Volume-4, Issue-5, May Special Issue-2015 • ISSN No 2277 - 8160

Research Paper | Engineering

Self-assured Data Repossession for Disruption Tolerant Military Networks

Suseela.S Computer Science and Engineering, Annamacharya Institute of Technology and Sciences, Tirupati, A.P, India.

Purushotham.B Computer Science and Engineering, Annamacharya Institute of Technology and Sciences, Tirupati, A.P, India.

ABSTRACT

A disruption tolerant military network(DTN) is a network that can overcome the intermittent failures in the data transmission of a private or public network. In wireless ad hoc networks there is no predefined architecture for the cells/stations to create path when data transmission required. So, they will cause interferences. In this paper, we are proposing an access technique that can surpass the intermittent failures caused in the secure networks like military, rescue operations etc. The proposed algorithm improves the Advanced Encryption Standard (AES) algorithm. The improvement will result in the protection of collusion between users of secure networks. It will also solve the key escrow problem and provides forward and backward secrecy. We also give an additional privilege for the relocated users that are part of the network and trying to create a private network for security reasons.

KEYWORDS : DTN, Access Control, AES

I. INTRODUCTION:

Mobile cells or stations in wireless ad hoc networkslike military especially in country borders or war areas suffer with regular breakage while transmitting the data. This is because collusion among authenticated users may happen or a dishonest centralized commander may leak the information. So, the administration department has to break the data transmission for even trusted stations. It will cause disruptions in the transmission. It consumes lot of cost to avoid them because security in those hostile regions is very important. This paper proposes a method to solve that problem in a cost effective manner.

II. LITERATURE SURVEY:

For the past few decades only text based passwords and graphical passwords are used. It is quite convincible by psychology studies that human brain easily remembers and recognizes images than text. That feature is applied in the latest trends. But in military like environments we cannot trust individual participant also. So, we have to provide an encryption mechanism that depends on users' attributes rather than their personal information. The AES does the same based on attribute based encryption.

III. DESCRIPTION OF THE PROPOSED SYSTEM:

In this section, we will discuss the implementation model for the proposed system.



Fig.1:Architecture for self-assured repossession of data in DTNs

A. System Description

The above figure shows the architecture for a DTN. As shown in that, the proposed system consists of the following entities.

1) Key Authorities: These are both local authorities and central authority. Each region has one central authority and two or more local authorities for the local sub regions. For example battalion 1 has a central authority of region 1 which can have local authorities of region 1.1, region 1.2 etc. In order encrypt the data that is to be transmitted these key authorities must send their attribute encryption keys to the sender node which has responsibility discussed below.

2) Sender node: This entity plays a key role in the whole secure self-assured repossession as it maintains the whole system. We will consider this entity also semi trusted as it may also collude with other hostile communities. So, it has to provide one key which will combine with the keys sent by local authorities. All keys together forms encryption mechanism in AES algorithm. Here, we can guarantee that sender node cannot decrypt the data because only the data belong to a particular region can only be decrypted by that local user or station only.

3) Storage node: In order to securely transmit the data to different regions without connecting to a public network we have to provide a storage node. Here we will provide forward and backward secrecy protection by giving privileges to the storage node the capability of reencrypting the data. For security purpose i.e., storage node should not decrypt the data which may result in undesirable result we will prevent storage node from decryption. This will be done because storage node will not contain any keys from both central authority and local authority. So, we will give permission to it only for re-encryption but not decryption.

4) User: This entity plays a key role because it only has to successfully repossess the data without any disruptions. If the attributes of the user match with the decryption keys of the data then it will easily decrypted and receive the data for usage. If even one of the attribute is failed to match then that user who tried to hack will blocked. Again administration has to unblock that person.

B. Proposed Model & Security Requirements

1) Data Confidentiality: Unauthorized persons who do not have enough attributes will completely block from the network after mismatching from the decryption key. And they can only be given again privileges for accessing the data by central administration. If ever a user provides sufficient and absolute attribute information he can easily decrypt the data and access it.

2) Collusion-resistance: Collusion is the process ofillegal compromises between authorized persons who have legal attribute information to decrypt the dat. As we are providing the AES algorithm with a combination of central authority and local authorities there is least chance of breaking encryption. The reasons for that can be analyzed by the following cases. I n first case, we may consider collusion between two local

authorities – it doesn't work because it don't have central authority key. In second case, we consider central authority collusion with other enemy party – it also doesn't work because it doesn't have local authority key. In third case, we may consider collusion between central authority and one local authority – it also obviously doesn't work because storage node re-encrypts the data after user relocated to a new region or battalion.

3) Backward and forward Secrecy: If a user moved to a new location then he should not be able to decrypt the previous location data. This can be done by restricting him to enter the keys of relocated data. This is called as backward secrecy. If a user moves to new battalion, then he must be able to decrypt the data related to that region without any disruptions. For this to happen we have to continuously update the keys to the users who are authenticated properly through storage node.

IV.RESULTS:

The simulation studies involve the Disruption Tolerant Military Network and the repossession of data at mobile nodes in those networks. The proposed method we perform AES algorithm 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.

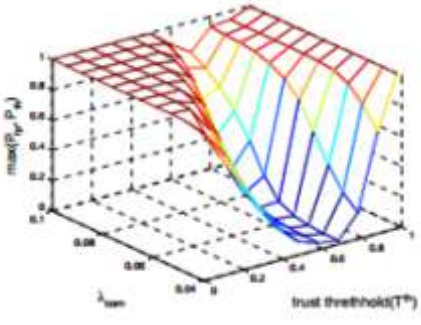


Fig.2:Analysing the trust threshold

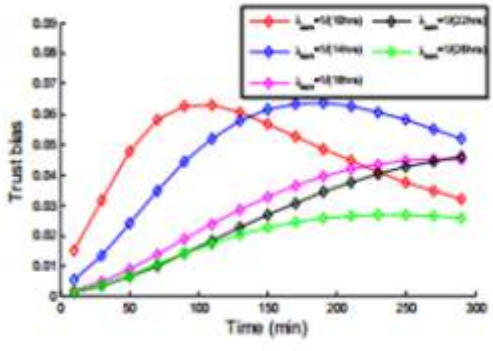


Fig.3. Calculating Trust Values

V. CONCLUSION:

Our paper may not be the unique one but we had put sincere efforts to propose a maximum implementable methodology for self-assured data repossession in DTNs that regularly suffer with intermittent failures. In this paper, we showed the improvement of AES algorithm along with its performance results. In improved AES we have proposed highly secured access policy mechanisms for encryption and decryption of dat. Our future work go along to create a highly protect private network so that in typical network areas like military and rescue operations we can provide maximum security for both intermittent failures and collusions among authorized persons also.

REFERENCES

[1] D. Huang and M.Varma, "ASPE: Attribute Based Secure Policy Enforcement In Vehicular Ad Hoc Networks," Ad Hoc Netw., Vol.7, no. 8, pp. 1526-1535, 2009.|| [2] S. Yu, C. Wang, K. Ren and W. Lou, "Attribute Based Data Sharing With Attribute Revocation," inProc. ASIACCS, 2010, pp. 261-270.|| [3] 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.|| [4] R. Ostrovsky, A. Sahai and B.Waters, "Attribute Based Encryption With Nonmonotonic Access Structures," in Proc. ACM Conf. Comput. Commun. Security, 2007, pp. 195-203.|| [5] J.Bethen Court, A. Sahai and B.Waters, "Cyphertext Policy Attribute Based Encryption", in Proc. IEEE symp. Security Privacy, 2007, pp. 321-334.|| [6] A. Lewko and B.Waters, "Decentralizing Attribute Based Encryption," Cryptology print Archive: Rep. 2010/351, 2010.|| [7] A. Sahai and B. Waters, "Fuzzy Identity Based Encryption", in Proc. Eurocrypt,2005, pp. 457-473.|| [8] J. Burgess, B. Gallagher, D. Jensen and B.Nlevine, "Max Prop: Routing For Vehicle Based Disruption Tolerant Networks," in Proc. IEEE INFOCOM, 2006, pp. 1-11.|| [9] M.M.B. Tarq, M. Ammar and E. Zerqura, "Message Ferry Route Design For Sparse Ad Hoc Networks With Mobile Nodes," in Proc. ACM Mobihocs., 2006, pp. 37-48.|| [10] L. Ibraimi, M. Petkovic, S. Nikova, P. Harpel and W. Jonker, "Mediated Ciphertext Policy Attribute Based Encryption And Its Application," in Proc. WISA, 2009, LNCS 5932, pp. 303-323.|| [11] M. Chuah and P. Yang, "Node Density Based Adaptive Routing Scheme For Disruption Tolerant Networks," in Proc. IEEE MILCOM, 2006, pp. 1-6.|| [12] M. Chuah and P. Yang, "Performance Evaluation Of Content Based Information Retrieval Scheme For DTNs," in Proc. IEEE MILCOM, 2007, pp. 1-7.|| [13] 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.|| [14] S. Roy and M. Chuah, "Secure Data Retrieval Based On Ciphertext Policy Attribute Based Encryption [CP-ABE] System For The DTNs," Lehigh CSE Tech. Rep, 2009.|| [15] N. Chen, M. Gerla, D. Huang and X. Hong, "Secure, Selective Route Broadcast In Vehicular Networks Using Dynamic Attribute Based Encryption," in Proc. Ad Hoc Netw. Workshop, 2010, pp. 1-8.