanged before he holds the attribute. On the other hand, forward secrecy means that any user who drops an attribute should be prevented from accessing the plaintext of the subsequent data exchanged after he drops the attribute, unless the other valid attributes that he is holding satisfy the access policy [8].

III. Preliminaries And Difinition

Cryptographic Background

We first provide a formal definition for access structure recapitulating the definitions in [2] and [3]. Then, we will briefly review the necessary facts about the bilinear map and its security assumption.

1) Access Structure: Let $\{P_1,P_2,\ldots P_n\}$ be a set of parties. A collection $\mathbb{A} \subseteq 2^{\{P_1,P_2,\ldots,P_n\}}$ is monotone if $\forall B, C$: If $B \in \mathbb{A}$ and $B \subseteq C$, then $C \in \mathbb{A}$. An access structure (respectively, monotone access structure) is a collection (respectively, monotone collection) $\mathbf{A}$ of nonempty subsets of $\{p_1, p_2, p_3, \ldots p_n\}$, i.e., $\mathbf{A}$ is subset of $2^{\{P1,P2,..Pn\}}\backslash\{\emptyset\}$. The sets in $\mathbf{A}$ are called the authorized sets, and the sets not in $\mathbf{A}$ are called the unauthorized sets.

In the proposed scheme, the role of the parties is taken by the attributes. Thus, the access structure $\mathbf{A}$ will contain the authorized sets of attributes. From now on, by an access structure, we mean a monotone access structure.

2) Bilinear Pairings: Let G_0 and G_1 be a ultiplicative cyclic group of prime order p. Let g be a generator of G_0. A map $e : G_0 \times G_0 \rightarrow G_1$ is said to be bilinear if $e(P^a, Q^b) = e(P,Q)^{ab}$ for all P,Q belongs to G_0 and all a,b belogs to Z^*_p, and and non degenerate $e(g,g) \neq 1$ if for the generator g of G_0.

We say that G_0 is a bilinear group if the group operation in G_0 can be computed efficiently and there exists G_1 for which the bilinear map $e : G_0 \times G_0 \rightarrow G_1$ is efficiently computable.

IV. PROPOSED SYSTEM

We are primarily interested in target tracking by considering both moving targets and mobile sensors as shown in Figure 1. Specifically, we are interested in the spatial resolution for localizing a target's trajectory. The spatial resolution refers to how accurate a target's position can be measured by sensors, and defined as the

Volume No:3, Issue No:6 (November-2017) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

worst-case deviation between the estimated and the actual paths in wireless sensor networks [2]. Our main objectives are to establish the theoretical framework for target tracking in mobile sensor networks, and quantitatively demonstrate how the mobility can be exploited to improve the tracking performance. Given an initial sensor deployment over a region and a sensor mobility pattern, targets are assumed to cross from one boundary of the region to another. We define the spatial resolution as the deviation between the estimated and the actual target traveling path, which can also be explained as the distance that a target is not covered by any mobile sensors.

A. Access Tree

1) Description: Let be a tree representing an access structure.

Each nonleaf node of the tree represents a threshold gate. If num_x is the number of children of a node x and k_x is its threshold value, then $0 \leq k_x \leq num_x$. Each leaf node of the tree is described by an attribute and a threshold value $k_x = 1$. λ_x denotes the attribute associated with the leaf node in the tree. p(x) represents the parent of the node in the tree. The children of every node are numbered from 1 to num. The function index(x) returns such a number associated with the node. The index values are uniquely assigned to nodes in the access structure for a given key in an arbitrary manner.

B. Revocation

We observed that it is impossible to revoke specific attribute keys of a user without rekeying the whole set of key components of the user in ABE key structure since the whole key set of a user is bound with the same random value in order to prevent any collusion attack. Therefore, revoking a single attribute in the system requires all users who share the attribute to update all their key components even if the other attributes of them are still valid. This seems very inefficient and may cause severe overhead in terms of the computation and communication cost, especially in large-scaled DTNs.

For example, suppose that a user $\mathbf{u_t}$ is qualified with **l** different attributes. Then, all **l** attribute keys of the user $\mathbf{u_t}$ are generated with the same random number $\mathbf{r_t}$ in the ABE key architecture. When an attribute of the user is required to be revoked (**l – 1** other attribute keys of the user are still valid), the other valid **l – 1** keys should be updated with another new $\mathbf{r'_t}$ that is different from $\mathbf{r_t}$ and delivered to the user. Unless the other keys **l - 1** are updated, the attribute key that is to be revoked could be used as a valid key until their updates since it is still bound with the same $\mathbf{r_t}$. Therefore, in order to revoke a single attribute key of a user, **O(l)** keys of the user need to be updated. If **n** users are sharing the attribute, then total **O(nl)** keys need to be updated in order to revoke just a single attribute in the system.

V. ANALYSIS

In this section, we first analyze and compare the efficiency ofthe proposed scheme to the previous multi authority CP-ABE schemes in theoretical aspects. Then, the efficiency of the proposed scheme is demonstrated in the network simulation in terms of the communication cost. We also discuss its efficiency when implemented with specific parameters and compare these results to those obtained by the other schemes.

Table I
EXPRESSIVENESS, KEY ESCROW, AND REVOCATION ANALYSIS

Scheme	Authority	Expressiveness	Key Escrow	Revocation
BSW [13]	single	-	yes	periodic attribute revocation
HV [9]	multiple	AND	yes	periodic attribute revocation
RC [4]	multiple	AND	yes	immediate system-level user revocation
Proposed	multiple	any monotone access structure	no	immediate attribute-level user revocation

A. Efficiency

Table I shows the authority architecture, logic expressiveness of access structure that can be defined under different disjoint sets of attributes (managed by different authorities), key escrow, and revocation granularity of each CP-ABE scheme. In the proposed

Volume No:3, Issue No:6 (November-2017) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

scheme, the logic can be very expressive as in the single authority system like BSW [3] such that the access policy can be expressed with any monotone access structure under attributes of any chosen set of authorities; while HV [9] and RC [4] schemes only allow the AND gate among the sets of attributes managed by different authorities. The revocation in the proposed scheme can be done in an immediate way as opposed to BSW. Therefore, attributes of users can be revoked at any time even before the expiration time that might be setto the attribute. This enhances security of the stored data by reducing the windows of vulnerability. In addition, the proposed scheme realizes more fine-grained user revocation for each attribute rather than for the whole system as opposed to RC. Thus, even if a user comes to hold or drop any attribute during the service in the proposed scheme, he can still access the data with other attributes that he is holding as long as they satisfy the access policy defined in the ciphertext. The key escrow problem is also resolved in the proposed scheme such that the confidential data would not be revealed to any curious key authorities.

Table II
EFFICIENCY ANALYSIS

System	Ciphertext size	Rekeying message	Private key size	Public key size
BSW [13]	$(2t+1)C_0+C_1+C_\mathcal{T}$	$l(2k+1)C_0$	$(2k+1)C_0$	C_0+C_1
HV [9]	$(2t+m)C_0+mC_1+C_\mathcal{T}$	$l(2k+1)C_0$	$(2k+m)C_0$	mC_0+mC_1
RC [4]	$(2t+3r+m)C_0+mC_1+C_\mathcal{T}$	0	$(3k+2m)C_0$	$m(t+4)C_0+mC_1$
Proposed	$(2t+1)C_0+C_1+C_\mathcal{T}$	$(n-l)\log\frac{n}{n-l}C_p$	$(2k+1)C_0+\log nC_k$	C_0+mC_1

C_0: bit size of an element in $\mathbb{G}_0$, C_1: bit size of an element in $\mathbb{G}_1$, C_p: bit size of an element in $\mathbb{Z}_p^*$,
C_k: bit size of a KEK, $C_\mathcal{T}$: bit size of an access tree $\mathcal{T}$ in the ciphertext, r: the number of revoked users,
l: the number of users in an attribute group, n: the number of all users in the system,
m: the number of authorities in the system, k: the number of attributes associated with private key of a user,
u: the number of attributes in the system, t: the number of attributes appeared in $\mathcal{T}$.

Table II summarizes the efficiency comparison results among CP-ABE schemes. In the comparison, rekeying message size represents the communication cost that the key authority or the storage node needs to send to update non revoked users' keys for an attribute. Private key size represents the storage cost required for each user to store attribute keys or KEKs. Public key size represents the size of the system public parameters. In this comparison, the access tree is constructed with attributes of **m** different authorities except in BSW of which total size is equal to that of the single access tree in BSW. As shown in Table II, the proposed scheme needs rekeying message **(Hdr)** size of at most $\mathbf{(n\text{-}l)\log^{n/(n-1)}}$ to realize user-level access control for each attribute in the system. Although RC does not need to send additional rekeying message for user revocations as opposed to the other schemes, its ciphertext size is linear to the number of revoked users in the system since the user revocation message is included in the ciphertext. The proposed scheme requires a user to store **log(n)** more KEKs than BSW. However, it has an effect on reducing the rekeying message size. The proposed scheme is as efficient as the basic BSW in terms of the ciphertext size while realizing more secure immediate rekeying in multi authority systems.

B. Simulation

In this simulation, we consider DTN applications using the Internet protected by the attribute-based encryption. Almeroth and Anmar [2] demonstrated the group behavior in the Internet's multicast backbone network (MBone). They showed that the number of users joining a group follows a Poisson distribution with rate **~λ**, and the membership duration time follows an exponential distribution with a mean duration **1/μ**. Since each attribute group can be shown as an independent network multicast group where the members of the group share a common attribute, we show the simulation result following this probabilistic behavior distribution.

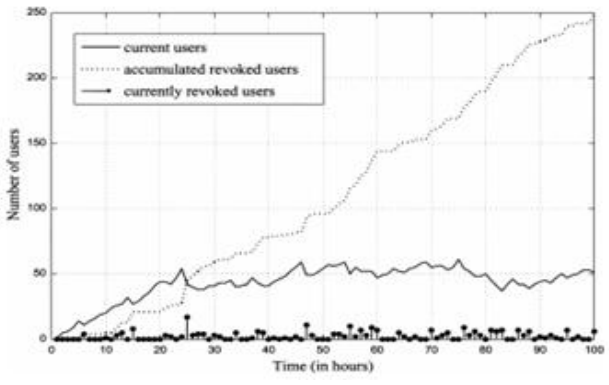

Fig2: Number of users in attribute group

Volume No:3, Issue No:6 (November-2017) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

We suppose that user join and leave events are independently and identically distributed in each attribute group following Poisson distribution. The membership duration time for an attribute is assumed to follow an exponential distribution. We set the interarrival time between users as 20 min **(~λ = 3)** and the average membership duration time as 20 h **(1/μ = 20)**.

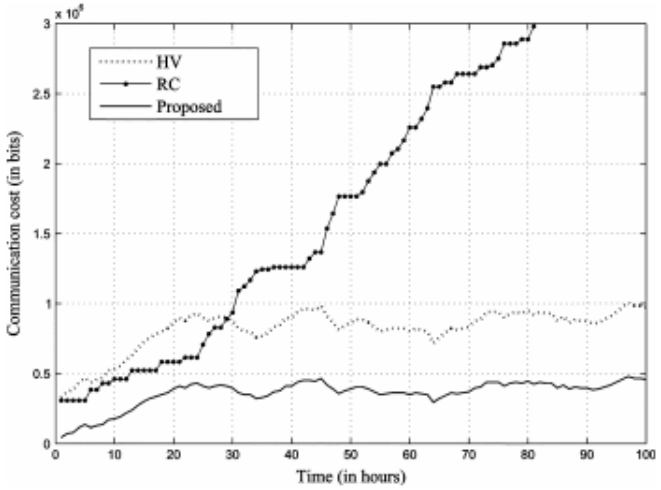

fig3: communication cost in the multi authority CP-ABP system

Fig. 2 represents the number of current users and revoked users in an attribute group during 100 h. Fig. 3 shows the total communication cost that the sender or the storage node needs to send on a membership change in each multiauthority CP-ABE scheme. It includes the ciphertext and rekeying messages for nonrevoked users. It is measured in bits. In this simulation, the total number of users in the network is 10 000, and the number of attributes in the system is 30. The number of the key authorities is 10, and the average number of attributes associated with a user's key is 10. For a fair comparison with regard to the security perspective, we set the rekeying periods in HV as **1/(~λ)** min. To achieve an 80-bit security level, we set $\mathbf{C_0 = 512}$, $\mathbf{C_p = 160}$. **CT** is not added to the simulation result because it is common in all multiauthority CP-ABE schemes. As shown in Fig. 3, the communication cost in HV is less than RC in the beginning of the simulation time (until about 30 h). However, as the time elapses, it increases conspicuously because the number of revoked users increases accumulatively. The proposed scheme requires the least communication cost in the network system since the rekeying message in is **Hdr** comparatively less than the other multiauthority schemes.

Implementation

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.

The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

Modules:

1. Mobile user Attackers Modules.
2. Tracker Sensor Routing Techniques.
3. Adversary Model.
4. Privacy Evaluation Model.
5. Security Analysis.

1. Tracker Attackers Modules:

The appearance of an endangered mobile user tracker (Attackers) in a monitored area is survived by wireless sensor, at the each time the inside and outside sensors are sensing to find out the attackers location and the timing. This information is passed to the server for analyzing. After analyzing the commander and tracker they are also can participate this wireless network. In the commander and tracker itself some intruders are there, our aim to capture the attackers before attempting the network.

2. Tracker Sensor Routing Techniques:

This section presents two techniques for privacy-preserving routing in sensor networks, a periodic collection method and a source simulation method. The

Volume No:3, Issue No:6 (November-2017) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

periodic collection method achieves the optimal location privacy but can only be applied to applications that collect data at a low rate and do not have strict requirements on the data delivery latency. The source simulation method provides practical trade-offs between privacy, communication cost, and latency; it can be effectively applied to real-time applications. In this paper, we assume that all communication between sensor nodes in the network is protected by pair wise keys so that the contents of all data packets appear random to the Global eavesdropper. This prevents the adversary from correlating different Data packets to trace the real object.

3. Adversary Model:

For the kinds of wireless sensor networks that we envision, we expect highly-motivated and well-funded attackers whose objective is to learn sensitive location-based information. This information can include the location of the events detected by the target sensor network such as the presence of a mobile user. The Mobile user-tracker example application was introduced in, and we will also use it to help describe and motivate our techniques. In this application, a sensor network is deployed to track endangered giant mobile users in a bamboo forest. Each mobile user has an electronic tag that emits a signal that can be detected by the sensors in the network. A clever and motivated poacher could use the communication in the network to help him discover the locations of mobile users in the forest more quickly and easily than by traditional tracking techniques.

In any case, it should be feasible to monitor the communication patterns and locations of events in a sensor network via global eavesdropping. An attacker with this capability poses a significant threat to location privacy in these networks, and we therefore focus our attention to this type of attacker.

4. Privacy Evaluation Model:

In this section, we formalize the location privacy issues under the global eavesdropper model. In this model, the adversary deploys an attacking network to monitor the sensor activities in the target network. We consider a powerful adversary who can tracker the communication of everySensor node in the target network. Every sensor node i in the target network is an observation point, which produces an observation (i, t, d) whenever it transmits a packet d in the target network at time t. In this paper, we assume that the attacker only monitors the wireless channel and the contents of any data packet will appear random to him.

5. Security Analysis:

The generation number of a packet can be hidden in the secure routing scheme through link-to-link encryption. In this way, attackers cannot find the generation number of a packet for their further analysis. Notice that secure routing paths are only required to be established at the beginning of each session; during the packet transmission, secure routing paths are not required to change or re-established for each new generation.

Table III
COMPARISON OF COMPUTATION COST

		Pairing	Exp. in $\mathbb{G}_0$	Exp. in $\mathbb{G}_1$	Computation (ms)
Time (ms)		2.9	1.0	0.2	
BSW [13]	S		$2t+1$	1	$2t+1.2$
	U	$2k+1$		$\log t$	$5.8k+0.2\log t$ $+2.9$
HV [9]	S		$2t+1$	1	$2t+1.2$
	U	$2k+m$		$m\log(t/m)$	$5.8k+2.9m$ $+0.2m\log(t/m)$
RC [4]	S		$3t+1$	1	$3t+1.2$
	U	$3k+m$		$m\log(t/m)$	$8.7k+2.9m$ $+0.2m\log(t/m)$
Proposed	S		$2t+1$	1	$2t+1.2$
	U	$2k+1$	k	$\log t$	$6.8k+0.2\log t$ $+2.9$

S: sender, U: user

Table III shows shows the computational time results. For each operation, we include a benchmark timing. Each cryptographic operation was implemented using the PBC library anad the computational time results. For each operation, we include a benchmark timing. The public key parameters were selected to provide 80-bit

Volume No:3, Issue No:6 (November-2017) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

security level. The implementation uses a 160-bit elliptic curve group based on the supersingular curve $y2 = x^2 + x$ over a 512-bit finite field. The omputational cost is analyzed in terms of the pairing, exponentiation operations in G_0 and G_1. The comparatively negligible hash, symmetric key, and multiplication operations in the group are ignored in the time result. In this analysis, we assume that the access tree in the ciphertext is a complete binary tree.

VI. SECURITY

In this section, we prove the security of our scheme with regard to the security requirements discussed in Section II.

A. Collusion Resistance

In CP-ABE, the secret sharing must be embedded into the ciphertext instead to the private keys of users. Like the previous ABE schemes [5], [7], the private keys **(SK)** of users are randomized with personalized random values selected by the **CA** such that they cannot be combined in the proposed scheme. In order to decrypt a ciphertext, the colluding attacker should recover $e(g,g)^{(a1+a2+...am)s}$. To recover this, the attacker must pair C_y from the ciphertext and D_y from the other colluding users' private keys for an attribute λ_y(we suppose that the attacker does not hold the attribute λ_y). However, this results in the value $e(g,g)^{(a1+a2+...am)s}$ blinded by some random value, which is uniquely assigned to each user, even if the attribute group keys for the attributes that the user holds are still valid. This value can be blinded out if and only if the user has the enough key components to satisfy the secret sharing scheme embedded in the ciphertext. Another collusion attack scenario is the collusion between revoked users in order to obtain the valid attribute group keys for some attributes that they are not authorized to have (e.g., due to revocation). The attribute group key distribution protocol, which is complete subtree method in the proposed scheme, is secure in terms of the key indistinguishability [9]. Thus, the colluding revoked users can by no means obtain any valid attribute group keys for attributes that they are not authorized to hold. Therefore, the desired value $e(g,g)^{(a1+a2+...am)s}$ cannot be recovered by collusion attack since the blinding value is randomized from a particular user's private key.

B. Backward and Forward Secrecy

When a user comes to hold a set of attributes that satisfy the access policy in the ciphertext at some time instance, the corresponding attribute group keys are updated and delivered to the valid attribute group members securely (including the user). In addition, all of the components encrypted with a secret key **s** in the ciphertext are reencrypted by the storage node with a random s^r, and the ciphertext components corresponding to the attributes are also reencrypted with the updated attribute group keys. Even if the user has stored the previous ciphertext exchanged before he obtains the attribute keys and the holding attributes satisfy the access policy, he cannot decrypt the pervious ciphertext. This is because, even if he can succeed in computing $e(g,g)^{r(s+sr)}$ from the current ciphertext, it will not help to recover the desired value $e(g,g)^{(a1+a2+...am)s}$ for the previous ciphertext since it is blinded by a random s^r. Therefore, the backward secrecy of the stored data is guaranteed in the proposed scheme.

On the other hand, when a user comes to drop a set of attributes that satisfy the access policy at some time instance, the corresponding attribute group keys are also updated and delivered to the valid attribute group members securely (excluding the user). Then, all of the components encrypted with a secret key **s** in the ciphertext are reencrypted by the storage node with a random s^r, and the ciphertext components corresponding to the attributes are also reencrypted with the updated attribute group keys. Then, the user cannot decrypt any nodes corresponding to the attributes after revocation due to the blindness resulted from newly updated attribute group keys. In addition, even if the user has recovered $e(g,g)^{(a1+...am)s}$ before he was revoked from the attribute groups and stored it, it will not help to decrypt the subsequent ciphertext $e(g,g)^{(a1+...+am)(s+sr)}$ re-

Volume No:3, Issue No:6 (November-2017) ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

encrypted with a new random $\mathbf{s}^r$. Therefore, the forward secrecy of the stored data is guaranteed in the proposed scheme.

VII. CONCLUSION

In this paper, we have studied the target tracking problem in mobile sensor networks. Specifically, we introduce performance metrics: spatial resolution and we investigate the resolution against moving targets. By modeling the dynamic aspects of the target tracking that depend on both sensor and target mobility, we derive the inherent relationship between the spatial resolution and a set of crucial system parameters including sensor density, sensing range, sensor and target mobility. The results demonstrated that mobility can be exploited to obtain better spatial resolution. There are several avenues for further research on this problem: (1) to consider the detection error of mobile sensors under varying sensor speeds. This can be formulated into an optimization problem for target tracking; (2) to refine the sensor mobility model, the network model, and the communication model among sensors in order to enable effective detection and tracking. For example, a practical distributed target tracking and sensing information exchange protocol becomes an interesting future research topic when sensors are required to trace the target paths.

VIII. REFERENCES

[1]. Greenpeace challenges japanese whaling industry with new satellitetracking system. In http://www.dailymail.co.uk/news/article-486608/, October 2007.

[2]. N. Shrivastava, R. Mudumbai, U. Madhow, and S.Suri. Target tracking with binary proximity sensors: Fundamental limits, minimal descriptions, and algorithms. In Proc. of SenSys. ACM, October 2006.

[3]. J. Aslam, Z. Butler, F. Constantin, V. Crespi, G. Cybenko, and D. Rus. Tracking a moving object with a binary sensor network. In Proc. Of SenSys. ACM, November 2003.

[4]. W. Kim, K. Mechitov, J.-Y. Choi, and S. Ham. On target tracking with binary proximity sensors. In Proc. of IPSN. IEEE, April 2005.

[5]. J. Singh, U. Madhow, R. Kumar, S. Suri, and R. Cagley. Tracking multiple targets using binary proximity sensors. In Proc. of IPSN. ACM, April 2007.

[6]. H. Zhang and J. C. Hou. Maintaining sensing coverage and connectivity in large sensor networks. Ad Hoc and Sensor Wireless Networks, 1(1- 2):89–124, March 2005.

[7]. M. Hefeeda and H. Ahmadi. Probabilistic coverage in wireless sensor networks. In Conference on Local Computer Networks (LCN). IEEE, November 2005.

[8]. T. Camp, J. Boleng, and V. Davies. A survey of mobility models for ad hoc network research. Wireless Communications and Mobile Computing, 2(5):483–502, September 2002.

[9]. R. Present. Kinetic Theory of Gases. McGraw-Hill Book, New York andLondon, 1958.