International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 6 | ISSN : 2456-3307

Efficient Parallel key management for Distributed Data Security in Content Delivery Networks

SK.Ahmad Shah[*1], Dr. Penmesta V Krishna Raja[2]

Assistant Professor, Department of IT, Aditya College of Engineering & Technology, Surampalem, Kakinada, East Godavari, Andhra Pradesh, India

Principal & Professor, Kakinada Institute of Engineering and Technology, Kakinada, East Godavari, Andhra Pradesh, India

ABSTRACT

Technology and its significant has changed the way of the time being lead to next level of journey to make classical technology to the ultra modern technology. Time being is called as the data to be secured with the node based cloud cluster mechanism. In this paper, we have the glimpse of the technology and its Significance may be loop based hole to imagine world, but in the terms of Reality really it's a wonder, where we think ability the more and more to explore things may be technology to give a seam less service the mankind. If we consider the networking where we made this ethereal world to a global village making things better, but there is no end of better. If we consider the parallel distributed network, where these days we face the difficulty in transferring the data, in turn we callas load balancing along with some other factors may also come. Hence, in this paper we try to give the glimpse of the best mechanism which involves the load balancing in Content Delivery Networks in the discrete acknowledge based dynamic method. We have taken consideration of the access control based approach where data sharing would base on the group based specific and acknowledgment based approach to implement the best cryptographic approach. In order to secure the best of the privacy we have implemented the dynamic group based encryption and decryption mechanism to some authorized group based on the clustered node where attribute based acknowledgement in the private share delivery networks.

Keywords : Access control, attribute-based encryption ABE, disruption-tolerant network (DTN), multi-authority, secure data retrieval.

I. INTRODUCTION

A novel class of wireless networks introduced as Vehicular Ad hoc Networks is presented in this research. In the network of topologies of moving vehicles used in similar and different radio interface technologies and equipped with wireless interfaces that use short-range to medium-range communication systems. One of the classes of the mobile ad hoc networks is a that facilitates communication between vehicles by using close stable equipment on a roadside when vehicles are surrounded by other vehicles. In the field of Vehicular Ad hoc Networks, new developments are strongly encouraged for industries that involve automotive and wireless technology. Firstly, we give an overview of the protocol, discussing the key points of its design. Secondly, analyze the prediction theory and algorithms at the basis of this. Thirdly, we discuss its implementation, focusing on the management of routing information for synchronous and asynchronous delivery. Finally, we present the design and implementation of a component for evaluating the predictability of the time series used to describe and Measure aspects of the mobile context. Firstly, we give an overview of the protocol, discussing the key points of its design. Secondly, we analyze the prediction theory and algorithms at the basis of this. Thirdly, we discuss its implementation, focusing on the management of routing information for synchronous and asynchronous delivery.

Finally, we present the design and implementation of a component for evaluating the predictability of the time series used to describe and measure aspects of the mobile context. DTN Geographic routings have been used in situations where there is no connectivity between vehicles in . This normally happens in sparse traffic environments. Unlike traditional ad hoc networks, the end-to-end path between a source and destination will only be available for a short and unpredictable period of time. In a DTN, the mobile node keeps a packet until it finds an opportunity to send it to the destination and when there is no connectivity between nodes, the data will be stored in the buffer. When a neighbor appears within the transmission range of the mobile node, the data in the buffer would be forwarded to that neighbor. However, in non DTN geographic routings, it is assumed that vehicles in a network have end-to-end connectivity.

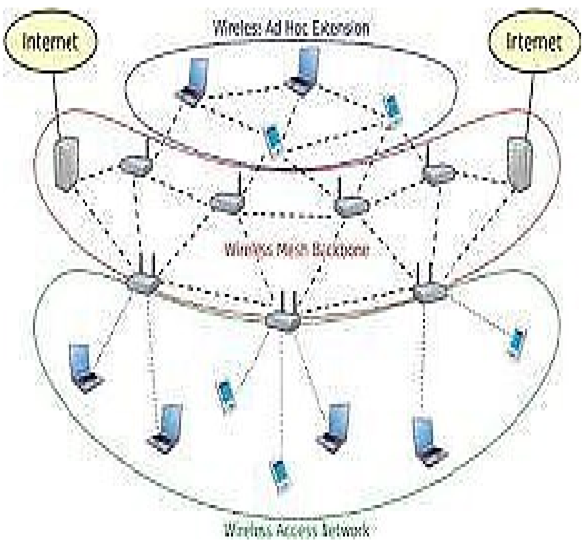

Fig. 1.1. Sample View of the Delay Routing Network

II. RELATED WORK

In the context of the related and find the Data delivery in Delay-Tolerant Networks (DTN) is quite challenging since end-to-end paths may never exist. However, data can be opportunistically forwarded via nodes that had contacts with the destination or that belong to the same group of the destination. In a world where devices are becoming very powerful in terms of processing and storage, it is expected that human-carried devices may become part of DTNs, also known as Pocket-Switched Networks (PSN). In PSNs, forwarding may be done opportunistically based on the mobility behavior of humans. However, the efficiency of PSNs may deeply depend on the accuracy of mobility prediction. The current routing trend is to consider human behavior regarding social relationships where a social-aware approach to opportunistic routing in DTNs may present higher efficiency, since human relationships are less volatile than human mobility. In addition, this latest routing trend is also taking into account interest of users to help forwarding. Another aspect that can also be considered is the existing legacy infrastructure that can have an important role in routing information. The technology advancement of the network delay and pocket delivery where we put the concept of the classical technology.

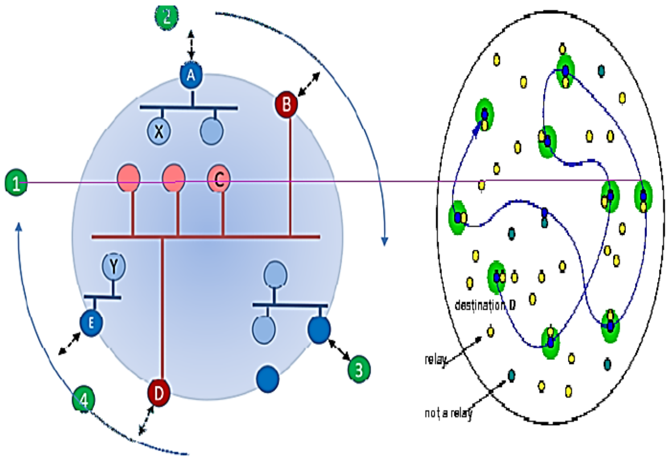

Fig. 2.1 Related View of the Delay Network in the Path of the Node

Networks in which nodes communicate occasionally, depending on contact opportunities are known as intermittently connected networks. This occasional communication may be the result of mobility of nodes where links between these nodes become unavailable due to obstacles or even distance. Independently of the used approach, one can notice that the level of social relationship used by forwarding and replication solutions can vary from simple encounters between nodes up to defining number of contacts and contact duration in order to determine the social ties, but they all aim to improve routing on DTNs.

III. PROPOSED METHODOLOGY

In the technology of the advancement and the dense networks are created by people moving around, opportunistic contacts were considered to increase delivery probability in networks with the aforementioned characteristics in a proposal called Epidemic. With an Epidemic routing approach every node in the network gets at least a copy of each message. Such a full replication strategy leads to an increase of the delivery rate. Replication of messages is done by means of summary vectors that are exchanged between any two encounters. Such summary vectors contain the list of messages each node is carrying, allowing nodes to exchange all messages that the other node is lacking. The proposal indeed increases delivery rate, since every potential forwarder has, with high probability, a copy of the message, assuming contacts with significant duration and sufficient buffer space in each node. However, to avoid a big waste of resources, each host sets a maximum buffer size that it is willing to allocate for epidemic message distribution. In general, nodes drop older messages in favor of newer ones upon reaching their buffer's capacity. This means that the efficiency of the delivery process depends upon the configured buffer space, which may be substantially improved with the usage of Bloom filters. In order to avoid messages to be replicated indefinitely, a hop count field determines the maximum number of epidemic exchanges that a particular message is subject to, being packets dropped based on the locally available buffer space. Since the number of hops towards the destination is not known in advance setting a hop count may decrease the delivery probability. A stale-data removal mechanism could be more efficient by removing messages that were already delivered.

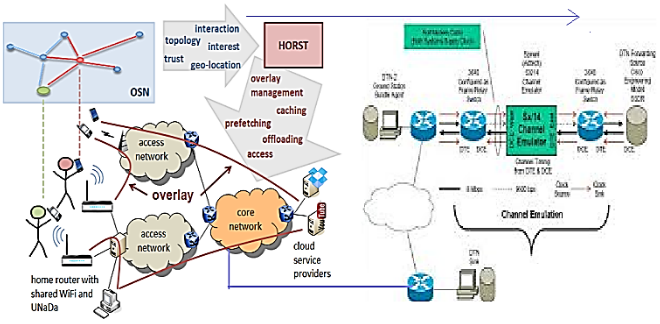

Fig.3.1. Architecture Design view of the Framework in the Overlay

Within this category, proposals attempt, First of all, to optimize the delivery probability while avoiding full replication of messages. Besides this core concern, there are proposals that take into account the capabilities of nodes, the priority of messages and the availability of resources aiming to achieve a high delivery ratio with low delay and resource consumption. Another concerns of some probabilistic-based approaches is to use as few meta-data as possible aiming to decrease concerns with respect to energy, processing and bandwidth saving. Having considerable control overhead increases contention in the network resulting in message discarding and retransmissions. Such link unavailability can also result from power-constrained nodes which must save power thus shut down their wireless cards. The reason for this is that social behavior takes into account human relationship characteristics such as contacts with other people, time spent with these people, and the level of relationship between people. And since computing devices are carried by humans, social-based forwarding decisions can consider people's socially meaningful relationships where the relationship information come from aspects such as human mobility, interaction, and social structures. This information can be used to perform forwarding, because the topology created from human social behavior varies less than the one based on mobility

IV. EVALUATION AND ANALYSIS

The cost for a path is the sum of the probability of each contact on the path not occurring. This cost estimation, along with the hop count, is then used to order messages for scheduling and for dropping. In addition, We assigns a higher priority to new messages (i.e., low hop count) to increase their chance of reaching the destination faster, and tries to prevent reception of the same message twice by including a hop list in each message, and uses acknowledgments to notify all nodes about message delivery.

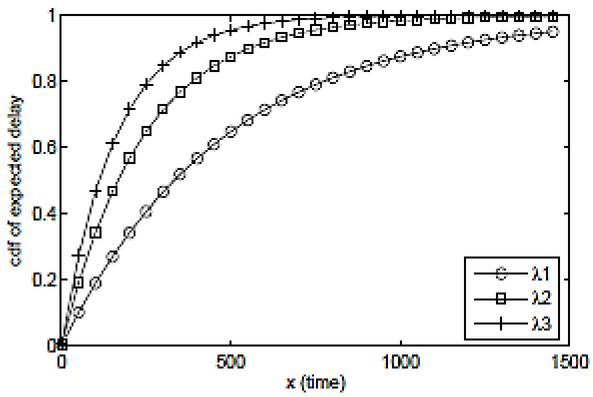

Fig.4.1 Comparison View of the Model View Framework with Time and Delay

Upon contact, two nodes exchange messages in a specific priority order: First, messages that have these nodes as Final destinations; second, information for estimating delivery likelihood; third, acknowledgments to remove stale messages; fourth, messages that have not traversed far in the network; and, fifth, send messages with highest priority.

V. CONCLUSION AND FUTURE WORK

It is important to mention that the delivery likelihood metric used in is different from the delivery predictability metric in the sense that the former depends solely on the probability of nodes to meet each other while in it depends on the probability to meet the destination itself, which means that requires more state. However, It requires nodes to compute possible paths to the destination by concatenation of delivery probability between nodes while does not require further computation. If the destination of a message is not the node in contact, the probability to deliver such message through that node is computed. If the probability of delivering the message via the contact node (based on the past average number of encounters with the destination) within a defined period of time is greater than or equal to a certain threshold, the message is passed to the node in contact. This proposal presents two methods for choosing the next node: the decision can be taken by the node that is sending the message or by the one which is receiving it. In the former case, a meta-data message is necessary to determine if the receiver is a good next hop. As for the latter, the receiver decides whether or not to keep the copy of the message considering its own probability of coming into contact with the destination.

VI. REFERENCES

[1]. A. Doria, M. Uden, and D. P. Pandey, Providing connectivity to the saaminomadic community, in Proceedings of the 2nd International Conference onOpen Collaborative Design for Sustainable Innovation (dyd 02), Bangalore, India, Dec 2002.

[2]. A. Pentland, R. Fletcher, and A. A. Hasson, A road to universal broadband connectivity, in Proceedings of the 2nd International Conference on Open Collaborative Design for Sustainable Innovation (dyd 02), Bangalore, India, Dec 2002.

[3]. G. E. Prescott, S. A. Smith, and K. Moe, Real-time information system technology challenges for NASAs earth science enterprise, in Proceedings of The 20th IEEE Real-Time Systems Symposium, Phoenix, Arizona, Dec 1999.

[4]. P. Juang, H. Oki, Y. Wang, M. Martonosi, L. S. Peh, and D. Rubenstein, Energy-efficient computing for wildlife tracking: design tradeoffs and early experiences with zebranet, in Proceedings of ACM ASPLOS, 2002.

[5]. Disruption tolerant networking, http://www.darpa.mil/ato/solicit/DTN/.

[6]. J. Ott and D. Kutscher, A disconnection-tolerant transport for drive-thruinternet environments, in Proceedings of IEEE INFOCOM, 2005.

[7]. G. W. Boehlert, D. P. Costa, D. E. Crocker, P. Green, T. OBrien, S. Levitus, and B. J. Le Boeuf, Autonomous pinniped environmental samplers; using instrumented animals as oceanographic data collectors, Journal of Atmospheric and Oceanic Technology, vol. 18, no. 11, pp. 18821893, 2001, 18 (11).

[8]. T. Small and Z. Haas, The shared wireless infostation model - a new ad hoc networking paradigm (or where there is a whale, there is a way), in Proceedings of The Fourth ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc 2003), June 2003, pp. 233244.

[9]. K. Fall, A Delay-Tolerant Network Architecture for Challenged Internets, SIGCOMM, August 2003.

[10]. A. Beaufour, M. Leopold, and P. Bonnet, Smart-tag based data dissemination, in First ACM International Workshop on Wireless Sensor Networks and Applications (WSNA02), June 2002.

[11]. A. Demers, D. Greene, C. Hauser, W. Irish, J. Larson, S. Shenker, H. Sturgis, D. Swinehart, and D. Terry, Epidemic algorithms for replicated database maintenance, in Proceedings of the ACM Symposium on Principles of Distributed Computing, 1987, pp. 112.

[12]. W. Vogels, R. V. Renesse, and K. Birman, The power of epidemics: Robust communication for large-scale distributed systems, In Proceedings of HotNets-I'02: First Workshop on Hot Topics in Networks, special issue of the ACMSIGCOMM Computer Communication Review, Princeton, NJ. October 2002.

[13]. Delay tolerant networking research group, http://www.dtnrg.org.

[14]. P. Zhang, C. M. Sadler, S. A. Lyon, and M. Martonosi, Hardware design experiences in zebranet, In Proc. ACM SenSys, pages 227238, 2004.

[15]. M. Motani, V. Srinivasan, and P. Nuggehalli, PeopleNet: Engineering a Wireless Virtual Social Network, In Proc. ACM Mobicom, pages 243257, Aug. 2005.

[16]. J. Partan, J. Kurose, and B. N. Levine, A Survey of Practical Issues in Underwater Networks, In Proc. ACM WUWNet, pages 1724, Sept. 2006.

AUTHOR DETAILS:

SK.Ahmad Shah he is working as an Assistant professor in Aditya College of engineering & Technology technology Surampalem, Kakinada, Andhra Pradesh, affiliated to JNTU Kakinada and he completed her M.Tech from University college of Engineering, JNTUK in the year 2012 and obtained her B.Tech Degree from KIET affiliated to JNTU Kakinada, Andhra Pradesh, India in the year 2007. He is interested in the fields of Computer Networking, Mobile Networks, Wireless networks, Ad-hoc sensor networks, Cloud computing, Image processing.

Dr. PenmetsV.Krishna Raja He is currently working as Professor in the department of CSE of Kakinada Institute of engineering Technology, Kakinada. He did his PhD from JNTU, Kakinada. He received his M.Tech (CST) from A.U, Visakhapatnam Andhra Pradesh,India. His research areas include Network Security, Cryptography ,Intrusion Detection, Neural networks, Data Mining and Software Engineering.