ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

Secure Group Communication to Prevent Unauthorized Messages in DTN Based Mobile Ad Hoc Networks

Rekha A[1], Anitha P[2], Selva Priya G[3], Gayathri R Krishna[4], Minojini N[5]

PG Scholar, Dept. of CSE, Dr N.G.P. Institute of Technology, Tamil Nadu, India[1, 3, 4, 5]

Assistant Professor, Dept. of CSE, Dr N.G.P. Institute of Technology, Tamil Nadu, India[2]

ABSTRACT: To establish a communication among wireless devices and to retrieve the data securely Disruption tolerant network (DTN) is introduced. For maintaining the data confidential many cryptographic solutions are used. The issues in accessing the information is solved by the algorithm called Ciphertext Policy-Attribute Based Encryption. This has enormous challenge in providing security for the information. In decentralized DTN, CP-ABE is implemented with multiple key authorities that handle the attributes individually. Two party computation protocols are introduced in CP-ABE to protect the authority's interest in knowing the private keys created by others. The fine-drawn secret reversals are made for each and every feature set. Any monotone access structure can be used for creating the access policy in CP-ABE. In this the key authorities may be adjusted or not entirely believed. To maintain the trust partially the assumption is made such that the central authority does not conspiracy with local authority. To improve the trust we proposed an improved CP-ABE, in this we determine the trust of each user node in a network by estimating the trust of every node and updates the trust, so the user can have their trust in authority that generates the key for confidential data. By including the trust in CP-ABE, the users can trust the key authority for accessing the information securely. The privacy of the sending data and the data which are stored in storage node are maintained confidential by using the proposed system. Thus the proposed system has high degree of trust in the nodes.

KEYWORDS: DTN, ABE, CP-ABE, 2PC, Improved CP-ABE, Trust estimate

I. INTRODUCTION

Network security prevents the data in a network from unknown access. It contains the approval for accessing to information throughout a network and it is measured by network manager. The demand for security is to secure the information as well as provide authentication and access control for resources, guarantee accessibility of resources. A continuous arrangement of large network of moving devices that are not undivided wires is known as mobile ad hoc network (MANET). The MANET features are active topology like mobile devices join/leave the network unexpectedly; they will conjointly move freely, every node conjointly is router; facilitate to relay packets received from neighbors. An associate degree rising application area for MANETs is Wireless Sensor Network (WSN). The MANETs provisions for confidence are accessibility, authorization and vital administration, transparency of information, separation of information, non envy. Sensors, intermittent property, long-delay links, and assumptions that are essential for ancient revisiting are the most important matter in information system.

The challenged networks area unit containing options or needs a networking design designer would notice shocking or tough to reason, or in operation atmosphere makes communications tough. Challenging Environments are random or predictable node qualities like Military/tactical networks, Mobile routers with separation, regular plan for transportation moving by a small town, stages of whole separation, massive delays and low information measure, massive delays and high information measure. Disruption Tolerant Networking (DTN) is new space of analysis and standards with several application situations with distinctive properties. DTN routers type associate overlay network like solely nodes are selected that have persistent storage. This routing topology will be a time-varying impress like links come back and go,

10.15680/ijircce.2015.0304099

use any/all links which will presumably scheduled, predicted, or forced Links, could also be target aspect, may acquire from report to judge the plan. Fragmented messages supported dynamics are proactive fragmentation: optimization of contact volume, reactive fragmentation: resume wherever you ineffective. The information is encrypted to enhance the security between different hosts located in a network location. There are different types of encryption algorithms used for transferring the data securely.

Bethencourt et al. [6] generates Cipher text-Policy Attribute Based Encryption (CP-ABE). It is encrypted data for complex access power in a structure. The group of features produces the personal key for users. The policies are specified by the party who is encrypting data over the attributes that specifies which user can capable to decrypt. This procedure possesses the encrypted data as confidential and secure opposed to collusion resistance. The access policy can be of any monotone access structure, single power and regular feature revocation are available in this algorithm. Key escrow is not addressed. To overcome the limitations of previous CP-ABE are overcome and it is intended by Hur et al. [1]. Using this procedure, several problems solved are feature reversal, secret security and attributes coordination that are generated by different authorities. The essential secret security problem is determined where key authorities may be adjusted. For every feature collection the fine-grained key revocation need to be done. The mechanism of a fractional customized and attribute key to a user issued by the local authority is performed using a protocol known as secure 2PC with the central authority. The user attribute key can be updated individually and instantly. Therefore the accessibility and certainty can be enhanced.

Diffie-Hellman key exchange method is a way in which people may generate combined confidential information that cannot be estimated by snooper.

Trust relies on the fact that the trusted entities do not act maliciously. In ad hoc networks, nodes that have never met before can communication with each other based on a mutual trust relationships developed over an interval of occasion. Trust is subjective, asymmetric and time dependent. A trust relationship derived from direct interactions. The ability of trust relationship built from recommendations by a trusted node that generates a trust path known as indirect trust. The usage of proposals can speed up the convergence of the trust evaluating process.

II. RELATED WORK

A. Attribute-based encryption (ABE)

In DTNs, ABE is an assuring idea that fulfills the needs for retrieving data securely. ABE structure a method that permits control on data accessibility that is cryptographically encrypted, feature attributes among private keys and ciphertexts.

- Disadvantages

Few security and confidential challenges are proposed by DTNs when employing ABE in it. The problems are users private key may be compromised, some users can modify their associated attribute or to maintain confidentiality of users, key reversal is necessary. Multiple users in ABE reveal each attribute based on their satisfaction, the above problems will become more difficult.

B. Key-Policy Attribute-Based Encryption (KP-ABE)

In KP-ABE, the encryptor only gets to label a ciphertext with a set of features. The policy are chosen by the central authority which helps to identify the ciphertext that they may able to decrypt by the user. The authorities distributes key to all user with the help of accessing policy.

C. Decentralized ABE

Different authorities issue the combined access policy above the attribute through encrypting the data several times. The key drawback of this method is expressivity and effectiveness of access policy.

- Disadvantages

The periodic attribute revocable ABE schemes have two major difficulties: first difficulty is reduction in security in particulars of the backward and forward secrecy, second difficulty is in scalability. At regular intervals, the central authorization broadcast the updating material for key through transmission of data package to a single recipient on every time-slot provided that each non-revoked user may update their keys. The single attribute updation modifies the entire non-revoked users which share the attribute. Somewhat the above solutions still have absence in performance of effectiveness. Further down in decentralized ABE the access policy must only be AND, and it needs repeated encryption. Thus they are limited in particular of access policy expressiveness, computation requirement and costs for storage.

D. Ciphertext policy attribute based encryption (CP-ABE)

For decentralized DTNs to retrieve the data securely based on attribute by using CP-ABE [1]. The key issuing protocol produces and distributes secret keys for the user by a secure two-party computation (2PC) protocol among the central and local authorities with their own master confidences. The 2PC protocol prevents the key authorities from attaining some master confidential data of each other in particular that no one of them can produce the entire set of user keys alone. Every local authority generates partial custom-built and feature key mechanism to the user through 2PC protocol along with central authority. Every user attribute key is independently and instantaneously updated.

- Advantages

The CP-ABE system have the following success, first instant feature reversal improves backward/forward secrecy of confidential data by decreasing the windows of vulnerability, second encryptors could describe a fine-drawn access policy by any monotone access structure further down the attributes are generated by any chosen set of attributes and third is the key escrow problem is determined by an escrow-free key issuing protocol that accomplished the feature of the decentralized DTN architecture. The privacy of information and secrecy could be enforcing cryptographically in the CP-ABE scheme.

III. PROPOSED ALGORITHM

A. Framework of DTN:

Disruption-Tolerant Network (DTN) technologies allow nodes to communicate with each other in the boundary networking situations. It means where there is no end-to-end association between a source and a destination pair, the exchange of data from the source node should need to remain in the intermediate nodes for an considerable amount of period until the association would be finally established.

B. *Cipher text-Policy Attribute-Based Encryption*:

The key authority produce separate key for users through using the authority's master secret keys to the connected set of attributes of users. Therefore key authority may decrypt each ciphertext that are addressed to the particular users through creating their attribute keys. If the key authority in DTN can cooperate with the enemy when employed in militant surroundings that shall be the possible danger for the confidential information.

C. 2PC Protocol Design

The 2PC protocol prevents the key authorities from attaining a few master confidential data of every user so that no one can create the entire sets of user key. Therefore users are not essential to trust the authority fully in order to prevent their data that is distributed. The information secrecy and privacy are protected by cryptographical enforcement in opposition to all the key authorities. The 2PC protocol protects the key authority from witting other master confidential such that no one of a single authority can create the full set of confidential keys for separate users.

D. Estimating the trust of the node

Step 1: Trust node computation

The trust degree values evaluated by monitoring the behavior of the neighbors form the basic blocks upon which the model is built. In this section, we give the solution that is used for estimating the node trust. For the sake of simplicity and also to minimize the overhead, we use the forwarding ratio to calculate a node trust. The forwarding ratio is the number of packets forwarded correctly to the number of those supposed to be forwarded. Correct forwarding means node not only transmits a packet to its next hop but also forwards reliably. For instance, when a malicious neighbor forwards a data packet after tampering with data, this is not considered as correct forwarding. If a sender observes such a modification, the forwarding ratio of the neighbor would reduce. At time t, $T^{d}_{i,j}(t)$ is determined by node forwarding ratio of node j by

$$T^{d}_{i,j}(t) = F_{i,j}(t) / R_{i,j}(t) \qquad [2]$$

$F_{i,j}(t)$ represents the number of packets forwarded correctly by node j at time t, $R_{i,j}(t)$ signifies the number of packets successfully received by node j from node i at time t. We place all nodes in the promiscuous mode. When a node overhears a neighbor forwarding a packet, it should first check the forwarding behavior. Whenever it finds that its immediate neighbor nodes have received a packet to forward, it increments $R_{i,j}(t)$ by one. Whenever it finds that its immediate neighbor nodes have forwarded a packet it has to forward, it increases the $F_{i,j}(t)$ by one. After each interaction, node i can monitor its neighbor nodes' forwarding behavior by passive acknowledgment [4]. If so, the trust degree between them increases. Otherwise, the trust degree decreases.

Step 2: Node trust updation

With the help of passive acknowledgement the trust degree of every node will be updated only when the interaction rise in a selected interval of time among nodes. With the help of neighbor node trust degree, every node trust degree is updated. Every node updates its total trust degree using moving average model for the assurance of processing the trust updation and correctness of every node. After the trust update interval Δt,

$$T'_{i,j}(t + \Delta t) = \mu \times T_{i,j}(t) + (1 - \mu) \times T_{i,j}(t + \Delta t) \qquad [2]$$

$T'_{i,j}(t + \Delta t)$ denotes the trust degree updation at time $t + \Delta t$,$T_{i,j}(t + \Delta t)$ is the node j trust degree measured by node i at time $t + \Delta t$, $\mu(0 < \mu < 1)$ is a weighting factor used to balance current measurement and previous estimation. Each node collects the information of trust and record in trust record table. Every neighbor node that receives the packets for forwarding, conserve the trust degree value record by all nodes. Node ID, trust of the node, degree of the node direct trust, present time, time of final updating are recorded in the trust record table.

E. Schema Construction and Revocation

The feature set keys are revised and sent to the acceptable feature set of members with confidential. Later every component are encrypted by using confidential key in the ciphertext that are again encrypted through the random storing node with random and components of ciphertext that corresponds to the attributes are encrypted again along with updated feature set keys. To revoke specific attribute keys of a user while not rekeying the entire set of key set of a user is sure with constant random price so as to forestall with few attacks. So cancelling an attribute inside the system needs all users to update all their key parts notwithstanding the opposite attributes of them area unit still valid. This appears terribly inefficient particularly in large-scaled DTNs.

F. Topology Construction

This stage involves crucial wherever to position the parts and the way to attach them. The improvement strategies which will be utilized in this stage return from a part of arithmetic known as Graph Theory. These strategies involve crucial the prices of transmission and therefore the cost of switch.

INPUT VALUE: Transmission Range, Network Size, propagation, bandwidth, no of node, routing protocol, channel usage. Loss monitor tool usage in the agent through that we calculate the no of packet received, data loss and throughput.

G. Simulation Results

TCP provides reliable, ordered delivery of a stream of bytes from a source to destination with constant bit rate of data packets.

IV. PERFORMANCE METRICS

- PACKET DELIVERY RATIO

The fraction of the data packets delivered to destination nodes to those sent by source nodes.

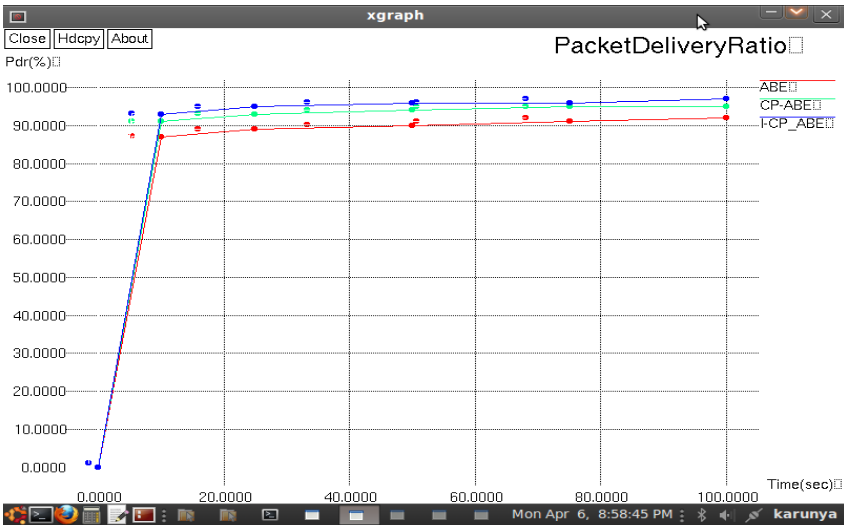

Fig.1. Packet Delivery Ratio

Packet delivery ratio of improved CP-ABE is more or less equal to CP-ABE but higher than ABE. In an improved CP-ABE the data packets are delivered per second to neighbour node is more when compare to other algorithm.

- END-TO-END DELAY

The average time taken by the data packets from sources to destinations, including buffer delays during a route discovery, queuing delays at interface queues, retransmission delays at MAC layer and propagation time is known as end-to-end delay.

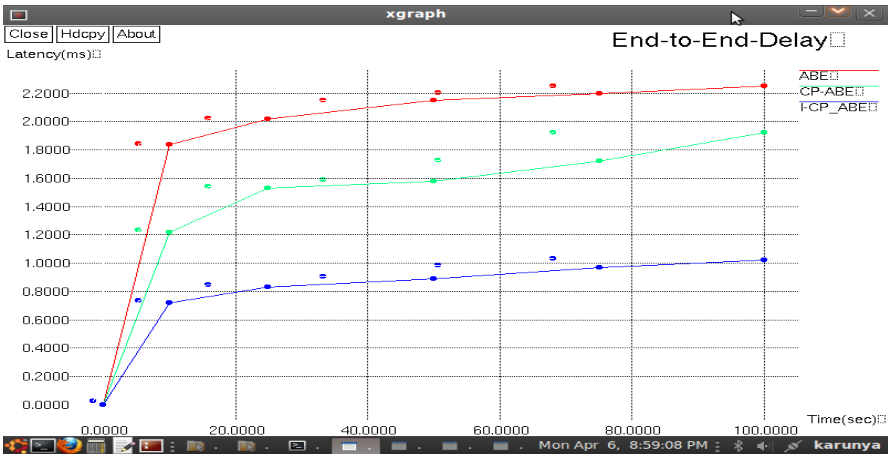

Fig.2. End-to-End Delay

Improved CP-ABE end-to-end delay is less than the CP-ABE end-to-end delay which is again less than the ABE. The data loss is less when compared to other algorithm while packets are sending to neighbour nodes in improved CP-ABE. The data loss is reduced with the help of estimation of trusting the node.

- DATA PACKET FORWARDING

Data packet forwarding is that the variety of helpful bits per unit of your time forwarded by the network from a particular supply to a specific target, no inclusion of overhead on protocol. Forwarding packet of data is that the quantity of digital knowledge per unit of time that's delivered over a physical or logical link that are send through a precise network node.

Data Packet Forwarding = (total_packets_received) / (simulation_time)

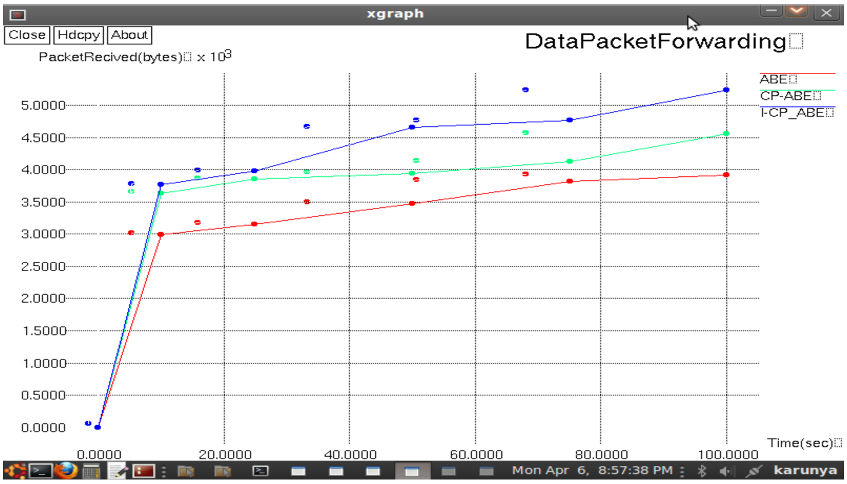

Fig.3. Data Packet Forwarding

Improved CP-ABE has the highest data packet forward than CP-ABE and ABE. Per second how much data packets are received and forwarded to neighbouring nodes are high in improved CP-ABE when compared to others. TQR makes the data packets forward at high speed.

- CONTROL OVERHEAD

The ratio of the number of control packets, including route request/reply/update/error packets to the number of data packets are known as control overhead. The control overhead is very less in improved CP-ABE when we use the node trust estimation and update of the trust when data is forwarded to other nodes. The other algorithm have high overhead without the node trust.

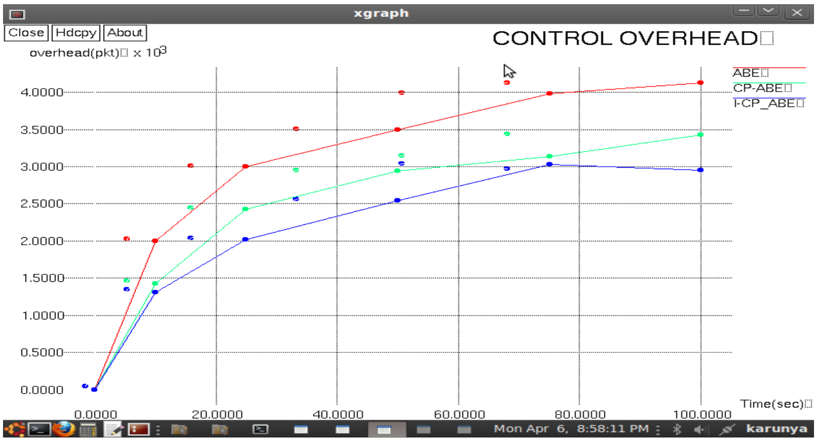

Fig.4. Control Overhead

ABE have high overhead in control. CP-ABE is less than the ABE. Improved CP-ABE is slightly less control overhead when compare to CP-ABE.

V. Conclusion and Future Work

CP-ABE with the help of two party computation protocol, prevents the authorities that creates secret key for each user independently from guessing secret key of the user issued by different authorities. To protect the confidentiality of the data 2PC protocol is used. In this paper we discussed improved ciphertext policy attribute based encryption for retrieving data securely with more trust in authorities. Trust of the node can be determined by estimating the trust of every node. The trust can be estimated by forwarding the data out of which are received successfully. Each time when the node forwards data, trust value gets updated for each node. The difference between CP-ABE and improved CP-ABE is trust of each node and authorities. The feature in improved CP-ABE is to improve the trust of the each node along with CP-ABE. Thus the trust of each node is estimated and updates the node's trust after sending data from a node to its neighboring nodes. Therefore the user can trust the key authorities more when compared to CP-ABE for retrieving the data more securely and confidential about data when it is stored in storage node.

References

1. Hur, J., and Kang, K.,"Secure data retrieval for decentralized disruption-tolerant military networks", IEEE/ACM Transactions on Networking, Vol.22, No.1, 2014.
2. Bo Wang, Xunxun Chen, and Weiling Chang, "A light-weight trust-based QoS routing algorithm for ad hoc networks", ELSEVIER, Pervasive and Mobile Computing, 2013.
3. Lewko, A., and Waters, B., "Decentralizing attribute-based encryption", Cryptology ePrint Archive: Rep. 2010/351, 2010.
4. Pirzada, A.A., McDonald, C., Datta, A.,"Performance comparison of trust-based reactive routing protocols", IEEE Transactions on Mobile Computing 5 (6), 695–710, 2006.
5. Goyal, V., Pandey, O., Sahai, A., and Waters, B., "Attribute-based encryption for fine-grained access control of encrypted data", ACM Conf. Comput. Commun. Security, pp. 89–98, 2006.
6. Bethencourt, J., Sahai, A., and Waters, B., "Ciphertext-policy attribute based encryption", IEEE Symp. Security Privacy, pp.321–334, 2007.