IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

Achieving Trust and Survivability for Mission Effectiveness in Tactical Network using CP-ABE

P. Rajapandian[1], C. Maleappane Lawrence[2], G. Siva Kumar [3]

Assistant Professor [Sr. Gr.] & Head, Dept of M.C.A., Christ College of Engg and Technology, Pondicherry, India[1]

Assistant Professor, Department of M.C.A., Christ College of Engineering and Technology, Pondicherry, India[2]

Final Year Student, Department of M.C.A., Christ College of Engineering and Technology, Pondicherry, India[3]

Abstract: In a military tactical network, maintaining trust among members in a mission group is critical to successful mission completion. However, maintaining high trust among group members in a resource-restricted tactical environment is difficult, which may lead to mission failure or low mission effectiveness. In this paper, we propose a secure data retrieval scheme using CP-ABE. Cipher text-policy attribute-based encryption (CP-ABE) is a promising cryptographic solution to the access control issues for tactical network, where multiple key authorities manage their attributes independently. We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the military tactical network.

Keywords: Group trust, tactical network, mission effectiveness, and key authorities.

I. INTRODUCTION

In military tactical network a user should only be able to access data if a user possesses a certain set of credentials or attributes. Currently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control. However, if any server storing the data is compromised, then the confidentiality of the data will be compromised. The concept of Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is a promising approach that fulfils the requirements for secure data retrieval in military tactical network. CP-ABE features a mechanism that enables an access control over encrypted data using access policies and attributes among private keys and cipher texts.

Especially, cipher text-policy ABE (CP-ABE) provides a scalable way of encrypting data such that the encryption defines the attribute set that the descriptor needs to possess in order to decrypt the cipher text. Thus, different users are allowed to decrypt different pieces of data per the security policy. So applying the CP-ABE to military tactical network introduces several security and privacy challenges to make systems secure.

II. RELATED WORK

Traditional networks are built on the assumption that network entities cooperate based on a mandatory network communication semantic to achieve desirable qualities such as efficiency and scalability. Over the years, this assumption has been eroded by the emergence of users that alter network behavior in a way to benefit themselves at the expense of others. At one extreme, a malicious user/node may eavesdrop on sensitive data or deliberately inject packets into the network to disrupt network operations. The solution to this generally lies in encryption and authentication. In contrast, a rational node acts only to achieve an outcome that he desires most. In such a case, cooperation is still achievable if the outcome is to the best interest of the node. The node misbehavior problem would be more pronounced in multihop wireless networks like mobile ad hoc and sensor networks, which are typically made up of wireless battery-powered devices that must cooperate to forward packets for one another. However, cooperation may be hard to maintain as it consumes scarce resources such as bandwidth, computational power, and battery power. So a game theory to achieve collusive networks behavior in such network environments. Our model builds on recent work in the field of Economics on the theory of imperfect private monitoring for the dynamic Bertrand oligopoly, and adapts it to the wireless multihop network. The model derives conditions for collusive packet forwarding, truthful routing broadcasts, and packet acknowledgments under a lossy wireless multihop environment, thus capturing many important characteristics of the network layer and link layer in one integrated analysis that has not been achieved previously.

Service science aims to explain and improve interaction in which multiple entities work together to achieve win-win outcomes or mutual benefits. In the context of service, service system entities are dynamic configuration of resources, and the four primary types of resources are people, organizations, shared information, and technology. As we can see, people as a part of service systems entities have important role to make the others entities work together to create a value. Thus, how people can work together is also interesting issue in area of service science. In recent years, there has been substantial progress on how people can work together. Game theory has formalized the issue as cooperation problem and represents it as a mixed-motive two-person game. The cognitive demands of forward-looking rationality have led game theorists to

explore models of cognition that explicitly describe the dynamics of stepwise decision making. As a result, learning-theoretic models of cooperative behavior are needed. The idea of modeling people as stimulus-response mechanism shaped by learning forces has a long history in psychology. The model uses aspiration as cognitive which stimuli people's action. In a group, people might have different aspiration toward their relationship and might learn with different way of learning to achieve a goal. How people with different aspiration can learn to work together is not a trivial work. A model of sharing aspiration among people in a group to increase cooperative behavior of the people.

Military communities in tactical networks must often maintain high group solidarity based on the trustworthiness of participating individual entities where collaboration is critical to performing team-oriented missions. Group trust is regarded as more important than trust of an individual entity since consensus among or compliance of participating entities with given protocols may significantly affect successful mission completion. This work introduces a game theoretic approach, namely Aoyagi's game theory based on positive collusion of players. This approach improves group trust by encouraging nodes to meet unanimous compliance with a given group protocol. However, when any group member does not follow the given group protocol, they are penalized by being evicted from the system, resulting in a shorter system lifetime due to lack of available members for mission execution. The results show that there exists the optimal trust threshold that can maximize group trust level while meeting required system lifetime (survivability).

Existing authorization mechanisms fail to provide powerful and robust tools for handling security at the scale necessary for today's Internet. These mechanisms are coming under increasing strain from the development and deployment of systems that increase the programmability of the Internet. Moreover, this "increased flexibility through programmability" trend seems to be accelerating with the advent of proposals such as Active Networking and Mobile Agents. The trust-management approach to distributed-system security was developed as an answer to the inadequacy of traditional authorization mechanisms. Trust-management engines avoid the need to resolve "identities" in an authorization decision. Instead, they express privileges and restrictions in a programming language. This allows for increased flexibility as well as standardization of modern, scalable security mechanisms. Further advantages of the trust-management approach include proofs that requested transactions comply with local policies and system architectures that encourage developers and administrators to consider an application's security policy carefully and specify it explicitly.

Ciphertext-Policy Attribute Based Encryption (CP-ABE) is a promising cryptographic primitive for fine-grained access control of shared data. In CP-ABE, each user is associated with a set of attributes and data are encrypted with access structures on attributes. A user is able to decrypt a ciphertext if and only if his attributes satisfy the ciphertext access structure. Beside this basic property, practical applications usually have other requirements. In particular, we resolve this challenging issue by considering more practical scenarios in which semi-trustable on-line proxy servers are available. As compared to existing schemes, our proposed solution enables the authority to revoke user attributes with minimal effort.

III.EXISTING SYSTEM

A game theoretic approach using the so called Aoyagi's game theory, a military environment also requires each entity to follow a given protocol or be penalized if any entity breaks the given rule. Due to the common characteristic, Aoyagi's game theoretic framework can provide an insightful solution to maximize group trust among group members. A Symmetric key approach ABE schemes are constructed on the architecture where a single trusted authority has the power to generate the whole private keys of users with its master secret information. Thus, the key escrow problem is inherent such that the key authority can decrypt every cipher text addressed to users in the system by generating their secret keys at any time. Military network can transfer the information to each zone and anyone can decrypt data. The military is distributing the data without secure authority in networks.

A. Data Transfer
- User sends the confidential data to the particular zone.
- The members in the zone can access the confidential data.

B. Data Retrieval
- Anyone from the zone can access the confidential data. Then the information is conveyed to other members in the zone.

C. Disadvantages:
- The information conveyed by the person in the zone is considered as the trusted information.
- Admin does not have the option to identify which person has accessed the confidential information.

IV.PROPOSED SYSTEM

A Ciphertext-Policy Attribute Based Encryption (CP-ABE) scheme is a multiauthority network environment to secure the data by encryption and decryption, and using key authority to generate the key for secure data retrieval of military tactical network. Each attribute key of a user can be updated individually and immediately. Thus, the scalability and security can be enhanced in the proposed scheme. The role of the parties is taken by the attributes. Different users are allowed to decrypt their data as per the security policy. Thus, the access structure will contain the authorized sets of attributes. Admin can send data to the individual user or multiple users and vice versa. That information will be viewed by the admin in admin storage node. The transferred information acknowledgement will be sent to the admin and viewed by the admin. The Data

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

transfer information will be sent to the admin. Admin monitor the user profiles based on the authorities. Based on the information transferred admin differentiate the trusted and most trusted user, finally the network performance is analysed by the graph.

A. System Architecture

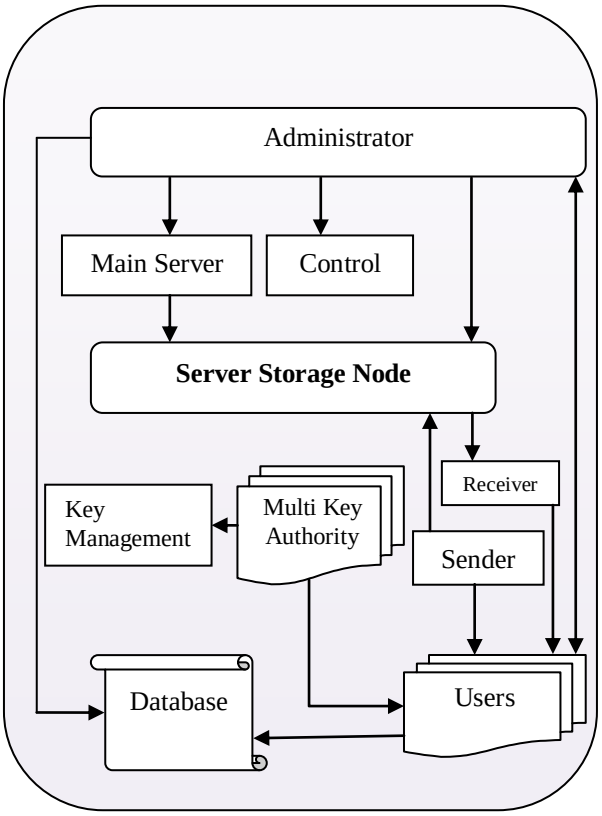

Fig. 1. System Architecture

The key authority generates private keys for users by applying the authority's master secret keys to users associated set of attributes. Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is used for Asymmetric key generation process. Each and every will be providing with a unique. The user will send the information from one zone to another zone for a particular user or multiple users. The information will be in the encrypted format. Thus the user can decrypt every ciphertext addressed to them by using their attribute keys.

B. Module Explanation

1. Key Generation:
The User Interface Design plays an important role for the user to move login the Application. This module has created for the security purpose. In this login page we have to enter user name and password, it will check username and password, if valid means directly go to home page, invalid username or password means show the error message and redirect to registration page. So we are preventing from unauthorized user entering into the login page to user page. It will provide a good security.

New users can register their details and after the completion of registration a unique secret key will be generated for each and every user by the key authority. These key authorities are responsible for user key generation process.

2. Storage Node:
The user will upload some data's in the User Page. The system will calculate size of the file and sends through Storage node. Therefore storage node can get the data without traffic and also transmit the data in less time. The data confidentiality and privacy can be cryptographically enforced against any curious key authorities or data storage nodes in the proposed scheme. This is an entity that stores data from senders and provide corresponding access to users.

3. Store-carry and forward:
This is an entity who owns confidential messages or data 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. 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 cipher text and obtain the data.

4. Decentralized User:
We provide a multiauthority CP-ABE scheme for secure data retrieval in military tactical network. Each local authority issues partial personalized and attribute key components to a user by performing secure with the central authority. Each attribute key of a user can be updated individually and immediately. Thus, the scalability and security can be enhanced.

5. Decentralized User:
In this module we are going to develop the file sharing concept and user satisfied trust worthiness. Then how long user touch with network and one more thing what type of file sharing and when it is user file sharing with time and date is calculated. After that we are calculated how many user using in same network based on to the trust implemented in user satisfactions.

V. CONCLUSION AND FUTURE WORK

We proposed an efficient and secure data retrieval method using Ciphertext-Policy Attribute-Based Encryption (CP-ABE) for military networks where multiple key authorities manage their attributes independently. Key authority issues set of attribute keys for their managing attributes to an authenticated user. The inherent key escrow problem is resolved such that the confidentiality of the stored data is guaranteed. The data confidentiality and privacy can be achieved by cryptographically enforced against any curious key authorities or data storage nodes. The future can extends user validation for set of attribute in

authentication of multiauthority network environment. We can hide the attribute in access control policy of a user. Different users are allowed to decrypt different pieces of data per the security policy. We going to achieve the data confidentiality and privacy can be cryptographically enforced against any curious key authorities or data storage nodes.

REFERENCES

[1] M. Siallagan and H. Deguchi, "Learning with sharing aspiration to promote cooperative behavior in a group," in Proc. 7th Int. Conf. Service Syst. Service Manag., Tokyo, Japan, Jun. 2010, pp. 1–5.
[2] J. Cho and A. Swami, "On tradeoffs between trust and survivability using a game theoretic approach," in Trust Management V (IFIP Advances in Information and Communication Technology), vol. 358. Berlin, Germany: Springer, 2011, pp. 190–205.
[3] S. Ng and W. Seah, "Game-theoretic approach for improving cooperation in wireless multihop networks," IEEE Trans. Syst., Man, Cybern. B, Cybern., vol. 40, no. 3, pp. 559–574, Jun. 2010.
[4] H. Li and M. Singhal, "Trust management in distributed systems," Computers, vol. 40, no. 2, pp. 45–53, Feb. 2007.
[5] L. Thiele, K. Miettinen, P. Korhonen, and J. Molina, "A preference-based evolutionary algorithm for multi-objective optimization," Evol. Comput., vol. 17, no. 3, pp. 411–436, 2009.
[6] E. Diecidue and J. Ven, "Aspiration level, probability of success and failure, and expected utility," Int. Econ. Rev., vol. 49, no. 2, pp. 683–700, 2008.
[7] Shucheng Yu, "Attribute Based Data Sharing with Attribute Revocation, 2010.
[8] Q. Han, T. Arentze, H. Timmermans, D. Janssens, and G. Wets, "An agent-based system for simulating dynamic choice-sets," in Proc. Spring Simul. Multiconf., Ottawa, ON, Canada, Apr. 2008, pp. 26–33.

BIOGRAPHY

P. Rajapandian is an Assistant Professor [Sr. Gr.] & Head of Master of Computer Application in Christ College of Engineering and Technology affiliated to Pondicherry University, India.

C. Maleappane Lawrence is an Assistant Professor of Master of Computer Application in Christ College of Engineering and Technology affiliated to Pondicherry University, India.

G. Siva Kumar is a final year Student of Master of Computer Application in Christ College of Engineering and Technology affiliated to Pondicherry University, India.

DOI 10.17148/IJARCCE.2016.55146