ijiarec.com

ISSN: 2348-2079 FEB-2015

International Journal of Intellectual Advancements and Research in Engineering Computations

Efficient Data Retrieval by using AES for Disruption Tolerant Military Networks

[1]P.Sobiyaa, [2]R.M.Bhavadharini, [3]S.Karthik

ABSTRACT:

Disruption Tolerant Military Networks are designed to provide communication in the most unstable and stressed environment, where security and privacy are often critical in military application. Due to this, any attack can disrupt the operations in any part of the network. Cipher text Policy Attribute Based Encryption is a scalable cryptographic solution to the control access and secure data retrieval issues, where multiple key authorities manage their attributes independently. Key escrow problem is inherent such that the key authority can decrypt every cipher text by generating their secret keys. The system uses symmetric key encryption for ensuing end-to-end secure communication. Therefore, the system generates random 256 bit keys using AES (Advanced Encryption Standard). The main goal of DTN architecture is to provide interoperability between different kinds of networks in wide-ranging regions. This architecture originated from the Interplanetary Internet architecture then it is spread to the challenged networks more generally. Moreover, implementation of DTN is a good solution to supply people in remote military areas with the less Internet service for their communication.

Key Words: Disruption Tolerant Military Network, Cipher text Policy Attribute based Encryption, Advance Encryption Standard.

INTRODUCTION

Disruption Tolerant Military Network (DTN) is an approach to computer network architecture that seeks to address the technical issues in heterogeneous networks that may lack continuous network connectivity. Examples of such networks are those operating in mobile or extreme terrestrial environments, or planned networks in space.

In many military network scenarios, connections of wireless devices carried by soldiers may be temporarily disconnected by jamming, environmental factors, and mobility, especially when they operate in hostile environments. Disruption Tolerant Military Network (DTN) is becoming successful solutions that allow nodes to communicate with each other in these extreme networking environments. Typically, when there is no end-to-end connection between a source and a destination pair, the messages from the source node may need to wait in the intermediate nodes for a substantial amount of time until the connection would be eventually established.

Disruption Tolerant Military Network examines the bulk of the technologies that began the field that is known today as Delay Tolerant Networking. Research began as projects under United States government grants relating to the necessity of networking technologies that can sustain the significant delays and packet corruption of space travel. Initially, these projects looked only short-range communication between manned missions to the moon and back, but the field quickly expanded into an entire sub-field of DTNs

Author for Correspondence:

[1]PG Scholar, Department of CSE, SNS College of Technology, Coimbatore, India, E-mail: sobiyaa123@gmail.com

[2]Assistant Professor, Department of CSE, SNS College of Technology, Coimbatore, India, E-mail: rmbhavadharini@yahoo.com

[3]Prof & Dean, Department of CSE, SNS College of Technology, Coimbatore, India, E-mail: profskarthik@gmail.com

that created the technological advances to allow for the Interplanetary Internet.

With the growing interest in mobile ad hoc routing and the increasing complexity of the Interplanetary Internet, the 2000s (decade) brought about a growing number of academic conferences on delay and disruption-tolerant networking. This field saw many optimizations on classic ad hoc and delay-tolerant networking algorithms and began to examine factors such as security, reliability, verifiability, and other areas of research that are well understood in traditional computer networking.

In efforts to provide a shared framework for algorithm and application development in DTNs, RFC 4838 and RFC 5050 were published in 2007 to define a common abstraction to software running on disrupted networks. Commonly known as the Bundle Protocol, this protocol defines a series of contiguous data blocks as a bundle—where each bundle contains enough semantic information to allow the application to make progress where an individual block may not. Bundles are routed in a store and forward manner between participating nodes over varied network transport technologies (including both IP and non-IP based transports). The transport layers carrying the bundles across their local networks are called bundle convergence layers. The bundle architecture therefore operates as an overlay network, providing a new naming architecture based on Endpoint Identifiers (EIDs) and coarse-grained class of service offerings.

Protocols using bundling must leverage application-level preferences for sending bundles across a network. Due to the store and forward nature of delay-tolerant protocols, routing solutions for delay-tolerant networks can benefit from exposure to application-layer information. For example, network scheduling can be influenced if application data must be received in its entirety, quickly, or without variation in packet delay. Bundle protocols collect application data into bundles that can be sent across heterogeneous network configurations with high-level service guarantees. The service guarantees are generally set by the application level, and the RFC 5050 Bundle Protocol specification includes "bulk", "normal", and "expedited" markings.

Addressing security issues has been a major focus of the bundle protocol. Security concerns for Disruption-Tolerant Networks vary depending on the environment and application, though authentication and privacy are often critical. These security guarantees are difficult to establish in a network without persistent connectivity because the network hinders complicated cryptographic protocols, hinders key exchange, and each device must identify other intermittently visible devices. Solutions have typically been modified from mobile ad hoc network and distributed security research, such as the use of distributed certificate authorities and PKI schemes.

SECURITY GOALS

Availability

The network should be available only for the authenticated entity.

Confidentiality

In MANET it is very hard to attain the confidentiality due to intermediate nodes routing, which can easily retrieve the information from the routing nodes.

Integrity

The transmission of information should be protected against any alteration and message modification.

Authentication

The network should be accessed only by the authenticated nodes such as Digital signature, Reply and Non repudiation.

Non-Repudiation

Ensure the user does not refute that he used the network.

RELATED WORK

Disruption Tolerant Military Networks (DTN) 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. An attribute based data retrieval schema [1] using Cipher text Policy-Attribute Based Encryption (CP-ABE) for decentralized DTNs where multiple key authorities manage their attributes independently. The problem of applying CP-ABE in decentralized DTNs introduces several security and privacy challenges with regard to the attribute revocation, key escrow, and coordination of attributes issued from different authorities. First, immediate attribute revocation enhances backward/forward secrecy of confidential data by reducing the windows of vulnerability. In the context of ABE, backward secrecy means that any user who comes to hold an attribute should be prevented from accessing the plaintext of the previous data exchanged before he holds the attribute. On the other hand, forward secrecy means that any user who drops an attribute should be prevented from accessing the plaintext of the subsequent data exchanged after he drops the attribute, unless the other valid attributes that he is holding satisfy the access policy. Second, encryptor can define a fine-grained access policy using any monotone access structure under attributes issued from any chosen set of authorities. Third, the key escrow problem is resolved by an escrow-free key issuing protocol that exploits the characteristic of the decentralized DTN architecture. The key issuing protocol generates and issues user secret keys by performing a secure two-party computation (2PC) protocol among the key authorities with their own master secrets. Thus, users are not required to fully trust the authorities in order to protect their data to be shared. The data confidentiality and privacy can be cryptographically enforced against any curious key authorities or data storage nodes. Unauthorized users who do not have enough credentials satisfying the access policy should be deterred from accessing the plain data in the storage node. In addition, unauthorized access from the storage node or key authorities is prevented. 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.

Mobile nodes in some challenging network scenarios suffer from intermittent connectivity and frequent partitions e.g. battlefield and disaster recovery scenarios. Disruption Tolerant Military Networks (DTN) is designed to enable nodes in such environments to communicate with one another. Several DTN routing schemes have been proposed. However, not much work has been done on providing information access in such challenging network scenarios. There are three main components in our content-based information retrieval system [7], namely data caching, query dissemination, and message routing. Data Caching Schemes consist of K-copy random caching and K-copy intelligent caching. In K-copy random caching where each node j, will pass a copy of the data item to a node that j encounters next. Such an action is repeated K times so K nodes will store this data item. In K-copy intelligent Caching where a spray and wait routing scheme where a source node generates L tokens for any message it generates. Query Dissemination Schemes is a list of data items that are currently stored in this particular node and within its L-hop neighborhood of this node. Once a query response is generated by a node, the query response will be delivered to the querying node using the underlying DTN message routing scheme. Two DTN routing scheme such as Prophet Scheme and Highest Encountered First Routing (HEFR) scheme are used.

MaxProp protocol [4] for effective routing of DTN messages. Disruption Tolerant Military Networks (DTNs) attempt to route network messages via intermittently connected nodes. Routing in such environments is difficult because peers have little information about the state of the partitioned network and transfer opportunities between peers are of limited duration. MaxProp is based on prioritizing both the schedule of packets transmitted to other peers and the schedule of packets to be dropped. These priorities are based on the path likelihoods to peers according to historical data and also on several complementary mechanisms, including acknowledgments, a head-start for new packets, and lists of previous intermediaries. Evaluations show that Max Prop performs better than protocols that have access to an oracle that knows the schedule of meetings between peers. Evaluations are based on 60 days of traces from a real DTN network deployed on 30 buses. DTN operations proceeds roughly in three stages, they are neighbour discovery, data transfer, storage management. Peers must discover one another before a transfer opportunity can begin, they do not know when the next opportunity will begin. When two peers meet, the amount of data they can transfer is limited. Peers do not know the duration of each opportunity. As packets are received from a neighbour, each peer must manage its finite local buffer space by selecting packets to delete according to some algorithm. Messages that are destined for a receiving peer are passed up to the application layer and removed from the buffer. Each peer carries all messages until the next meeting occurs. A peer will continue to forward a message to any number of other peers until its copy of the message times out, it is notified of delivery by an ack, or the message is dropped due to a full buffer. Bandwidth can be a limited resource when the transfer opportunities are of short duration (which may be the result of a slow neighbour discovery protocol) or when the radio used has low bandwidth. Storage can be limited when such devices as motes, PDAs, or cell phone are used. Offered message load can affect both storage and bytes transferred. MaxProp as an effective protocol for DTN routing, particularly for the context of real DTN deployment. MaxProp unifies the problem of scheduling packets for transmission to other peers and determining which packets should be deleted when buffers are low on space.

EXISTING SYSTEM

Key Authorities

There are key generation centers that generate public/secret parameters for CP-ABE. The key authorities consist of a central authority and multiple local authorities. There are secure and reliable communication channels between a central authority and each local authority during the initial key setup and generation phase. Each local authority manages different attributes and issues corresponding attribute keys to users. They grant differential access rights to individual users based on the users' attributes. The key authorities are assumed to be honest-but-curious. That is, they will honestly execute the assigned tasks in the system; however they would like to learn information of encrypted contents as much as possible.

Storage Node

This is an entity that stores data from senders and provide corresponding access to users. It may be mobile or static. Similar to the previous schemes, we also assume the storage node to be semi trusted, that is honest-but-curious.

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.

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 revoked in any of the attributes, then he will be able to decrypt the cipher text and obtain the data. Since the key authorities are semi-trusted, they should be deterred from accessing plaintext of the data in the storage node, meanwhile, they should be still able to issue secret keys to users.

PROPOSED SYSTEM

Disruption Tolerant Military Network are becoming successful solutions that allow nodes to communicate with each other in the extreme networking environment. The Advanced Encryption Standard applies more confidentiality in sending the data by applying security policies from source to destination in DTN, where unauthorized users who do not have enough credentials satisfying the access policy should be deterred from accessing the data in the storage node. In addition, unauthorized access from the storage node or key authorities should be also prevented. The algorithm is secure in nature especially against variety of active and passive attacks. Proposed scheme features the following achievements. First, immediate attribute revocation enhances backward/forward secrecy of confidential data by reducing the windows of vulnerability. Second, the key escrow problem is resolved by using Advanced Encryption Standard. Third, the energy consumption can be reduced as nodes only communicate with storage unit.

The proposed mechanism is cluster based in which, when DTN is deployed for any application, nodes form two-hop cluster for coordination. In cluster-based DTN, the optimal cluster size is two hop as presented. The concept of clustering in Disruption Tolerant Networking, especially about routing and security. Moreover, we think that the implementation of cluster based DTN is a good solution to supply people in remote military areas with the less Internet service for their communication.

Energy consumption can be reduced when nodes only communicate with storage unit. So our energy model is cluster-based DTN. To reduce the energy consumption, the system applies clustering in DTN architecture is to provide interoperability between different kinds of networks in wide-ranging regions.

The mechanism is secure in nature especially against variety of active and passive attacks. The system uses symmetric key encryption for ensuing end-to-end secure communication like SSL but this approach is very difficult to be applied to this disruption-tolerant environment due to handshake for generating a shared key. Therefore, the system generates random 256 bit keys using AES (Advanced Encryption Standard). The recipients encrypt this key using its public key and decrypt the data after decrypting the AES key by using their own private key.

CONCLUSION

DTN 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. Existing system which uses the two Party Computation protocol to solve key escrow problem, however, 2PC protocol is carried out only once during the initial key generation phase for each user. The proposed system solve the inherent key escrow problem by using Advanced Encryption Standard, such that the confidentiality of the stored node is guaranteed even under the hostile environment where key authorities might be compromised or not fully trusted. The data confidentiality and privacy can be cryptographically enforced against any curious key authorities in the proposed system.

REFERENCES

[1]. Aparna.V, Jabisha Arul, Nandhini. S, Vishnu Kumar. A, (2013) "Multi Attribute Based Technique in Key Generation System", IJEAT ISSN: 2249– 8958, Volume-2, Issue-4.

[2]. Ashokbaburaj. S,Alagarsamy. K, (2014) "Repetitive trust management and adversary detection for delay tolerant networks", Journal of theoretical and applied information technology, Vol. 61 no.3.

[3]. Burgess. J, Gallagher. B, Jensen. D, and Levine. B.N, (2006) "Maxprop:Routing for vehicle-based disruption tolerant networks", in Proc.IEEE Infocom,pp. 1–11.

[4]. Chase. M and Chow. S.S.M, (2009) "Improving privacy and security in multiauthority attribute-based encryption", in Proc. ACM Conf. Comput. Commun. Security,pp. 121–130.

[5]. Chen. N, Gerla. M, Huang. D, and Hong. X, (2010) "Secure, selective group broadcast in vehicular networks using dynamic attribute based encryption", in Proc. Ad Hoc Netw. Workshop,pp. 1–8.

[6]. Chuah. M and Yang. P, (2007) "Performance evaluation of content-basedInformation retrieval schemes for DTNs", in Proc. IEEE MILCOM,pp. 1–7

[7]. Chuah. M and Yang. P, (2006) "Node density-based adaptive routing schemefor disruption tolerant networks", in Proc. IEEE MILCOM, pp.1–6.

[8]. Gunasekaran. M, Premalatha. K, (2014) "An Anonymity Based Secure On-Demand Routing for Mobile Ad Hoc Networks", International Journal of Computer, Information, Systems and Control Engineering.

[9]. Haojin Zhu, Xiaodong Lin, Rongxing Lu, Yanfei Fan, and XueminShen, (2009) "SMART: A Secure Multilayer Credit-Based Incentive Scheme for Delay-Tolerant Networks", IEEE Transactions on Vehicular Technology, vol. 58, no. 8.

[10]. JunbeomHur and Kyungtae Kang, (2014) "Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks", IEEE/ACM transactions on networking, vol.22, no.1.

[11]. Pirretti. M, Traynor. P, McDaniel. P, and Waters. B, (2006) "Secure attribute based systems", in *Proc.* ACM Conf. Comput. Commun. Security, pp. 99–112.

[12]. Rafaeli. S and Hutchison. D, (2003) "A survey of key management for secure group communication", Comput. Surv., vol. 35, no. 3, pp. 309–329.

[13]. Rongxing Lu, Xiaodong Lin, (2006) "PReFilter: An Efficient Privacy-preserving Relay Filtering Scheme for Delay Tolerant Networks", IEEE/ACMtransactions on networking.

[14]. Sahai. A and Waters. B, (2005) "Fuzzy identity-based encryption", in Proc.Eurocrypt, pp. 457–473.

[15]. Wong. C.K, Gouda. M, and Lam. S.S, (1998) "Secure group communications using key graphs", in Proc. ACM SIGCOMM, pp. 68–78.