# Improving Security Using Text Based Encryption For Military Networks

***Deepa.V***
***Faculty of Department of CSE***
***Velammal Engineering College***
***Anna University Chennai,India***
***Email:deeptrinu@gmail.com***

***Mariyaselvi.J***
***Student of Department of CSE***
***Velammal Engineering college***
***Anna University Chennai,India***
***Email:jmariyaselvi@gmail.com***

***ABSTRACT***
***Tolerant network technology become a successful solution provided.soldiers carried wireless devices are walky talkie etc. they communicate each other and access confidential informnatio.To develop security mechanism provide text based encryption method is used .In this paper data access scheme which is based on text based approach.that is only accessed by authorized users.In this paper will remove the the attacks.sender can only encrypted the test and also destination users only decrypted the message.***
***INDEXTERMS:TextBasedEncryption(TBE),Tolerant Network,Data retrieval***

## 1.INTRODUCTION

In the distruption tolerant networks that allow communicate with each other with any networking environment.[1].end to end communication between the source and destination.the intermediate node concept.first sending message to the sender and through the intermeaiate node then message reach destination. For example,if a user joins or leaves an attribute group, the associated.Attribute key should be changed and redistributed to all the othermembers in the same group for backward or forward secrecy. Several DTN routing schemes [2,3] have been proposed.

In Text Based Approach the key authority generates private keys of users by applying the authority's master secret keys to users secret key associated by the separate users. There are two main problems: one concern of security of the encryption,the other the privacy of the users. Our design consists of three main components, (a) data caching, (b) query dissemination, and (c) message routing. In [8], the authors study the optimal number of replicas for a set of objects in large two-dimensional wireless mesh networks such that the access cost can be minimized.In [3], The authors propose three distributed caching techniques for wellconnected adhoc networks, namely CacheData, CachePath and HybridCache. For example, in a battlefield, soldiers need to access information related to detailed geographical maps, intelligentinformation about enemy locations, new commands from the general, weather information etc. This allows us to save battery power, bandwidth consumption and the data item retrieval time. Several current solutions [4] follow the traditional cryptographic-based approach where the contents are encrypted before being stored in storage nodes, and the decryption keys are distributed only to authorized users. Contents are encrypted under an access policy such that only those users whose attributes match the access policy are able to decrypt. Note that Lin *et al.* [5] recently proposed a different approachfor building a multi-authority TBE scheme withouta central authority. This is due to the fact that the different authorities generate their own attribute keys using their own independent and individual master secret keys. A key generation mechanism based on the singlemaster secret is the basicmethod for most of the asymmetric encryption systems such as the attribute-based or identity-based encryption protocols.

Key policy using the text based encryption.Each user embedded in user key.First problem in this project degradation of security that means the forward and backward secrecy[8].The users scenario that soldiers may change their attributes frequemtly. Our system supports both push and pull mechanisms that work in disruption tolerant network environment .There are two caching steps.one is cache data and another one is cache hybrid. Cache Data which stores and send to the data through database,cache hybrid which is send the data to cache and send to the path. The user can interact with each authority under a different pseudonym in such a way that it is impossible to link multiple pseudonyms belonging to the same user.consider fixed tree model means total privacy cost.dynamaic tree

model is minimized with respect to communication

**1.1 RELATED WORK**

**2. LITERATURE SURVEY**

The important idea of literature review is, it convey others contribution on our research area. It gave idea for new researches and related works are accomplished by others. Literature survey demonstrates our understanding of the relevant proposal of others and our ability for summarizing information gained from others works. There are two key steps should follow in literature survey. They are finding sources and synthesizing information. These steps are accomplished in my literature review about reduce attacks using no central authority.The literature review provides TextBasedEncryption the user can interact with each authority under a different pseudonym in such a way that it is impossible to link multiple pseudonyms belonging to the same user.In this project using anonymous secret key used.

**2.1 TBE(TEXT BASED ENCRYPTION)**

Generates header message contains the encrypted group messages and group members using keys.Each header message associated attribute group.The attribute group members include joining backward secrecy and also leaving the forward secrecy.attribute group members not affected by the membership changes.

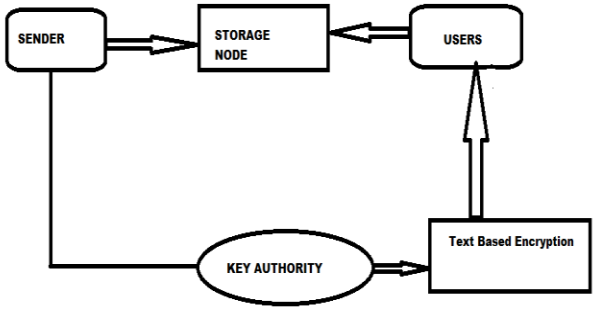


**Fig: II. 1 Text Based Encryption**

Key authorities consists of generation of key center.and also use central authority and multiple local authority.system assigned tasks and execute the system.this method use only encrypted contents.Text Based Encryption produced Text.senders can stores the information and corresponding users access to them.users is nothing but the node access information from storage node.

**3. ALGORITHMS AND IMPLEMENTATION MODELS**

cost.information retrieval system increase the efficiency.

**3.1 SYNCHRONIZATION OF KEYS**

Senders can sending messages to the destination.Each and every message can be encrypted to the separate keys at the same key can be decrypted to that message.In the data Decryption process can be decrypted the message using the keys and also using recursion method.header contains attribute group of messages.In this way using the anonymous key protocol.M-2 collusion appear.Yk denoted by k outside of attribute group.

**3.2ADVANCEDENCRYPTION STANDARD(AES)**

It is a symmetric key algorithm .Sender can send the message to the destination that key can be encrypting with 64 bits in my paper.each and every message is very secure in due to the AES algorithm because us government also top secret information are using 192 and 256 key length used.In my project Text Based Encryption provides Text that text can be encrypted using secret keys that prevent attacks .TBE can send the request will pass amoung the nodes.AES is more secure than DES because that AES send maximum amount of data transfer with single encryption key with 32 GB.

**3.3 SECURE MESSAGE PASSING**

Location client message passing to the nodes.The nodes will be divided in to 3 different paths.Each and every nodes can broadcast beacon.the beacon using particular interval and distance nodes is called.Dataitem generate by particular item.when a node receives a beacon.nodes advertised by the data items matched by storage queries.items can be retrieved by the available storage space.

**3.4 PROTOCOL DESIGNING AND ATTACKS DETECTION**

In my exixting system using DSDV that means distance sequence destination vectorIn this protocol using table driven scheme in mobile adhoc network.Each and every source and destination using routing table that contains routing table information and sequence number.In this protocol that have loss of information is more.There are attacks appear in our project.

Each node broadcasts the beacon periodically.when the node receives a message that needs to be forwarded.each node has a separate value .the value can be exceed to the threshold value then go to the nexthop of the path.when a node receives the beacon that node can be matched to the

data items.then will generate the query response to that node.

In my proposed system using AASR that means anonymous authenticated security routing.In this protocol is onion routing that means appear in onion layers.In this technique use anonymous communication.originator select set of nodes that chosen make a path which is contain chain or circuit.originator can send the message from first node to second node.second node only decrypt not use the first node.same message can send second node to third node.third node only decrypt it.

### 3.5 DESIGNING SYSTEM

Each encryptor can have the key values hi,hk.every keyvalues can have corresponding threshold values.the value of threshold adjusting dummy variables Ji,Jk.this is flexible to threshold policy in cipher text.different users using different threshold values Fk.

access structure can also message and key also encrypt and decrypt them.using randomized algorithm input message M and access structure D and produce ciphertext.

## 4.RESULTS AND DISCUSSION

In my project using TBE(Text Based Encryption**).**80 percentage of data loss could be reduced.

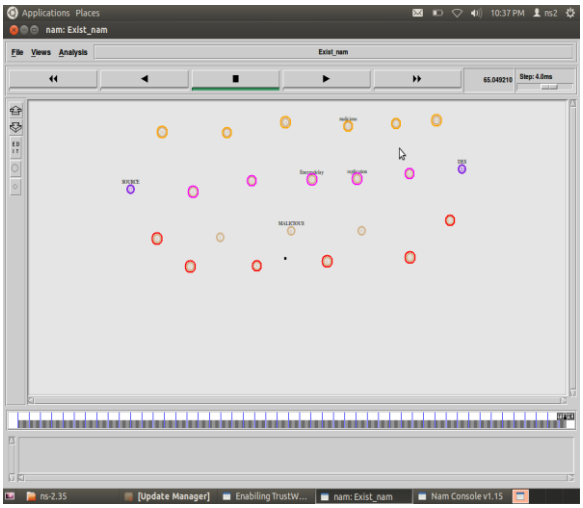


**Fig:V)ATTACKS APPEAR IN MILITARY APPLICATION**

## 5. CONCLUSION

In this project we explored Text Based Encryption(TBE). Main focus of this project is implementing preventing attacks that is sending message can be encrypted by the particular key concept. For this we use text produced and evaluated using a designed to models in different scenarios.This project also explains how to achieve the confidential information from text based encryption method .To prevent the loss of information.

## 6.REFERENCES

[1] J. Burgess, B. Gallagher, D. Jensen, and B. N. Levine, “Maxprop: Routing for vehicle-based disruption tolerant networks,” in *Proc. IEEE INFOCOM*, 2006, pp. 1–11.

[2] M. M. B. Tariq, M. Ammar, and E. Zequra, “Mesage ferry route design for sparse ad hoc networks with mobile nodes,” in *Proc. ACM MobiHoc*, 2006, pp. 37–48.

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

[4] S. Jin, L. Wang, “Content and Service Replication Strategies in Multihop Wireless Mesh Networks”, Proceedings of MSWiM, Oct, 2005.

[5] L. Yin, G. Cao, “Supporting Cooperative Caching in Adhoc Networks”, Proceedings of IEEE Infocom, 2004. T. Spyropoulos et al, “Efficient routing in intermittently connected mobile networks: single copy case” to appear in IEEE/ACM Transactions on Networking, 2007

.