RESEARCH ARTICLE OPEN ACCESS

Attacks Identification Detections Based on Disruption Tolerant Networks

[1] A.Senthil Kumar, [2] R.Sathya

[1]Asst.professor, Dept.of.Computer science, Tamil University, Thanjavur-613010.

[2]Research Scholar, Dept.of.Computer Science, Tamil University, Thanjavur-613010.

----------**********----------

Abstract:

Malicious and selfish behaviors represent a serious threat against routing in disruption tolerant networks. Due to the unique network characteristics, designing a misbehavior detection scheme in DTN is regarded as a great challenge. In this paper, we propose iTrust, a probabilistic misbehavior detection scheme, for secure DTN routing toward efficient trust establishment. Selfish node B receives the packets from node A but launches the black hole attack by refusing to forward the packets to the next hop receiver C. Since there may be no neighboring nodes at the moment that B meets C, the misbehavior cannot be detected due to lack of witness, which renders the monitoring-based misbehavior detection less. This research Proposal Further includes The concepts of contact schedules, contact capacity and Link metrics. In addition the proposed aigorithm C T P A B En facilitates encrcyption functionality based on the user needs.The number of users in the DTN is limited and can be scalable in the future.

Keywords— ***layers ,security,attacks***

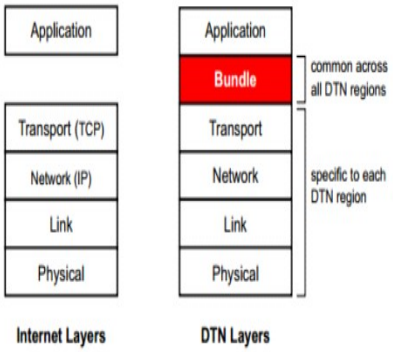
----------**********----------

I. INTRODUCTION

DELAY tolerant networks (DTNs), such as sensor networks with scheduled intermittent connectivity, vehicular DTNs that disseminate location-dependent information local ads, traffic reports, parking information, and pocket-switched networks that allow humans to communicate without network infrastructure, are highly partitioned networks that may suffer from frequent disconnectivity. In DTNs, the in-transit messages, also named bundles, can be sent over an existing link and buffered at the next hop until the next link in the path appears a new node moves into the range or an existing one wakes up. This message propagation process is usually referred to as the "store-carry-and-forward" strategy, and the routing is decided in an "opportunistic" fashion. In DTNs, a node could misbehave by dropping packets intentionally even when it has the capability to forward the data sufficient buffers and meeting opportunities.

Even though the existing misbehavior detection schemes work well for the traditional wireless networks, the unique network characteristics including lack of contemporaneous path, high variation in network conditions, difficult to predict mobility patterns, and long feedback delay have made the neighborhood monitoring based misbehavior detection scheme unsuitable for DTNs. Selfish node B receives the packets from node A but launches the black hole attack by refusing to forward the packets to the next hop receiver C. Since there may be no neighboring nodes at the moment that B meets C, the misbehavior cannot be detected due to lack of witness, which renders the monitoring-based misbehavior detection less.

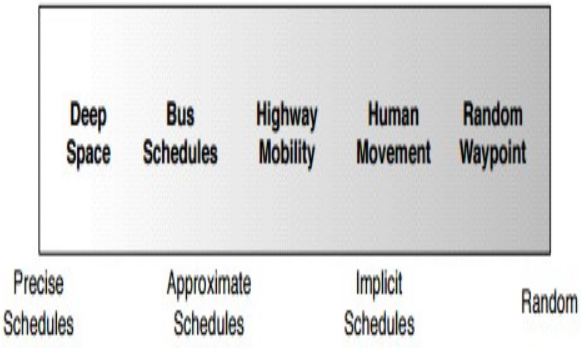
A comparison of the Internet and the DTN is illustrated in figure 1. What makes DTN disruptive and delay-tolerant is how the data, which is stored in bundles, can be transferred in regard to time by various methods. The versatility of the methods means that DTN can rely on TCP/IP or other protocols where suitable. Each DTN region can contain different delivery methods and implementations depending, on the unique situation.



1.1.Elements of a DTN application

The imagined principles of DTN applications are often mentioned in relation to extreme environments and to developing regions in rural areas, where they are expected to help with information access, e-government services, health care, education, and citizen journalism. Just as in a "legacy" Internet application, a DTN application is created to transfer information between nodes in a network: text, images, video, sound etc. Applications can be implemented in a network to perform a certain task, whether it be automated or user-generated data.

1.2.Contact Schedules



Of the four inter-node delay components, the most significant is likely to be the waiting time, since it might range anywhere from seconds to days whereas the others are typically much shorter. Thus, one of the most important characteristics of a DTN is the contact schedule, which depends strongly on the application area under consideration. Contact schedules can be placed on an approximate spectrum based on how predictable they are, as shown in Figure 2. At one extreme they have contact schedules that are very precise. An example would be deep space networks, where disconnections are caused by movements of objects in space thatcan be calculated very accurately. One step less predictable would be scheduled networks with errors.

II. EXISTING SYSTEM

- In this existing system the individual user data can be exchanged over the thirds party server [TPS].
- Individual data can be accessed through the third party server, and it can be out sourced.
- Before outsourcing, the secrety data must be encrypted and the same data are outsource.
- In this system, the particular secrecy data can be maintained by the central authority (CA) to the key management on behalf of third party owners.
- In this system, the malicious behaviors which may lead to the exposure of the secrecy data.
- In Existing the access policy based mechanism is not used.
- The nodes are trusted blindly.

2.1.Disadvantages

- In this system, for the individual user, there is a central authority for encryption and decryption.
- The Data can be accessed by the third party server and can be accessed by unauthorized users.
- Easily Notes may be Compromised and Reveals Secure Data.

III.PROPOSED SYSTEM

- In the proposed system, the secured sharing of secrecy data is stored in the trusted server storage along with the user's key.
- It can be protected using the CP-ABE Cipher text-Policy Attribute-Based and Encryption can be used to encrypt the particular user data as per the user needs.
- The encryption and the decryption of the key generation can be based on the type of attributes that user chooses.
- In this to improve security the user is categorized into public access data and the personal domains can be categorized.

- In the public domain, we will use multi authority to improve the security and to avoid unauthorized user access problem.
- Probabilistic Value is Calculated for Every nodes to identify node Trust

.

3.1.Advantages

- Data Integrity is maintained in CP-ABE
- In this system, improve the performance and Security of accessing the information based on Access policy and CP-ABE Algorithm.
- In this system, the individual user attribute information is selected based on the user needs of encrypting the data and for easily access using the CP-ABE.
- Probabilistic value based node trust raises Node Security for Data Transfer.

This could mean that an application could use legacy Internet where provided, if it can support the transition technically. For instance, if an application user travels between an urban city and an extreme environment where DTN communication is available, the application can in principle be made smart enough to recognize whether it is in an DTN environment or not, and use that information to select the optimal strategy.

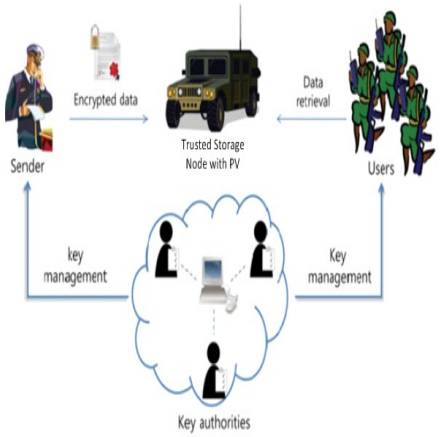
IV.METHODOLOGY

Methodology is the systematic, theoretical analysis of the methods applied to a field of study, or the theoretical analysis of the body of the methods and principles associated with a branch of knowledge. It, typically, encompasses concepts such as paradigm, theoretical model, phases, quantitative and qualitative techniques.

- DTN Network Initialization
- Identify Possible Path from Source to Destination
- Calculate Probabilistic Values of Intermediate Node
- Secure Data Transfer by using CB-ABE based on Probabilistic Values
-

4.1.DTN Network Initialization

The DTN network is used for data transfer in Military Applications, due to the Storage Capacity and Coverage type. The DTN network is constructed to the Military Users for Communication to the group of users based on the Coverage range. The User requested to the DTN network is joined to the network by the network provider Admin. Each Node or User is provided with Network Id and Secure Key for Data Transfer and Communication.



V. CONCLUSIONS

DTN 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. CP-ABE is a scalable cryptographic solution to the access control and secure data retrieval issues. In this paper, we proposed an efficient and secure data retrieval method using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. The inherent key escrow 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. In addition, the fine-grained key revocation can be done for each attribute group. We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network. Hence Attack identifications are detected by applying the techniques of CP - ABE algorithm and securely transactions on excuted in the network.

VI.FUTURE ENHANCEMENT

In CP-ABE the idea is purely related on the security of data, No one is concentrated on the problem in data transmission, to avoid such thread, the nodes in the DTN network are monitored by

Trusted Authority and set a probabilistic value, the probabilistic value denotes the node trust. So the Probabilistic misbehavior Scheme is used for secure data transmission.

VII. 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

[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, "Mesage ferry route design for sparse ad hoc networks with mobile nodes," in Proc. ACM Mobi Hoc, 2006

[4] 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.

[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 in vehicular ad hoc networks," Ad Hoc Netw., vol. 7, no. 8, pp. 1526–1535, 2009.

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