International Journal For Technological Research In Engineering
Volume 3, Issue 8, April-2016 *ISSN (Online): 2347 - 4718*

SHIELDED REPOSSESS DATA ON DISRUPTION-TOLERANT NETWORK

M.A Rama Prasad[1], Pradeep Kumar.P[2]
[1]Student of M.Tech (CSE), [2]Asst. Prof, Department of Computer Science and Engineering,
Chirala Engineering College, CHIRALA

ABSTRACT: In the corpulent number of outgrowing viable environment each and everything depends on the other sources to transmit the data securely and maintain the data as well in the familiar medium. Transferable nodes in military environments, for example, a adjoin line or a hostile area are prone to experience the under go of irregular system network and frequent partitions. Disruption-tolerant network (DTN) modernization are getting to be fruitful results that permit remote device conveyed by officers to speak with one another and access the confidential data or secret data or summon dependably by abusing outside facility nodes or storage nodes. Thus an innovative methodology is introduced to impart successful communication between each other in addition to access the confidential information present by some major authorities like commander or other superiors. The method is called Disruption-Tolerant Network (DTN). In many sensor applications, the data collected from individual nodes is aggregated at a base station or host computer. To reduce energy consumption, many systems also perform in-network aggregation of sensor data at intermediate nodes enroute to the base station. When any node within the group needs to transfer the data, it transfers slices of data to other nodes in that group, encrypted by individual authentication keys. Each receiving node decrypts, sums up the slices and transfers the encrypted data to the aggregator. The aggregator aggregates and encrypts the data with the shared secret key of the sink and forwards it to the sink. The set of nodes is reselected with new set of authentication keys in the second round of aggregation. By simulation results, we demonstrate that the proposed technique resolves the security threat of node capture attacks.

I. INTRODUCTION

Mobile nodes in a military environments as a battlefield or a hostile regions are likely to be suffer from an intermittent networks connectivity and frequent partitions and Disruption tolerant network (DTN) technologies are becoming a successful solutions that allow a wireless devices carried by a soldiers to communicate with each other's and access the confidential information's or command reliably by exploiting the external storage nodes. The most challenging issues are an enforcement of authorization policy and the policies update for a secure data retrieval. Cipher text policy attribute based encryption is a hopeful cryptographic emulsion to access control problems.

1.1 Wireless Sensor Networks

Wireless sensor networks consist of the latest technology that has attained notable consideration from the research community. Sensor networks consist of numerous low cost, little devices and are in nature self organizing ad hoc systems. The job of the sensor network is to monitor the physical environment, gather and transmit the information to other sink nodes. Generally, radio transmission ranges for the sensor networks are in the orders of the magnitude that is lesser that of the geographical scope of the unbroken network. Hence, the transmission of data is done from hop-by-hop to the sink in a multi-hop manner. Reducing the amount of data to be relayed thereby reduces the consumption of energy in the network. [1]. Wireless sensor network consists of a huge number of tiny electromechanical sensor devices that are capable of sensing, computing and communicating. These electromechanical sensor devices can be made use for gathering sensory information, like measurement of temperature from an extensive geographical area [2]. Many features of the wireless sensor networks have given rise to challenging problems [3]. The most important three characteristics are:

- Sensor nodes are exposed to maximum failures.
- Sensor nodes which make use of the broadcast communication pattern and have severe bandwidth restraint.
- Sensor nodes have inadequate amount of resources.

1.2 Data Aggregation

Data aggregation is considered as one of the basic dispersed data processing measures to save the energy and minimize the medium access layer contention in wireless sensor networks [4]. It is used as an important pattern for directing in the wireless sensor networks. The fundamental idea is to combine the data from different sources, redirect it with the removal of the redundancy and thereby reducing the number of transmissions and also saves energy [5]. The inbuilt redundancy in the raw data gathered from various sensors can be banned by the in-network data aggregation. In addition, these operations utilize raw materials to obtain application specific information. To conserve the energy in the system thereby maintaining longer lifetime in the network, it is important for the network to preserve high incidence of the in-network data aggregation [6].

II. NETWORK ARCHITECTURE

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

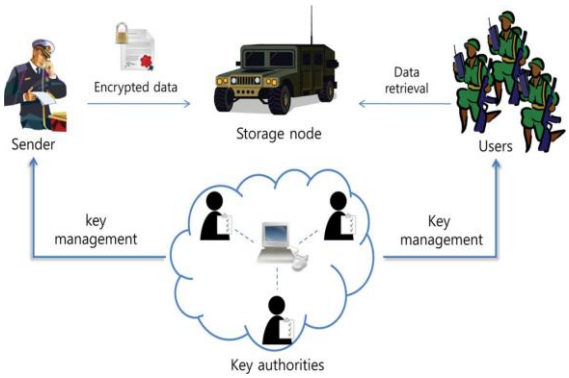

Fig.1. Architecture of the methodology to underrate routing incursion in informatics networks

A. 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; 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 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 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).

B. 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 cipher text by combining their attributes even if each of the users cannot decrypt the cipher text alone [11]–[13]. 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 cipher text 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 prevented 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.

III. IMPLEMENTATION

System Modules:

Secure Data retrieval is enhanced by using EMTS method and finding the location of users or nodes in DTN through Geographical Routing Algorithm.

The system is divided into four major modules:

- CP-ABE Encryption & Decryption
- InTrust Evaluation system
- Location Tracking

1) CP-ABE Encryption & Decryption:

This module describes how the key generating authority generates key for user. Key revocation for forward and backward secrecy and also solving key escrow problems. For each every step we need to concentrate on master key and private key of users.

There are key generation centres that generate public parameters for CP-ABE. It may consist of one central authority and multiple local authorities. For secure communication key authority generate attribute keys to the user. The next step is to encrypt the data to be stored in storage node securely. On receiving the request query from user the storage node respond to the user. Here sender can define the access policy under attributes. When user receives the cipher text from storage node, the user decrypts the cipher text with its secret key. On other hand, when a user comes to drop a set of attributes that satisfy the access policy

at some instance, the corresponding attribute group keys also updated and delivered to valid attribute group securely.

2) In Trust Evaluation system:

In this section, advocate that both social trust components such as connectivity, intimacy, honesty and unselfishness, and Qos trust components such as competence, reliability and delivery ratio be considered. Let X denote a trust component selected and let Tij Xt denote node i‟s assessment toward node j in trust property X at time t. When a trustor node (node i) evaluates a trustee node (node j) in the same level at time t, it updates Tij Xt as follows:

Tij

$Xt = 1 - \alpha XT$ij

$Xt - \Delta t + \alpha XT$i,j

X,direct t ifi ∧ jare1 – hop neighbours;

avg $1 - \gamma XT$ij

$Xt - \Delta t + \gamma XT$kj

X, recom t

$k \in Ni$

otherwise

If node i is a 1-hop neighbor of node j at time t, node i will use its direct observations Tij

X, direct t and past experiences

Tij $Xt - \Delta t$ where Δt is a trust update interval toward node j to update Tij . We use a design parameter αX with $0 \leq \alpha X \leq 1$ to weight these two contributions and to consider trust decay over time for trust property X. A larger αX means that trust evaluation will rely more on direct observations. Here Ti,jX,direct t indicates node i‟s trust value toward node j based on direct observations accumulated over the time period [0, t] possibly with a higher priority given to more recent interaction experiences. On the other hand, if node i is not a 1-hop neighbor of node j, node i will use its past experiences Tij$Xt - \Delta t$ and recommendations Tkj X ,recomm $t\ 's$ where k is a recommender to update TijXt .

Here TkjX,recomm t is the recommendation from node k toward node j in component X and can be just TijXt .A parameter γX is used here to weigh these two contributions and to consider trust decay over time as follows:

$\gamma X = \beta XT$ik $t1 + \beta XT$ik t

hop neighbors at time t for X=intimacy, honesty, unselfishness (social components) and competence (a Qos component) below.

Intimacy: This measures intimacy or closeness of node i toward node j. If there is a priori knowledge that node i is close to node j, e.g., deriving from a “friendship” matrix as input, then$T$i, jintimacy, direct t = 1. Otherwise node i can compute Ti, jintimacy, direct t by the ratio of the number of interactions it has with node j during $t - d\Delta t,t$ to the maximum number of interactions with any other node. Here d is the window size giving recent interaction experiences higher priority over ancient experiences.

Honesty: This refers to the belief of node i that node j is honest based on node i‟s direct observations during $t - d\Delta t,t$. Node i estimate Ti,jhonesty,direct$t$ by the ratio of the number of suspicious interaction experiences observed during $t - d\Delta t,t$ to a system honesty threshold to reduce false positives.

Unselfishness: This provides the belief of node I that node j is unselfishness based on direct observations during$t - d\Delta t,t$. Node i can estimate$T$i, jun selfishness, direct t by the ratio of the number of cooperative interaction experiences to the total number of protocol interaction experiences.

Competence: This refers to the belief of node i that node j,, s is competent at time t. Node i estimates$T$i, j competence, direct t by the ratio of the number of positive packet transmission experiences to the total number of packet transmission experiences.

3) Location Tracking:

A simple scheme is presented for geographic forwarding that is similar to Cartesian routing. Each node determines its own geographic position using a mechanism such as GPS; positions consist of latitude and longitude. A node announces its presence, position, and velocity to its neighbours (other nodes within radio range) by broadcasting periodic HELLO packets. Each node maintains a table of its current neighbours‟ identities and geographic positions. The header of a packet destined for a particular node contains the destination’s identity as well as its geographic position. When node needs to forward a packet toward location P, the node consults its neighbour table and chooses the neighbour closest to P. It then forwards the packet to that neighbour, which itself applies the same forwarding algorithm. The packet stops when it reaches the destination.

IV. RESULTS

The simulation studies involve the Disruption Tolerant Network. The proposed ETMS We perform secure data retrieval in proposed system by using Trust value and Threshold value of requesting node in military network. It helps in identifying the malicious nodes in DTN environment. From fig. 2. Trust threshold value gets calculated for requesting node in DTN. Social trust and Qos trust is calculated in fig.3 by checking the unselfishness, honesty, intimacy and competence

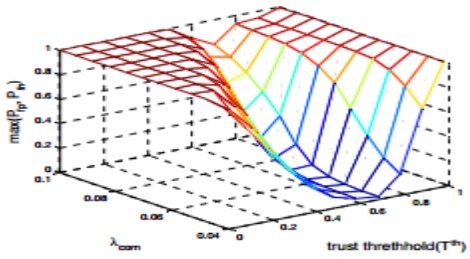

Fig.2. Analyzing the trust threshold

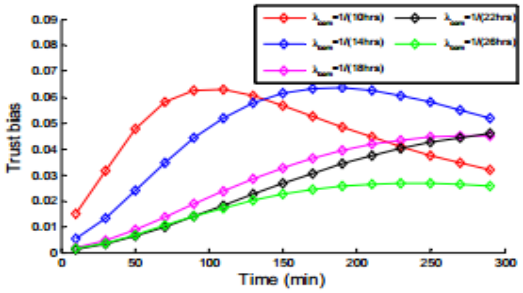

Fig.3. Calculating Trust Values

V. CONCLUSION

Our project is not the unique one, but is an Endeavour attempt to have a precise scenario of what the terms "the methodology to underrate routing incursion in informatics networks" is meant to be and its implementation as well on which we are currently working. As stated before, our proposed system can enhance the security of military network by using CP-ABE mechanism. CP-ABE is a scalable cryptographic solution to the access control and secures data retrieval issues. In this paper, we proposed an efficient and secure data retrieval method using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. The inherent key escrow problem is resolved such that the confidentiality of the stored data is guaranteed even under the hostile environment where key authorities might be compromised or not fully trusted. In addition, the fine-grained key revocation can be done for each attribute group. We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption- tolerant military network.

REFERENCES

[1] Muhammad Adnan Tariq, Boris Koldehofe, and Kurt Rothermel Securing Broker-Less Publish/Subscribe Systems Using Identity-Based Encryption. IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 2, FEBRUARY 2014

[2] M. Chuah and P. Yang, "Node density-based adaptive routing scheme for disruption tolerant networks," in Proc. IEEE MILCOM, 2006, pp.1–6.

[3] M. M. B. Tariq, M. Ammar, and E. Zequra, "Message ferry route design for sparse ad hoc networks with mobile nodes," in Proc. ACM MobiHoc, 2006, pp. 37–48.

[4] S. Roy and M. Chuah, "Secure data retrieval based on cipher text policy attribute-based encryption (CP-ABE) system for the DTNs," Lehigh CSE Tech. Rep., 2009.

[5] M. Chuah and P. Yang, "Performance evaluation of content-based information retrieval schemes for DTNs," in Proc. IEEE MILCOM, 2007, pp. 1–7.

[6] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable secure file sharing on untrusted storage," in Proc. Conf. File Storage Technol., 2003, pp. 29–42.

[7] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Mediated cipher text-policy attribute-based encryption and its application," in Proc. WISA, 2009, LNCS 5932, pp. 309–323.

[8] N. Chen, M. Gerla, D. Huang, and X. Hong, "Secure, selective group broadcast in vehicular networks using dynamic attribute based encryption," in Proc. Ad Hoc Netw. Workshop, 2010, pp. 1–8.

[9] D. Huang and M. Verma, "ASPE: Attribute-based secure policy enforcement in vehicular ad hoc networks," Ad Hoc Netw., vol. 7, no. 8, pp. 1526–1535, 2009.

[10] A. Lewko and B. Waters, "Decentralizing attribute-based encryption,"Cryptologye Print Archive: Rep. 2010/351, 2010.

[11] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Proc. Eurocrypt, 2005, pp. 457–473.

[12] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. ACM Conf. Comput. Commun. Security, 2006, pp. 89–98.

[13] J. Bethencourt, A. Sahai, and B. Waters, "Cipher text-policy attribute based encryption," in Proc. IEEE Symp. Security Privacy, 2007, pp. 321–334.

[14] R.Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," in Proc. ACM Conf. Comput. Commun. Security, 2007, pp. 195–203.

[15] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in Proc. ASIACCS, 2010, pp. 261–270.

[16] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in Proc. ACM Conf. Comput. Commun. Secure it

AUTHORS PROFILE

AUTHORS PROFILE

Pradeep kumar.p Presently pursuing his M.Tech in Computer Science & Engineering from Chirala Engineering College, Chirala, Prakasam District, A.P, India. Affiliated to Jawaharlal Nehru Technological University, Kakinada. Approved by AICTE, New Delhi. His B.Tech completed at Bapatla Engineering College Affiliated to ACHARYA NAGARJUNA University Guntur District, A.P, India.

M A RAMA PRASAD is an Assistant Professor in Computer Science& Engineering Department in Chirala Engineering College, Chirala, Prakasam District, A.P, India.

