International Journal of Scientific Research and Modern Education (IJSRME)
ISSN (Online): 2455 – 5630
(www.rdmodernresearch.com) Volume I, Issue I, 2016

ENHANCING SECURITY IN DATA RETRIEVAL BY USING CB-ABE AND TRUST ESTABLISHMENT USING TRUST AUTHORITY

M. Ramesh* & A. Anitha**

* PG Scholar, Department of Master of Computer Applications, Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamilnadu

** Assistant Professor, Department of Master of Computer Applications, Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamilnadu

Abstract:

Malicious and selfish behaviors represent a serious threat against routing in delay/disruption tolerant networks. Due to the unique network characteristics, designing a misbehavior detection scheme in tolerant network (TN) is regarded as a great challenge. The sending information from source to destination, the message stored in a node in spite of destination user in a non- coverage area. In this paper, we propose iTrust Delay Torrent network (DTN), a probabilistic misbehavior detection scheme, for secure DTN several routing toward efficient trust establishment to the base station. The basic idea of iTrust is introducing a periodically available Trusted Authority (TA) to judge the node's behavior based on the collected routing evidences and probabilistically checking. We model iTrust as the inspection game and use game theoretical analysis to demonstrate that, by setting an appropriate investigation probability, TA could ensure the security of iTrust DTN routing at a reduced cost. To further improve the efficiency of the proposed scheme, we correlate detection probability with a node's reputation, which allows a dynamic detection probability determined by the trust of the users. The extensive analysis and simulation results demonstrate the effectiveness and efficiency of the proposed scheme.

Introduction:

DELAY tolerant networks (DTNs), such as sensor networks with scheduled intermittent connectivity, vehicular DTNs that disseminate location-dependent information (e.g., 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 dis-connectivity. 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 (e.g., 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 (e.g., sufficient buffers and meeting opportunities). Routing misbehavior can be caused by selfish (or rational) nodes that try to maximize their own benefits by enjoying the services provided by DTN while refusing to forward the bundles for others, or malicious nodes that drop packets or modifying the packets to launch attacks. The recent researches show that routing misbehavior will significantly reduce the packet delivery rate and, thus, pose a serious threat against the network performance of DTN. Therefore, a misbehavior detection and mitigation protocol is highly desirable to assure the secure DTN routing as well as the establishment of the secured among DTN nodes in DTNs. Mitigating routing misbehavior has been well studied in traditional mobile ad hoc networks. These works use neighborhood monitoring or destination acknowledgement to detect packet dropping, and exploit credit-based and reputation-based incentive schemes to stimulate rational nodes or revocation schemes to revoke malicious nodes. 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, difficulty 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 (e.g., dropping messages) cannot be detected due to lack of witness, which renders the monitoring-based misbehavior detection less.

Existing System:

In this existing system the individual user data can be exchanged over the thirds party server. Individual data can be accessed through the third party server, and it can be out sourced. Before outsourcing, the secrecy data to be encrypt and outsource the data. 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.

Disadvantages:

- ❖ In this system, for the individual user having the central authority for the encrypting and decrypting the Data.
- ❖ The Data can be accessed by the third party server and can be accessed by unauthorized users.
- ❖ Easily Compromised nodes and Reveals Secure Data.

Proposed System:

In the proposed system, iTrust Delay Torrent Network (DTN) is preferred for the Packets Node transmission and the secure sharing of secrecy data is storing on the trusted base station server storage nodes in presence of key management by users. It can be protected using the CP-ABE (Cipher text-Policy Attribute-Based 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 depend on the key authorities. 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.

Advantages:

- ❖ Data Integrity and Data Confidentiality 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.

Modules:

- ❖ DTN Network Initialization
- ❖ Identify Possible Path from Source to Destination
- ❖ Secure Data Transfer by using DES
- ❖ Identify the Coverage and Non-Coverage Node for packets transmission

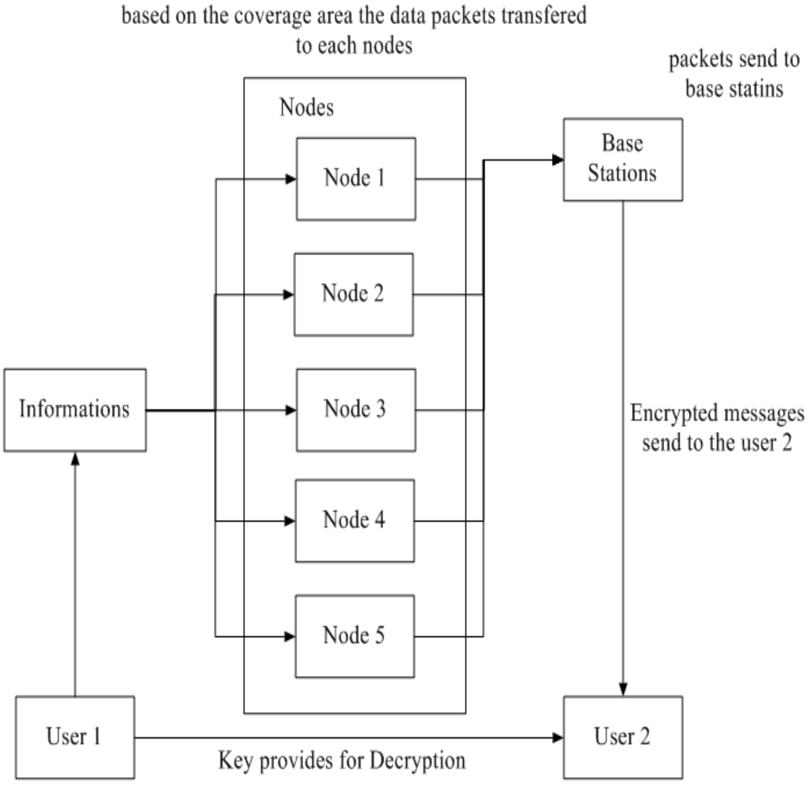
DTN Network Initialization: The DTN network is used for data transfer in Military Applications, due to the Storage Capacity and Coverage type. The DTN network is constructed to the Military Users for Communication to the group of users based on the Coverage range. The User requested to the DTN network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

Identify Possible Path from Source to Destination: In DTN network, the users to communicate with each other, the network users should be within the communicate range interconnected with multi number of nodes. The Network User is not to be aware of each node and make request to the base station, and the data send through number of packets in each node, if the connection is establish to the destination user, then the number of possible node path is to be identify from Source node to the base station. Then for each path the Intermediate node is to be Determined.

Identify the Coverage and Non-Coverage Node for Packets Transmission: The DTN node is monitored by each node in the tolerant networks. The Data packet is transferred to nearest node. DTN search the nearest coverage nodes. If the node is in coverage area, the data packets transferred. Otherwise the DTN search the another coverage node, For Example consider 3 nodes A, B, C So it distributes a broadcast message to each node A and C enquiring B, If the node A and B relays the Data Transfer Information and Acknowledgement of B, Then the data is transferred to B node is in coverage area, otherwise the packets transferred to node c.

Secure Data Transfer by using DES: The node is transferred based on the Delay Torrent Network, and the Node Security is determined, Now to improve the monitoring of the Data in the coverage area, Triple-Data Encryption Standard (DES) is Used, triple DES means data Encryption it Encrypts the node packets, then the Cipher text is transferred through the each node, The protocol agents thus act as surrogates for end-to-end sources and destinations, then the Cipher text is received and decrypted by the Destination node by Efficient Key Management.

System Architecture:


based on the coverage area the data packets transfered to each nodes
packets send to base statins
Nodes
Node 1
Node 2
Node 3
Node 4
Node 5
Base Stations
Informations
Encrypted messages send to the user 2
User 1
User 2
Key provides for Decryption

Conclusion:

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. DES is a scalable cryptographic solution to the access control and secures data retrieval issues. In this paper, we proposed an efficient and secure data retrieval method using DES 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.

Future Enhancement:

In DES 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.

References:

1. J. Burgess, B. Gallagher, D. Jensen, and B. N. Levine, “Max Prop: Routing for vehicle-based disruption-tolerant networking,” in Proc. IEEE Conf. Comput. Commun., Barcelona, Spain, Apr. 2006, pp. 1–11.
2. P. Hui, A. Chaintreau, J. Scott, R. Gass, J. Crowcroft, and C. Diot, “Pocket switched networks and the consequences of human mobility in conference environments,” in Proc. ACM SIGCOMM Workshop Delay Tolerant Netw., Philadelphia, PA, USA, Aug. 2005,pp. 244–251.
3. D. Zhao, H. Ma, S. Tang, et al., “COUPON: A cooperative framework for building sensing maps in mobile opportunistic networks,” to appear in IEEE Trans. Parallel Distrib. Syst., Feb.2014.
4. A. Seth, D. Kroeker, M. Zaharia, S. Guo, and S. Keshav, “Low-cost communication for rural internet kiosks using mechanical backhaul,” in Proc. 12th Annu. ACM Int. Conf. Mobile Comput. Netw., Los Angeles, CA, USA, Sep. 2006, pp. 334–345.
5. M. Grossglauser and D. N. C. Tse, “Mobility increases the capacity of ad hoc wireless networks,” IEEE/ACM Trans. Netw., vol. 10, no. 4, pp. 477–486, Aug. 2002.
6. P. Gupta and P. R. Kumar, “The capacity of wireless networks,” IEEE Trans. Inf. Theory, vol. 46, no. 2, pp. 388–404, Mar. 2000.
7. P. Li, Y. Fang, J. Li, and X. Huang, “Smooth trade-offs between throughput and delay in mobile ad hoc networks,” IEEE Trans. Mobile Comput., vol. 11, no. 3, pp. 427–438, Mar. 2012.
8. D. Ciullo, V. Martina, M. Garetto, and E. Leonardi, “Impact of correlated mobility on delay-throughput performance in mobile ad hoc networks,” IEEE/ACM Trans. Netw., vol. 19, no. 6, pp. 1745–1758, Dec. 2011.