Timely and Secure Data Transmission in Disruption Tolerant Networks

S. Hemalatha[1], S. Priyanka[2]

[1]*Assistant Professor* [2]*Research Scholar*

Abstract—Disruption Tolerant Networks (DTNs) include mobile devices. The most plan for that approach wont to support cooperative caching in DTNs, that make the sharing and coordination of cached information among multiple nodes and reduces information access delay. Conjointly produce the designedly cache information in an exceedingly set of network central locations (NCLs), which may be simply access by alternative nodes within the network. Propose AN economical methodology that ensures applicable NCL choice supported a probabilistic choice metric and coordinates multiple caching nodes to optimize the trade-off between information accessibility and caching overhead. The chosen NCLs attain high possibilities for prompt response to user queries with low overhead in network storage and communication. The utility-based cache replacement theme is wont to dynamically modify cache locations supported question history, and this theme achieves smart trade-off between the info accessibility and access delay. To introduce the novel caching protocol adjustive to the difficult for DTNs. To derive AN adjustive caching sure for every mobile node per its specific contact pattern with others, to limit the nice amount of data into its caches. During this manner, each the space for storing and therefore the contact opportunities are higher used. Intensive trace-driven simulations show that our cooperative caching protocol will considerably improve the performance of knowledge access in DTNs.

Keywords— Disruption Tolerant Networks, network central locations, attribute-based encryption, access points, Cipher text-policy attribute-based encryption.

I. INTRODUCTION

The design of the present net service models is predicated on some assumptions like (a) the existence of associate degree finish to-end path between a supply and destination, and (b) low rout trip latency between any node. However, the nodes don't hold in some rising networks. Some examples ar: (i) battleground and ad-hoc networks in wireless devices carried by troopers operate in hostile environments that are ECM, environmental factors and quality could cause temporary disconnections, and (ii) conveyance ad-hoc networks the buses are equipped with wireless modems and have intermittent RF property with each other. within the on top of eventualities, associate degree end-to-end path between a supply and a destination combine might not invariably exist wherever the links between intermediate nodes could also be timeserving, predictably connectable, or sporadically connected. This enable nodes to speak with one another within the extreme networking environments, and [2] the Disruption-tolerant network (DTN) technologies are used for productive solutions that enable nodes to speak with one another. Typically, once there's no end-to-end association between a supply and a destination combine, the messages from the supply node are often ought to wait within the intermediate nodes for a considerable quantity of your time till the association ought to be established. Once the association is made, the message is delivered to the destination node. In storage nodes in DTNs [19] knowledge are often hold on or replicated specified solely licensed mobile nodes will access the mandatory data quickly. A demand in some security-critical applications is to style associate degree access system to safeguard the confidential knowledge hold on within the storage nodes or contents of the confidential messages routed through the network. As associate degree example, in an exceedingly battleground DTN, a storage node could have some guidance that ought to be accessed solely by many current solutions. The standard cryptographic-based approach wherever the contents are encrypted before being hold on in storage nodes, and therefore the secret writing keys are distributed solely to licensed users. In such approaches, flexibility and graininess of content access management depends heavily on the underlying cryptologic primitives being employed. It's arduous to balance between the quality of key management and therefore the graininess of access management mistreatment any solutions that are supported the standard combine wise key or cluster wise key primitives. The on top of approach must give a scalable resolution which will give fine-grain access management. that's a DTN design wherever multiple authorities issue and manage their own attribute keys severally as a redistributed DTN. A CP-ABE[4] primarily based secret writing theme provides fine-grained access management. in an exceedingly CP-ABE theme, every user is related to a collection of attributes supported that the users non-public secret is generated. The Contents are encrypted underneath associate degree access policy .This access policy supported the users attributes match the access policy so knowledge are often decode. Our theme will give not solely fine-grained access management to every content object

however additionally additional subtle access management antics. Cipher text-policy attribute-based secret writing (CP-ABE) could be a guaranteeing cryptologic account the proper to realize entrance management problems. In several case, the problem of applying CP-ABE in redistributed DTNs presents some securities and protection challenges on the property and coordination of characteristics issued from distinctive powers.

II. SYSTEM MODEL

For each data item in the network, the locations where it is cached are dynamically adjusted via cache replacement. This replacement is based on data popularity, and generally places popular data nearer to the central nodes of NCLs. Proposing a probabilistic cache replacement strategy, which appropriately selects the data to be cached and balances between the cumulative data accessibility and access delay.

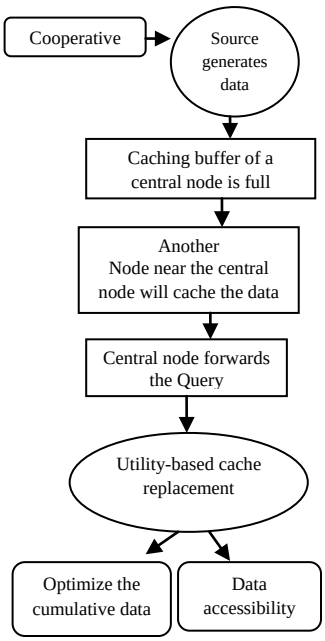

Figure1: System model

Proposed intentional caching scheme achieves much better successful ratio and delay of data access.

When a data source generates data, it pushes data tocentral nodes of NCLs, which are prioritized to cache data. One copy of data is cached at each NCL. If the caching buffer of a central node is full, another node near the central node will cache the data. Propose a utility-based cache replacement scheme to dynamically adjust cache locations based on query history, and to achieves good tradeoff between the data accessibility and access delay. To intentionally cache data at a set of network central locations (NCLs), this can be easily accessed by other nodes in the network. Data access scheme to probabilistically coordinate multiple caching nodes for responding to user queries.

III. PREVIOUS WORK

Efficient relay selection metrics to approach the performance of Epidemic routing with lower forwarding cost, based on prediction of node contacts in the future. Some schemes do such prediction based on their mobility patterns, which are characterized by filter or semi-Markov chains. In some other schemes, node contact pattern is exploited as abstraction of node mobility pattern for better prediction accuracy based on the experimental and theoretical analysis of the node contact characteristics. The social network properties of node contact patterns, such as the centrality and community structures, have also been also exploited for relay selection in recent social-based data forwarding schemes. The aforementioned metrics for relay selection can be applied to various forwarding strategies, which differ in the number of data copies created in the network. While the most conservative strategy always keeps a single data copy and Spray-and-Wait holds a fixed number of data copies, most schemes dynamically determine the number of data copies. In Compare-and-Forward a relay forwards data to another node whose metric value is higher than itself. Delegation forwarding reduces forwarding cost by only forwarding data to nodes with the highest metric. Data access in DTNs, on the other hand, can be provided in various ways .Data can be disseminated to appropriate users based on their interest profiles.

Publish/subscribe systems were used for data dissemination, where social community structures are usually exploited to determine broker nodes. In other schemes without brokers, data items are grouped into predefined channels, and are disseminated based on users' subscriptions to these channels. Caching is another way to provide data access. Cooperative caching in wireless ad hoc networks, in which each node caches pass-by data based on data popularity, so that queries in the future can be responded with less delay. Caching locations are selected incidentally among all the network nodes. Some research efforts have been made for caching in DTNs, but they only improve data accessibility from infrastructure network such as WiFi access points (APs) or Internet. Peer-to-peer data sharing and access among mobile users are generally neglected. Distributed determination of caching policies for minimizing data access delay has been studied in DTNs, assuming simplified network conditions. In , it is assumed that all the nodes contact each other with the same rate. Users are artificially partitioned into several classes such that users in the same class are identical. Data are intentionally cached at appropriate network locations with generic data and query models, but these caching locations

are determined based on global network knowledge. Comparatively, in this paper, propose to support cooperative caching in a fully distributed manner in DTNs, with heterogeneous node contact patterns and behaviors.

IV. PROPOSED METHODOLOGY

The propose a completely unique approach to support cooperative caching in DTNs, that allows the sharing and coordination of cached knowledge among multiple nodes and reduces knowledge access delay. The fundamental plan is to designedly cache knowledge at a collection of network central locations (NCLs), which might be simply accessed by different nodes within the network. Propose associate degree economical theme that ensures acceptable NCL choice supported a probabilistic choice metric and coordinates multiple caching nodes to optimize the trade-off between knowledge accessibility and caching overhead. Propose a completely unique theme to handle the said challenges and to expeditiously support cooperative caching in DTNs. the fundamental plan is to designedly cache knowledge at a collection of network central locations (NCLs), every of that corresponds to a gaggle of mobile nodes being simply accessed by different nodes within the network. every NCL is pictured by a central node, that has high quality within the network and is prioritized for caching knowledge. thanks to the restricted caching buffer of central nodes, multiple nodes close to a central node is also concerned for caching, and make sure that fashionable knowledge area unit perpetually cached nearer to the central nodes via dynamic cache replacement supported question history. The elaborate contributions area unit listed as follows

To develop associate degree economical approach to NCL choice in DTNs supported a probabilistic choice metric. the chosen NCLs reach high probabilities for prompt response to user queries with low overhead in network storage and transmission. The propose an information access theme to probabilistically coordinate multiple caching nodes for responding to user queries. To optimize the trade-off between knowledge accessibility and caching overhead, to attenuate the typical variety of cached knowledge copies within the network. The propose a utility-based cache replacement theme to dynamically regulate cache locations supported question history, and also the theme achieves smart trade-off between the information accessibility and access delay.

Network Central Locations

During this section, describe a way to choose NCLs supported a probabilistic metric evaluating the information transmission delay among nodes in DTNs; validate the pertinence of such metric in follow supported the no uniformity of node contact pattern in realistic DTN traces. moreover, propose elaborate ways for choosing NCLs in follow supported completely different handiness of network info.

Multichip opportunist association On Network

The information transmission delay between 2 nodes A and B, indicated by the variant Y, is measured by the burden of the shortest opportunist path between the 2 nodes. In follow, mobile nodes maintain the data concerning shortest opportunist methods between one another in an exceedingly distance-vector manner after they inherit contact.

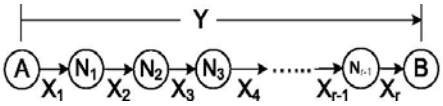

Figure 2. Opportunist Path

Caching theme

During this section, gift cooperative caching theme. the fundamental plan is to designedly cache knowledge at a collection of NCLs, which might be promptly accessed by different nodes. The theme consists of the subsequent 3 components:

1. once supply generates data, it pushes knowledge to central nodes of NCLs, that area unit prioritized to cache knowledge. One copy of knowledge is cached at every NCL. If the caching buffer of a central node is full, another node close to the central node can cache the information. Such choices area unit mechanically created supported buffer conditions of nodes concerned within the pushing method.

2. A requester multicasts a question to central nodes of NCLs to drag knowledge, and a central node forwards the question to the caching nodes. Multiple knowledge copies area unit came to the requester, and optimize the trade-off between knowledge accessibility and transmission overhead by dominant the quantity of came knowledge copies.

3. Utility-based cache replacement is conducted whenever 2 caching nodes contact and ensures that fashionable knowledge area unit cached nearer to central nodes. For usually cache additional copies of fashionable knowledge to optimize the additive knowledge access delay. Additionally probabilistically cache less fashionable knowledge to make sure the general knowledge accessibility.

Caching Location

Whenever a node S generates new knowledge, S pushes the information to NCLs by causation an information copy to

every central node representing a NCL. Use the opportunist path weight to the central node as relay choice metric for such knowledge forwarding, and a relay forwards knowledge to a different node with the next metric than itself. This "Compare-and-Forward" strategy has been wide utilized in the literature for economical knowledge forwarding. For new generated knowledge, the initial caching locations area unit mechanically determined throughout the forwarding method supported node buffer conditions. The caching locations area unit then dynamically adjusted by cache replacement delineate consistent with question history. In general, knowledge area unit forwarded to and cached at central nodes. This forwarding method solely stops once the caching buffer of ensuing relay is full, four and knowledge area unit cached at this relay in such cases. In different words, throughout forwarding method toward central nodes relays carrying data area unit thought-about as temporal caching locations of the information. Such determination of caching location is illustrated in Fig. 8, wherever the solid lines indicate opportunist contacts accustomed forward knowledge, and also the broken lines indicate knowledge forwarding stopped by node buffer constraint. Central node

•C1 is ready to cache knowledge, however knowledge copies to C2 and C3 area unit stopped and cached at relays R24 and R33, severally, as a result of neither C2 nor R3 four has enough buffer to cache knowledge.

•Note that the caching location at a NCL might not be the contacted neighbor of a central node, just like the case of nodes R33,in Fig. 8.

•From this strategy, it's straightforward to visualize that the set of caching nodes at every NCL forms a connected sub graph of the network contact graph at any time throughout knowledge access.

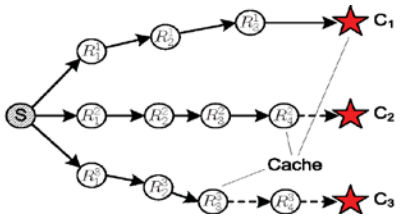

Figure3. Determining

Queries

Assume that any node could request knowledge, and hence, knowledge requesters area unit every which way distributed within the network. Requester multicasts a question with a finite time constraint to any or all the central nodes to drag knowledge, and existing multicast schemes in DTNs will be exploited for this purpose. when having received the question, a central node right away replies to the requester with knowledge if it's cached domestically. Otherwise, it broadcasts the question to the nodes close.

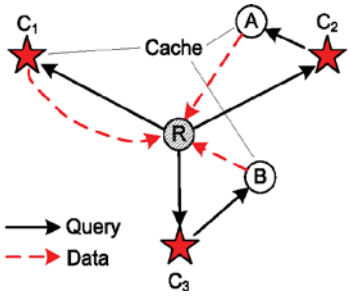

Figure4 propulsion knowledge from the NCLs

This method is illustrated in Fig. 3 whereas the central node C1 is ready to come the cached knowledge to R right away, the caching nodes A and B solely reply to R when they receive the question from central nodes C2 and C3, severally. The question broadcast finishes once question expires.

Cache Replacement

For every knowledge item within the network, the locations wherever it's cached area unit dynamically adjusted via cache replacement. This replacement relies on knowledge quality, and usually places fashionable knowledge nearer to the central nodes of NCLs. ancient cache replacement methods like LRU, that removes the least-recently-used knowledge from cache once new knowledge area unit out there, area unit ineffective thanks to its over simple thought of knowledge quality. Greedy-Dual-Size calculates knowledge utility by considering knowledge quality and size at the same time, however cannot guarantee best choice of cached knowledge. to boost previous work by proposing a probabilistic cache replacement strategy, that befittingly selects {the knowledge the info the information} to be cached and heuristically balances between the additive data accessibility and access delay.

Ncl Load equalization

First, the central nodes cache the foremost fashionable knowledge within the network and answer the frequent queries for these knowledge. Second, the central nodes also are accountable for broadcasting all the queries they receive to different caching nodes close. However, such practicality could quickly consume the native resources of central nodes that embody their battery life and native memory. additionally, would love our caching schemes to be resilient to failures of central nodes. during this section, To specialise in addressing this challenge, and propose ways that

expeditiously migrate the practicality of central nodes to different nodes in cases of failures or resource depletion. In general, the ways resent during this section will be accustomed regulate the readying of central nodes at runtime, like adding or removing central nodes consistent with up-to-date necessities on caching performance.

Selecting the New Central Node

When a central node fails or its native resources area unit depleted, another node is chosen as a replacement central node. Intuitively, the new central node ought to be the one with the very best NCL choice metric worth among this non central nodes within the network. However, such choice could degrade the caching performance.

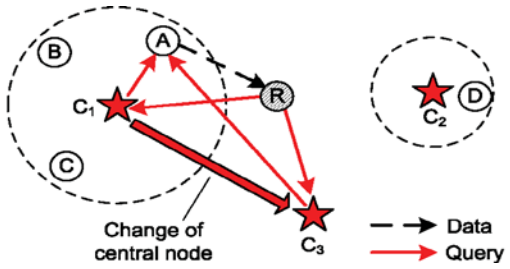

Figure5..Central node

V. SIMULATION/EXPERIMENTAL RESULT

For evaluate the performance of our proposed caching scheme by comparing it with the following schemes:

No Cache, where caching is not used for data access and each query is only responded by data source. Random Cache, in which every requester caches the received data to facilitate data access in the future.

Cache Data, which is proposed for cooperative caching in wireless ad hoc networks, and lets each relay in DTNs cache the pass-by data based on their popularity.

Bundle Cache, which packs network data as bundles and makes caching decision on pass-by data by considering the node contact pattern in DTNs, so as to minimize the average data access delay.

Cache replacement algorithms are proposed in Cache- Data and Bundle Cache, and will also be used in our evaluations. For Random Cache, LRU is used for cache replacement. The following metrics are used for evaluations. Each simulation is repeated multiple times with randomly generated data and queries for statistical convergence:

Successful ratio: The ratio of queries being satisfied with the requested data. This ratio evaluates the coverage of data access provided by our proposed caching schemes.

Data access delay: The average delay for getting responses to queries.

Caching overhead: The average number of data copies being cached in the network

VI. CONCLUSIONS

In this paper, propose a novel scheme to support cooperative caching in DTNs. Our basic idea is to intentionally cache data at a set of NCLs, which can be easily accessed by other nodes. To ensure appropriate NCL selection based on a probabilistic metric; approach coordinates caching nodes to optimize the tradeoff between data accessibility and caching overhead. Extensive simulations show that scheme greatly improves the ratio of queries satisfied and reduces data access delay, when being compared with existing schemes.

For the future work proposed Cipher text policy attribute-based encryption (CP-ABE) is a promising cryptographic solution to the access control issues. In this paper, to propose a secure data retrieval scheme using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. In CP-ABE, the key authority generates private keys of users by applying the authority's master secret keys to users' associated set of attributes.

VII. FUTURE SCOPES

In future work based on in addition, the fine-grained key revocation can be done for each attribute group. The proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network. The data confidentiality and privacy can be cryptographically enforced against any curious key authorities or data storage nodes in the proposed scheme.

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, "Mesage 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 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,"CryptologyePrint Archive: Rep. 2010/351, 2010.

[11] A. 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.

[16] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in *Proc. ACM Conf. Comput. Commun. Security*, 2008, pp. 417–426.

[17] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure attributebased systems," in *Proc. ACMConf. Comput. Commun. Security*, 2006, pp. 99–112.

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

[19] S. Mittra, "Iolus: A framework for scalable secure multicasting," in *Proc. ACM SIGCOMM*, 1997, pp. 277–288.

[20] P. Golle, J. Staddon, M. Gagne, and P. Rasmussen, "A content-driven access control system," in *Proc. Symp. Identity Trust Internet*, 2008, pp. 26–35.

[21] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in *Proc. ACM Conf. Comput. Commun. Security*, 2007, pp. 456–465.

[22] V.Goyal, A. Jain,O. Pandey, andA. Sahai, "Bounded ciphertext policy attribute-based encryption," in *Proc. ICALP*, 2008, pp. 579–591.

[23] X. Liang, Z. Cao, H. Lin, and D. Xing, "Provably secure and efficient bounded