International Journal of Research In Science & Engineering e-ISSN: 2394-8299
Volume: 4 Issue: 2 March-April 2018 p-ISSN: 2394-8280

A REVIEW OF ROUTING PROTOCOLS AND APPLICATIONS IN DELAY TOLERANT NETWORK

Archana Luhan[1], Prof. Apurva Kukade[2]

Mtech Scholar,Department of Computer Science, Alpine College of Technology ,Ujjain,India
er.archanaluhan@gmail.com
Assistant Professor,Department of Computer Science,Alpine College of Technology ,Ujjain,India
apurvak4u@gmail.com

Abstract— Delay-tolerant networks, DTNs, are defined through lacking deliver end-to-end paths between conversation resources and locations. A form of routing protocols like Epidemic, PROPHET and Spray-and-Wait DTN routing protocols are described on this paper. In a DTN, most of the time there aren't any end-to-end paths from conversation sources to destinations due to node mobility, wireless propagation results, sparse node density, and distinct negative elements. For this class of network, traditional ad hoc routing protocols, which rely upon give up-to-give up paths, fail to work. Spray-and-Wait routing protocol controls the spreading of messages within the network. Unlike PROPHET routing however like Epidemic routing, it has no preceding information of encountering nodes and certainly forwards more than one copies of messages to nodes it encounters.

Keywords— DTN, ERP, PRoPHET Routing Protocol, Spray and wait protocol, Applications.

I. INTRODUCTION

DTN [1] is a category of networking technology that intends to offer the conversation in environments wherein give up-to-stop course isn't solid or disintegrate quickly after it has been found. The message transmission is done through opportunistic contacts by way of adopting shop-convey and ahead paradigm. Accordingly, the node shops the incoming message in its buffer, includes it at the same time as moving and forward whilst comes inside the transmission variety of different contacts. The goal of DTN routing protocols is to increase the delivery of the message by consuming the least extent of network sources. However, due to frequent disconnection and network partitions, the delivery like hood is raised by means of forwarding the a couple of copies of the equal message alongside diverse paths.

One such strategy is called Epidemic routing [2] in which every node executes the pair wise alternate of the message on all encountering nodes. This phenomenon increases the message transmissions and exhausts the network assets. The probabilistic PRoPHET routing protocol[3] transmits the message by way of looking at motion sample in phrases of encountering rate of nodes amongst each other. For example, the node forwards the message to every other node that holds high probability value to meet its destination than its personal.

The PROPHET protocol blocks the message transmission on peers maintaining minimum predictability value. However, the message diffusion from the least probable node continues on the higher probable connections. In this manner, PRoPHET Protocol operates as the probabilistic version of Epidemic based dimension. Moreover, when a node is highly probable to meet several destinations then it is expected to receive the traffic flow from multiple sources. Since, energy is the most important aid that a node consumes to transmit and get hold of the messages. Hereby, with finite strength the receiver may devour its battery best in receiving the messages. As a result, the node can go to the dead state and will reduce the network throughput because the previously stored
Messages have lost their opportunity to be delivered. In addition, most of the previous [4][5][6][20] work has focused on the consumption of node energy in comparison of the number of transmissions.

Despite the message transmission provides a good view about measuring energy usage, the real-time traffic consists of heterogeneous data packets of random sizes. It is apparent that a message of large size calls for extra strength from the sender to send and get hold of to get hold of. Therefore, the number of transmissions cannot provide a very good insight approximately the energy size of the routing protocol. The contribution to this paper is as follows:-

• We have proposed Look-Ahead probabilistic Energy Aware Routing approach for DTN that operates underneath finite strength.
We have proposed a software element called as energy supervisor that operates at the top of the bodily tool, i.e. Battery.

- We have proposed a new metric referred to as Estimated Energy (EE) that computes the energy consumption (transmit, acquire) of nodes primarily based at the message sizes.
- We have proposed energy aware transmission technique that operates with Estimated Energy (EE) and ahead the message via staring at the closing energy of transmitter and receiver.

II. DELAY TOLERANT NETWORK

DTN are a category of networks that lack continuous connectivity between nodes because of restricted wireless radio coverage, broadly scattered mobile nodes, confined strength sources, high levels of interference or because of a few other similar channel impairment [5]. Most of these DTN routing protocols belong to one of these three classes:

A. Message-ferry-based
A. Message-ferry-based
In message-ferry-based totally methods, structures typically The greater mobile nodes as ferries for message delivery. The trajectory of these ferries is managed to enhance transport performance with shop-and-bring message forwarding mechanism.

B. Opportunity-based totally
In possibility-based totally schemes, nodes forward messages randomly hop through hop with the expectation of eventual delivery, however without a guarantees. Generally, messages are exchanged only whilst nodes meet on the equal area, and more than one copies of the equal message are flooded in the network to increase the chance of transport.

C. Prediction-based totally
In prediction-based schemes, routing protocols make relay selection with the aid of estimating metrics relative to a hit delivery, inclusive of transport opportunity or expected delay based totally on a history of observations.

Characteristics Message	**Ferry-based**	**Opportunity-based**	**Prediction based**
Forwarding method	Reactive/Proactive	Flooding	Proactive
Node Types	Heterogeneous	Homogeneous	Homogeneous
Mobility	Controlled	Random	Semi-random
Delay	Highest	Lowest	Moderate
Message Duplication	Upon ferry encounter	Every node encounter	Neighbours that meet Criteria
Energy Consumption	Lowest	Highest	Moderate
Retain Encounter Information Partially		No	Yes
Use of location Information	Yes	No	No

Complexity	Moderate	Simple	Highest

III. DTN ROUTING PROTOCOLS

In this paper, we don't forget Epidemic, PROPHET and Spray-and-Wait DTN routing protocols and we in brief describe them under.

A. Epidemic Routing Protocol

Epidemic routing protocol [6] is one of the first routing protocols that come to be proposed for DTN. That can be one motive why it is easy and clean to enforce. In Epidemic routing protocol, a node forwards a replica of a message to all nodes it encounters, as a result the call Epidemic. A node will not receive the message if it has the message already in its buffer. Eventually all nodes will have the same message. The protocol provides the optimum delivery time however the consumption of nodes resources along with reminiscence and network sources including bandwidth are inefficient. So in order to improve the efficient use of resources and delivery probability the following two protocols were proposed.

B. PRoPHET Routing Protocol

In order to enhance the delivery chance of messages and decrease the network and node assets, Lindgren et al. Proposed PRoPHET routing protocol [7, 8]. The basic idea of PRoPHET is that a cell node does not flow randomly, as a substitute it has repeated movement styles, i.e. It tends to pass thru some places more regularly than others and more likely meet the nodes it has met within the beyond again. Therefore if a node X encounters a node Y regularly, node Y has higher delivery opportunity for messages of node X. So when node X encounters node Y and a few other nodes which it has not met earlier than it's going to a head messages to Y instead of different nodes. Unlike Epidemic routing protocol, in PRoPHET routing protocol, a node forwards messages simplest to some better transport possibility nodes, not all nodes it encounters therefore saves resources.

PROPHET establishes a summary vector that indicates what messages a node are carrying. Furthermore establishes a probabilistic metric called delivery predictability, P (a, b) (0, 1), at each node a for every known destination b. It is signify how likely it is that this node will be capable to deliver a message to that destination. The computation of the delivery predictabilities has three parts. First, whenever a node is encountered, the metric is updated as Equation. a, where P in it is an initialization constant. P [a,b]old = P[a, b]old + [1 – P[a,b]old] *P init (a) Second, if a pair of nodes do not encounter each other in a while, they are less likely to be good forwards of messages to each other, thus the delivery predictability values must age.

C. Spray-and-Wait Routing Protocol

Spray-and-Wait routing protocol controls the spreading of messages within the network. Unlike PROPHET routing but like Epidemic routing, it has no previous knowledge of encountering nodes and certainly forwards a couple of copies of messages to nodes it encounters. The foremost distinction with Epidemic routing is that it spreads only L copies of message. The protocol has two levels: (i) Spray segment: a supply node spreads a limited range of copies (L) of message to nodes which it encounters. (ii) Wait section: after spreading of all copies of the message is achieved and the destination node isn't always encountered through the source node, each node with the duplicate of the message inside the unfold section, tries to deliver its own reproduction to the destination node through direct transmission.

In order to enhance the overall performance of the set of rules, authors have proposed binary Spray-and-Wait protocol. In this protocol, a source node prepares L copies of message and transmits 1/2 of it to a node it encounters first. The source node and other nodes that have copies of the message,

transmit half of of the message to nodes they encounter and do now not have the message. The manner is repeated until most effective one reproduction of the message is left. When only one reproduction is left, nodes with the copy of the message will try to deliver it to vacation spot node thru direct transmission. Here, we use binary Spray-and-Wait
protocol with L = 6.

IV. DTN APPLICATION

A. Inter-planet satellite communique networks: The objective of the interplanetary Internet turned into to outline the structure and protocols for Interoperation of the internet resident on earth with over remotely positioned residents on different planets or spacecrafts. The Earth's Internet is largely a community of interconnected networks. This network is may consequently be therefore be thought of as a network of disconnected Internets.[18]

B. Space mobile ad hoc networks:
This network may additionally have intermittent connection due to mobility or area deployment. [18]. At times sporadic connectivity inside the network could be periodic or predictable [18].

C. Country- side area networks: DTN can carry digital connectivity to rural areas and other environments with restricted or no present infrastructures. The eventualities transportation system which includes cars, buses and boats are used to offer relaying of messages through shifting round and handing over message to various nodes.

D. Military battlefield networks: In a military setting DTN allows for a wealthy set of packages along with dissemination of assignment-crucial statistics in battlefields. These form of programs, the delay tolerant protocol must transmit messages across multi-hop network consists of various solar networks based totally on network parameters inclusive of delay and loss[18,19].

E. WSN: Wireless sensor networks are regularly characterized via confined quit-node assets consisting of power, reminiscence and CPU power. Communication within these networks is often aimed toward limited usage of this useful resource. Lack of infrastructure might also force sensor community gateways to be intermittently linked to operator's network. Scheduled down time, interference, or environmental hostility may also purpose the interruption of operable conversation links. [20]

F. Exotic media Networks: Exotic conversation media consists of near earth satellite communications, very long distance radio links, acoustic transmission in air or water, free areas communications and networks[21].

V. LITERATURE SURVEY

Bhed Bahadur Bista, et.al. [2] In a DTN, nodes are intermittently related. In order to deliver a message from a source node to a destination node, the message is copied and forwarded to an intermediate node when the connection between the nodes is established. The node that receives the message stores it and forwards the copy of it to another node it encounters. The process is repeated until the destination node is encountered or the message's life time expires. PROPHET is one of the essential DTN routing protocols. However, PRoPHET does not consider energy consumption of nodes. Energy consumption of mobile wireless devices has been a major issue recently as the devices are ubiquitously used. In this paper, we propose an Energy Aware PRoPHET that considers energy of nodes and available free buffer of nodes for storing forwarded messages. We extensively simulated our proposal and have shown that our proposed routing performs far better than PRoPHET in terms of energy consumption, extension of network existence, message delivery chance and overhead ratio.

In this paper, for secure routing optimization we are introducing dynamic trust control protocol in records centric network and DTN environments. In the existing system, dynamic trust control for

DTN is used to address the detection of the selfish, malicious misbehaving nodes and authentic loss nodes. To disrupt DTN operations, malicious nodes performing accept as true with-related attacks. Human conveying message gadgets in a DTN are communally egotistic to outsiders but altruistic to friends. The proposed system is designed to identify the malicious node and selfish node based on checking the node energy level and buffer level using multi-hop forwarding algorithm. But it's time consuming method. In the Proposed System, we put into effect ICN for validating the node data primarily based on payoff calculation of node. It gives security and much less time consumption. Before statistics transmission, ICN identifies the malicious node and selfish node based totally on Repetitive Trust Management and Adversary Detection scheme. But it is time eating procedure. In the Proposed System, we put into effect ICN for validating the node history based on payoff calculation of node. It gives safety and less time intake. Before facts transmission, ICN identifies the malicious node and selfish node based totally on Repetitive Trust Management and Adversary Detection scheme.

Bhed Bahadur Bista, et.Al. [4] The technique is repeated until the destination node is encountered or message life time expires. PRoPHET (Probabilistic Routing Protocol Using History of Encounters and Transitivity) is one of the main DTN routing protocols. However, PRoPHET does not consider energy consumption of nodes. Energy consumption of mobile wireless devices has been a major issue recently as the devices are ubiquitously used. In this paper, we advise an Enhanced PRoPHET routing protocol that considers power of nodes. We extensively simulated our proposal and have shown that our proposed protocol performs better than the original PRoPHET routing protocol in terms of energy consumption, message delivery probability and overhead ratio.

Yue Zhang, et.al. [5] In this paper, primarily based on the prevailing routing protocol, congestion control mechanism, energy -saving mechanism in the mobile DTN, we propose congestion control balancing strategy with the consideration of the energy constraint. We take remaining cache and energy of nodes as a basis, and the nodes in the network are divided into different levels after the node receives the request of messages. For such a purpose, the proposed approach firstly checks the rank status at the mobile devices. It then adopts different strategies depending on the different levels. If the level is on the verge of congestion, it will take the packet dropping strategy. If the node is in a lower energy level, it will take the method of delaying receiving messages, and if the congestion leve l and energy level are at a low state, the node stops to receive messages. This method allows nodes that congestion level and energy level is lower to prioritized participate in the routing, so that controls network congestion and balances energy in the network. Simulation results show that the proposed algorithm improves the network congestion within the equal network surroundings and extends the life of the complete network.

Pham Thi Ngoc Diep, [6] advanced to cope with intermittent connectivity and long delay in wireless networks. Due to the restricted connectivity, DTN is vulnerable to blackhole and greyhole attacks in which malicious nodes intentionally drop all or part of the received messages. Although present proposals ought to as it should be come across the attack launched by people, they fail to address the case that malicious nodes cooperate with every different to cheat the protection machine. In this paper, we propose a scheme referred to as Statistical-primarily based Detection of Blackhole and Greyhole attackers (SDBG) to cope with each individual and collusion attacks. Nodes are required to alternate their encounter file histories, based totally on which other nodes can examine their forwarding behaviors. To come across the individual misbehavior, we outline forwarding ratio metrics which could distinguish the behavious of attackers from ordinary nodes. Malicious nodes might keep away from being detected by means of colluding to control their forwarding ratio metrics. To continuously drop messages and sell the metrics on the equal time, attackers need to create fake come upon data often and with high forged numbers of sent messages. We exploit the bizarre sample of appearance frequency and wide variety of despatched messages in fake encounters to layout a robust set of rules to detect colluding attackers. Extensive simulation suggests that our answer can works with various losing chances and distinctive wide variety of attackers in step with collusion at high accuracy and low false positive.

El arbi abdellaoui alaoui [2015] et al present that, there are an amount of circumstances the place availability is irregular, and a given goal is usually not reachable right now a message is sent. Networks with these attributes are known as DTN. The NECTAR protocol proposed listed here is established on the contacts historical past with a purpose to create a regional Index and then assess the most appropriated route for DTNs. Simulations carried out with real knowledge retrieved from mobile and wireless environments at Dartmouth university in scenarios the place the incidence of totally Partitioned networks is frequent, and with the presence of resource restrained nodes show that NECTAR is ready to provide extra
messages than Epidemic and PROPHET protocols with lower consumption of network resources [7].

Sapna Grover [2014] et al present that, the development of routing protocols for irregularly associated ad hoc networks and discusses about the pattern toward social-based routing protocols. A review of present routing arrangements is introduced, where routing protocols for crafty networks are named set up on the network diagram utilized. They have to seize performance tradeoffs from a multi- objective viewpoint is highlighted [8].

Bunty Badgujar [2014] et al present that, Disruption Tolerant architecture, DTN is intended to outfit connectivity in Heterogeneous networks which need unremitting connectivity due to interruptions or giant delays like that of networks operating in mobile or extreme terrestrial situations or arranged network in space. The internet protocols fail to operate safely inside the context of ICNs (Intermittently connected Networks), accordingly elevating a type of contemporary difficult disorders which are attracting the attention of the networking research community. Delay-/DTN emerged as a incredibly energetic subject of research the place networking gurus compete in addressing the various ICN issues. The DTN successfully enhances network communications the place the network connectivity is Periodic/Intermittent as well as inclined to disruptions. The Store and Forward technique thru the Bundle Protocol (BP) of the DTN helps the go with the flow of data /statistics throughout any complicated or intermittent network visitors. The applications of simple erasure based codes to messages have been considered. [9].

B.Shubashini [2014] et al present that, The delay tolerant networks (DTN), which form the mobile and wireless ad hoc networks, are characterized by intermittent connectivity, asymmetric flow, high error rate and lengthy or variable delivery time, specially whilst the destination isn't within the equal area because the source. The cause of this paper is to examine two classes (flooding strategy and forwarding strategy) established on two-pronged strategy, mainly the replication strategy that refers to the following protocols: Epidemic, Spray and Wait. The expedition strategy associated with the following protocols: Prophet and Max-Prop. Moreover, our contribution is situated on a combination of routing protocols DTNs and the mannequin of bundle layer end-to-end retransmission (BLER) to enhance routing in DTN networks and operating nodes that enable the distribution of information between the shared networks. This study is performed on our simulator programmed in java centered on Opportunistic Network Environment simulator (ONE) so as to evaluate the performance of routing protocols DTN. The results of the evaluation exhibit that the performance of distinctive protocols can benefit from optimizing the efficiency of DTN in terms of the delivery probability, ordinary latency and overhead rates [10].

Vrunda Gamit [2014] et al present that, Delay Tolerant Networking (DTN) data can switch in difficult environments the place a fully linked finish to finish path may additionally without a doubt now not exist among a source and destination. These networks manage substantial transmission delays, regularly disconnected paths, high connection and way error and limited resources. Modern Internet protocols reveal inefficient efficiency in these networks the place the connectivity between finish nodes has intermittent property as a result of Dynamic topology much like MANET or VANET. Network environment the areas the nodes are characterized with the support of opportunistic connectivity are known as DTN. [11].

Mary R. Schurgot [2012] et al present that, Delay Tolerant Network (DTN) is detailed type of wireless MANET characterized through intermittent connectivity, long or variable delay, uneven data and high error rates. In this paper we evaluate a few of well-known routing protocols namely Max-Prop, Epidemic, Spray and Wait, Prophet and First Contact. On this paper we've got analyzed protocols on the basis Transmission variety and Buffer dimension of nodes. We examined the behavior of protocols in two different scenarios firstly with constant transmission range & varying buffer size, second with constant buffer size & varying transmission Range. Simulation results shows that supply ratio with steady transmission range is virtually equal for all routing protocols and supply ratio with regular buffer measurement is highest in Max-Prop protocol. [12].

TABLE I. COMPARISION TABLE

Sr. no	System proposed	Advantage	Disadvantage
1	CP-ABE process [13]	Secure against collusion attack	Safety debasement in day and age of in reverse and ahead mystery.
2	Decentralized CP-ABE process [14]	Flexible exceptional-grained entry manipulates.	Effectivity and expressiveness of entry policy.
3	Max-prop: Routing Method [15]	Propose a DTN routing protocol, called Max-Prop that performs significantly better than previous approaches.	Load is increased
4	Plutus: Novel Method [16]	Proposed methodology is more secure and productive.	With overhead comparable to frameworks that scramble all network traffic
5	Distributed KP-ABE Method[17]	It enables more realistic deployment of attribute based access control.	Performance degradation.
6	Performance analysis of content headquartered knowledge retrieval system [18]	Proposed procedure achieved smaller question response time and consequently obtain bigger query success rate.	The question load increments with the end goal that there is a cradle flood of put away inquiries, and afterward the question achievement rate will drop.

7	MCP-ABE Method [19]	Instantaneous attribute revocation.	No way to revoke an attribute before the expiration date.
8	ABE Method [20]	Performance better than existing system.	Less Expressive method.
9	KP-ABE Method [21]	Efficient sharing of encrypted data.	Selectively shared most effective at a coarse-grained stage.

Conclusion

Delay Tolerant Networks (DTN) are a class of networks that lack continuous connectivity between nodes due to limited wireless radio coverage, widely scattered mobile nodes, controlled energy resources, high levels of interference or due to some other related channel impairment. DTN required to store messages in non-unstable memory whilst reliable delivery is required. DTN is a proposed protocol standard which lets in interoperability between unique and challenged networks with an easy to apply API. In this paper, we mentioned various routing protocols with their description and the applications on delay tolerant network discussed.

References

[1] S. Farrell and V. Cahill, "Delay and Disruption Tolerant Networking," Artech House, ISBN:1596930632, Artech House, Inc. Norwood, MA, USA ©2006.

[2] Bhed Bahadur Bista, Danda B. Rawat, EA-PRoPHET: An Energy Aware PRoPHET-Based Routing Protocol for Delay Tolerant Networks, IEEE 31st International Conference on Advanced Information Networking and Applications. 1550-445X/17 $31.00 © 2017 IEEE.

[3] M. Malathi, S. Jayashri, "Design and Performance of Dynamic Trust Management for Secure Routing Protocol". 2016 IEEE International Conference on Advances in Computer Applications (ICACA). 978-1-5090-3770-4/16/$31.00©2016 IEEE

[4] Bhed Bahadur Bista, Danda B. Rawat, "Enhancement of PRoPHET Routing in Delay Tolerant Networks from an Energy Prospective", Region 10 Conference (TENCON) — Proceedings of the International Conference, 978-1-5090-2597-8/16/$31.00 c 2016 IEEE

[5] Yue Zhang, Xiangyu Bai, Na Dang, Junli She, Zhichao Song, "Congestion Control Balancing Mechanism Based on Energy-Constraint in Mobile Delay Tolerant Network". 2016 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery. 978-1-5090-5154-0/16 $31.00 © 2016 IEEE

[6] Pham Thi Ngoc Diep, Chai Kiat Yeo, "Detecting Colluding Blackhole and Greyhole Attacks in Delay Tolerant Networks". 1536-1233 (c) 2015 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information

[7] Said, Agoujil & Abdellaoui Alaoui, El Arbi & Moha, Hajar & Qaraai, Youssef. (2015). The Performance of DTN Routing Protocols: A Comparative Study. WSEAS Transactions on Communications. 14. 121-130.

[8] Sapna Grover, Aditya Panchol and Sonika Arora," FSR: Ferry-based Secure Routing Algorithm for Delay Tolerant Networks", International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 3 Issue 5 may, 2014 Page No. 6104-6108.

[9] Bunty Badgujar, Manpreet Kandara & Yash Dotania and Ms Preeti Nagrath," Analysing impact of range and storage constraints on various routing protocols in Delay Tolerant Networks To choose the best

routing protocol in the context of delivery probability, overhead ratio & average latency", IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501Vol.4, No.6, December 2014, pp: 376-379

[10] B.Shubashini and Dr.Antony Selvadoss Thanamani," An Opportunistic On Routing Protocols and Persisting Challenges in Delay-Tolerant

Networking", International Journal of Innovative Research in Computer and Communication Engineering Vol. 2, Issue 8, August 2014, pp: 5373-5379

[11] Vrunda Gamit and Mr. Hardik Patel," Evaluation of DTN Routing Protocols", international journal of engineering sciences & research technology, [Gamit, 3(2): February, 2014], pp: [588-592].

[12] Mary R. Schurgot and Cristina Comaniciu, "Beyond Traditional DTN Routing: Social Networks for Opportunistic Communication", IEEE Communications Magazine, 0163-6804/12/$25.00 © 2012 IEEE.

[13] J. Bethencourt, A. Sahai, and B. Waters,"Ciphertext-policy attribute based encryption," in Proc. IEEE Symp. Security Privacy, 2007,pp.321–334.

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

[15] 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.

[16] 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.

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

[18] 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.

[19] 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.

[20] 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.

[21] 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.