Highly Secured Data Encryption in Decentralized Wireless Network

Amol G. Dhoke
Computer Science and Engineering
Rajiv Gandhi college of Engineering, Research and Technology.
Chandrapur,India
amol.dhoke@yahoo.in

Prof. P S. Kulkarni
Department Of Information Technology
Rajiv Gandhi college of Engineering, Research and Technology.
Chandrapur,India
kulkarnips1811@gmail.com

***Abstract*—** As the use of web side information for critical services has been increased, the significant amount of attacks against Network applications has grown as well. To protecting many Network applications, many of intrusion detection systems have been proposed. Several techniques which are meant for detection of Network application related attacks. The Attacking detection system provides the following: Monitoring and analyzing of user and system activity. Auditing of system an arrangement of parts and vulnerabilities, Evaluating the nature of the integrity of the files and critical system, Activity patterns of relating to the use of statistics analysis , Abnormal activity analysis, Operating system audit.

Keywords: *Side information, Attacking detection, operating system audit.*

*****

1. INTRODUCTION

Mobile nodes in military environments such as a battlefield or a hostile region are likely to suffer from intermittent network connectivity and frequent partitions. Disruption-tolerant network (DTN) technologies are becoming successful solutions that allow wireless devices carried by soldiers to communicate with each other and access the confidential information or command reliably by exploiting external storage nodes. Some of the most challenging issues are the enforcement of authorization policies and the policies update for secure data retrieval.Attribute-based encryption (ABE) is a promising cryptographic solution to the access control issues. However, the problem of applying ABE in decentralized DTNs introduces several security and privacy challenges with regard to the attribute revocation, key Management and coordination of attributes issued from different authorities, proposing a secure data retrieval scheme using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently.To apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network data sets in order to illustrate the advantages of using such an approach.

2. PROBLEM DEFINATION

- Military Network should require increased protection of confidential data including access control methods.
- In many cases, it is desirable to provide differentiated access services such that

Data access policies are defined over user attributes or roles, which are managed by the key Management System. It propose a D2C2 algorithm for visual pattern discovery by joint analysis of visual content and side information. A content collection is partitioned into subsets based on side information, and the unique and common visual patterns are discovered with multiple instance learning and clustering steps that analyzes across and within these subsets. Those patterns help to imagine the data content and generate vocabulary-based features for semantic classification. The proposed framework is rather general which can handle all types' offside information, and incorporate different common/unique pattern extraction algorithms. One future work is to improve the generation of common patterns by emphasizing the shared consistencies, instead of the current heuristic clustering.

3. LITERATURE REVIEW

Secured Data Retrieval for Decentralized Disruption-Tolerant Military Networks [1] Junbeom Hur , Kyung tae Kang, IEEE/ACM TRANSACTIONS ON NET, VOL.22, NO. 1, FEB14.

Mobile nodes in military environments such as a battlefield or a hostile region are likely to suffer from intermittent network connectivity and frequent partitions. Disruption-tolerant network (DTN) technologies are becoming successful solutions that allow wireless devices carried by soldiers to communicate with each other and access the confidential information or command reliably by exploiting external storage nodes. Enforcement of authorization policies and the policies update for secure data retrieval. Attribute-based encryption (ABE) is a promising cryptographic solution to the access control issues.However, the problem of applying ABE in decentralized DTNs introduces several security and privacy challenges with regard to the attribute revocation, key

management, and coordination of attributes issued from different authorities.

A dynamic Methodical procedure of introducing an activity pattern for WSN-based solutions Ramzi Bellazreg1, Noureddine Boudriga1, Khalifa Tunisia and 3Korea University ©2013 IEEE.

Wireless Sensor Networks (WSNs) are based on elementary sensors that detect the occurrence of particular events in a monitored area. The recent adverse WSN applications one can find the border surveillance applications. The Aim of this class of applications is to monitor a country border and detect the presence of intruders near the border line. , investigating theoretically the effects of natural factors on dynamic deployment scheme of a hierarchical WSN-based solution providing two lines of surveillance. Measurable factor such as the wind effect, the altitude and speed of the airjet from which the sensors are thrown are put into equation to optimize the area coverage and WSN connectivity. Then, proposing mathematical models that evaluate the quality of connectivity and coverage of the deployed network and allow planning and dimensioning of a border solution.

Blockade Coverage with Airdropped Wireless Sensors Anwar Saipulla Benyuan Liu Jie Wang Department of Computer Science University of Massachusetts Lowell Lowell, MA 01854 USA 2008 IEEE.

Barrier coverage of a wireless sensor network aims at detecting attacks crossing the network. It provides a feasible choice for monitoring boundaries of battlefields, country borders, Sea lines, and perameters of disapproving comments of infrastructures. Early studies on blockade coverage typically assume that sensors are deployed uniformly at random in a large area. This assumption are theoretically interesting, may be unfeasible in real applications. Taking a more feasible approach in this paper. In particular, consider that sensors are airdropped from an aircraft along its flying route. Wind, geographic terrain, and other factors may cause a sensor to land in a location deviating from its targeted landing point with a random offset. Thus, it is more feasible to assume that sensor nodes are distributed with a normal offset along the deployment line.

4. PROPOSED METHOD

1) Key Authorities: They are key generation centers that generate public/secret parameters for ABE. The key authorities consist of a central authority and multiple local authorities. Assume that there are secured and capable of relied communication channels between a central authority and each local authority during the initial key setup and generation phase.–

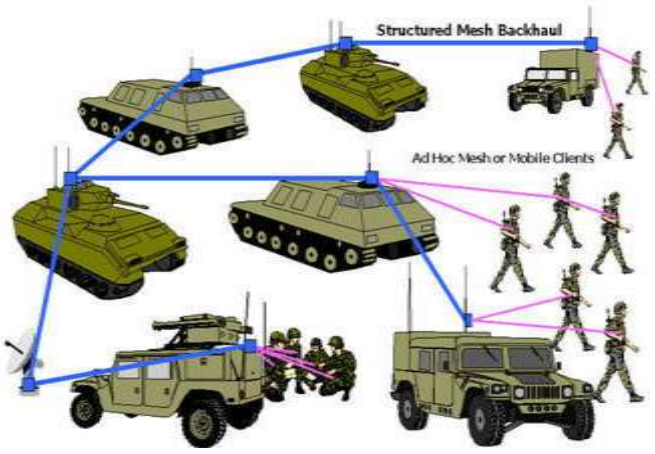

Fig:- Decentralized Military Network

Each local authority manages different attributes and issues corresponding attribute keys to users. They permit differential access rights to individual users based on the user attributes. The key authorities are assumed to be honest but curious. That is,Local authorities will honestly execute the assigned tasks in the system, however users would like to learn information of encrypted data possible.

2) Storage node: An entity that stores data from senders and provide corresponding access to users. It may be mobile or lacking in movement. Similar to the previous schemes, Assume the storage node to be semi trusted 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 abrogate in any of the attributes, then he will be able to decrypted the International Data Encryption Algorithm i.e IDEA Algorithm and obtain the data. Since the key authorities are half-trusted, they should be deterred from accessing plaint text of the data in the storage node; they should be still able to issue secret keys to users. In order to realize this somewhat in mutually consistent requirement, the enter authority and the local authorities engage in the arithmetic 2 PC protocol with master secret keys of their own and issue independent key components to users during the key issuing phase. 2 PC 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.

5. METHODLOGY

Attribute-based secure data retrieval scheme using ABE for decentralized DTNs. The present scheme features the following achievements. First, instant attribute abrogation enhances backward/forward secrecy of confidential data by reducing the windows of vulnerability. Second, encryptors can define a fine-texture access policy using any monotone access structure under attributes issued from any chosen set of authorities. Third, the key management problem is resolved by an escrow-free key issuing protocol that exploits the characteristic of the decentralized DTN architecture. The key permits protocol generates and gives user secret keys by performing a secure two-party computation (2PC) protocol among the key authorities with their own master secrets. The 2 PC protocol disuade the key authorities from obtaining any master secret information of each other such that none of them could generate the whole set of user keys alone.

Thus, users are not required to fully trust the authorities in order to protect their data to be shared. The data intent to be private and privacy can be cryptographically enforced against any curious key authorities or data storage nodes in the proposed scheme.

6. CONCULSION

Technologies are becoming successful solutions in military applications that allow wireless devices to communicate with each other and access the confidential information reliably by exploiting external storage nodes. It is a scalable cryptographic solution to the access control and secure data retrieval issues. An efficient and secured data obtaining method using this method for decentralized DTNs where multiple key authorities manage their attributes independently. The inherent key bond or deed 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.

ACKNOWLEDGMENT

This work was supported by Prop S. Kulkarni, Head, Department of Information Technology**,** R.C.E.R.T, Chandrapur. Prof.Rahila Sheikh, Assistant Professor, Computer Technology, R.C.E.R.T., Chandpur and Prof. R K.Krishna, Assistant Professor, Department of Electronics, R.C.E.R.T. for their encouragement to accomplish my work on time and also Prof. Nitin J. Janwe, Head, Department of Computer Technology, R.C.E.R.T., Chandrapur and honorable Dr. K. R. Dixit, Principal, R.C.E.R.T., Chandrapur, for being a constant source of inspiration. The authors would like to thank the anonymous reviewers for their valuable and constructive comments on improving the paper.

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. 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 andM. Chuah, "Secure data retrieval based on ciphertext 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 ciphertext-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 n vehicular ad hoc networks," Ad Hoc Netw., vol. 7, no. 8,pp. 1526–1535, 2009.

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

[11] 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, "Ciphertext-policy attributebased 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.