International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463
Vol. 3 Issue 2, February-2014, pp: (82-87), Impact Factor: 1.252, Available online at: www.erpublications.com

Dynamic cluster based cache consistency attacks using NDD technique in mobile network

K. Pretheeba[1], Mr. R. Manivannan[2]
[1]Department of CSE, E. G. S. Pillay Engineering College, Tamilnadu, India
[2]Assistant professor, Department of CSE, E.G.S Pillay Engineering College, Tamilnadu, India

Abstract: In mobile environment have using Caching is an essential mechanism. Mobile node makes access dynamic changing data object to their server and to get the interested data to keep their own as local copies in the cache. If the centralized server database is updated, the data cached in mobile client is invalidated and it becomes inconsistent between client and server. We have to design the dynamic cluster based caching and neighbor discovery distance techniques in mobile node, this technique improves data accessibility, reduces the query latency and easy to maintains cache consistency in mobile environment. Designed a Dynamic Cluster Based Cache Consistency (DCBCC) used to server and the client using Neighbor Discovery Distance (NDD) technique. Cluster head is selected nearest to the center of the grid and full battery power among other nodes in the mobile environment. Simulation is done on NS2, result show that reduces update delay, reduces Query delay, high throughput, high energy level when compared with existing approaches Distributed Cache Invalidation Method (DCIM).

Keywords: DCBCC, DCIM, AODV, MAC, NDD, OTCL.

1. Introduction

Mobile environment has rigorous limitations in network resources, such as bandwidth and connectivity. Mobile network data are kept in cached at clients to increase performance, data availability. Although a number of studies have been made in this subject, few researchers focused on mobile data access. We design a node as cluster head. A mobile background, when data updated at the server, the client hosts must get the latest updated information otherwise it becomes invalidate their local cache data, if not the host would continue to answer queries with the cached incorrect data.

To reduce power consumption either at node level or on the network in general, all proposed solutions have a kind of trade-off that let go to have clear energy saving. To bring out this performance trade-off, this paper presents, the observed performance metrics based on the simulation results posted by the various algorithms under review. We consider the following as major performance demands for all the protocols: the number of routes established during route discovery, the message overheads the cost of performing the data packet transmission and reception by different nodes, average energy conserved, data packet delivery ratio, the network throughput, the end-to-end data packet delay.

All cache consistency algorithms are developed with the same goal in mind to increase the probability of serving data items from the cache that is identical to those on the server. A large number of such algorithms have been proposed in the literature, and they fall into three groups: server invalidation, client polling, and time to live (TTL). With server invalidation, the server sends a report upon each update to the client. Two examples are the Piggyback server invalidation and the Invalidation report mechanisms.

The cooperative cache adopts a widely accepted system model in which each data object is associated with a single node that can update the source data. Each data object can be a collection of nodes called the caching nodes. The data copies held by the caching nodes are called the cache copies. There are two basic mechanisms for cache consistency maintenance i.e., push and pull. Using push, the data source node informs the caching nodes of data updates. Using pull, the caching node sends a request to the data source node to check the update. In designing cooperative cache the source data updates and the cache queries follow the Poisson Process. The routing protocol employed in the network layer provides the hop count between each pair of nodes, and the hop count of data transmission is used to measure the consistency maintenance.

2. Related work

Mobile Ad hoc Networks (MANET) have been highly vulnerable to attacks due to the dynamic nature of its network infrastructure. Along with these attacks, routing attacks have received extensive attention since it could cause the most devastating damage to MANET Earlier there is binary fuzzy and naïve response decisions is considered. Binary responses may result in the unpredicted network division causing supplementary damages to the network infrastructure, and negative fuzzy responses could lead to ambiguity in countering routing attacks in MANET. To overcome this we move to the proposed system.

The problem of cache consistency maintenance in mobile environment and it has its own drawback. In this study cooperation based database caching system. In this method query delay and bandwidth utilization more. In this approach is middle server between main server and client. But more workload on server queuing model approach reduce the traffic but still more work load on server. In this method is used to reduce the bandwidth requirement, the server transmits in one of the three modes slow.

The server sends data updates to the Cache Node (CN) request Mobile host that desires a data item send its request to its nearest Query Directory (QD). If this QD finds the query in its cache, it forwards the request to the CN caching the items, Otherwise it forward, it to its nearest QD, if the request traverses all QDs without being found, a miss occurs and it gets forwarded to the server which sends the data item to the request mobile host.

Several cache consistency (invalidation) schemes have been proposed in the literature [3], [4] for MANETS. In general, these schemes fall into three types i.e., pull or client model (caching node (CN) asks for updates from server), push or server model, (server sends updates to CN), and cooperative model (CN and server cooperate to keep the data up-to-date). Pull-based strategies achieve smaller query delay times at the cost of higher traffic load, whereas push- based strategies achieve lower traffic load at the cost of larger query delays. Cooperative-based strategies tend to be halfway between both ends.

Recently, many researchers start to look into security issues in ad hoc networks. In addressed the issues of distributing public keys in ad hoc networks, by proposing to let users issue certificates for each other based on their personal acquaintances. A solution based on threshold cryptography. Based on a trusted certificate authority, the authors proposed a solution to secure the routing protocol of ad hoc wireless networks. To address the high overhead associated with obtaining and verifying the digital certificates, in proposed a protocol to secure on-demand routing protocols, an efficient broadcast authentication scheme that requires loose time synchronization.

3. Proposed approach

The enhanced security at the expense of open functionality is particularly appropriate in the context of Mission-critical applications with the potential of an adversarial presence e.g., military Mobile Network. It provided dynamic cluster nodes form, the neighbor discovery distance relationships among themselves in a manner consistent with current policy. However, this initial analysis neglected the possibility of nodes or wireless channel being subverted by a knowledgeable adversary. In mobile network data caching is essential as it reduces contention in the network, increases the probability of nodes getting desired data, and improves system performance. The major issue that faces cache management is the maintenance of data consistency between the client cache and the server.

3.1 Dynamic Cluster on network

Some of the node is grouped as cluster; mobile node data cached is placed in cluster head (coordinator). The cluster head are near to the other node. So the communication cost, energy consumption are very less, easy to update the cache data and easily maintain consistency. If Data requested is not available in local cache, the node agent send the broadcast request to the Dynamic cluster head agent. Dynamic Cluster head agent receive the packet, search in the cache and send the acknowledge data to the node agent. The head satisfy the nearest node request Advantage is low cost for communication and reduces the network traffic in mobile networks.

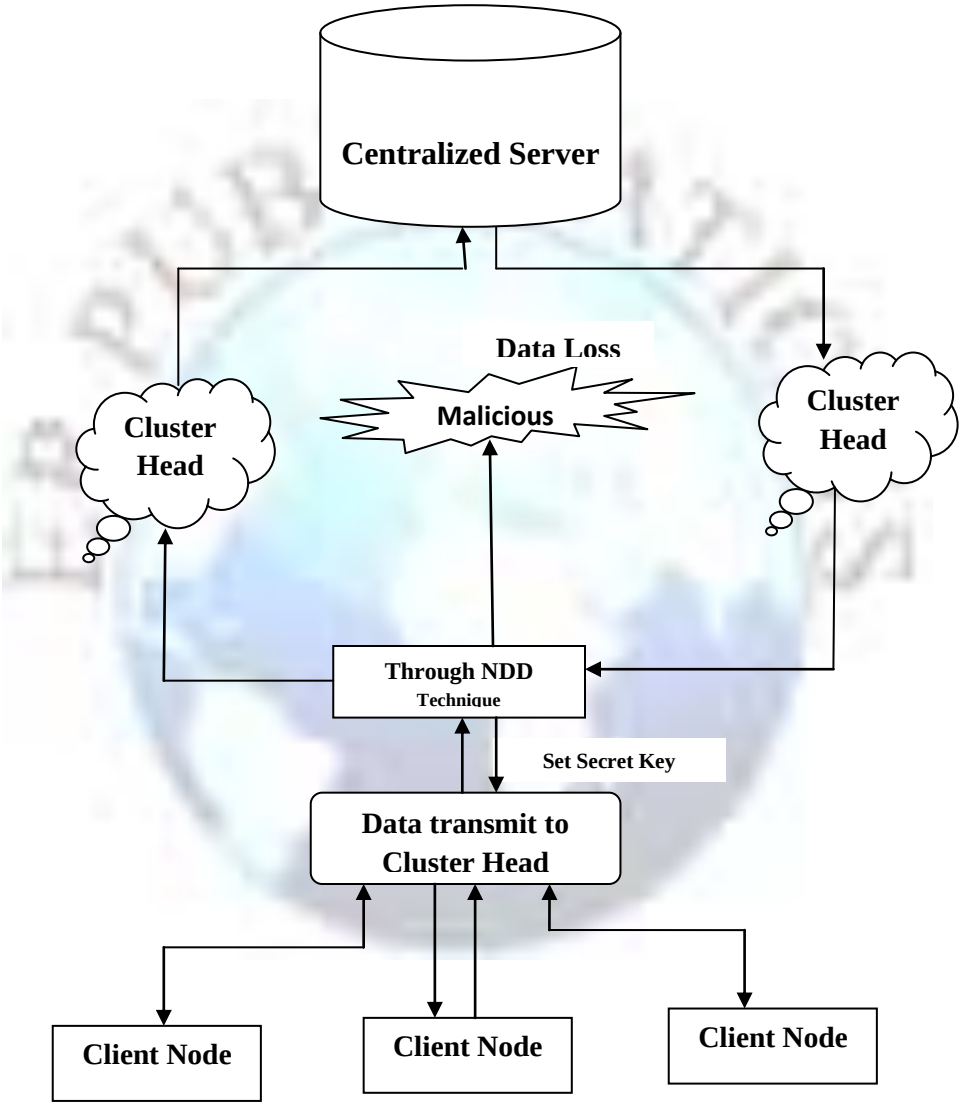
3.2 Neighbor Discovery Distance

In ad hoc network identity like as Neighbor discover distance (NDD) node to watch the transmission on the network. Our proposed system used the NDD Algorithm. Use these algorithms to transfer the data in source to destination without any

damage or loss as well as each node to have the neighbor's node address. Depends on the address the data will be transmitted in to correct destination. If they have any packet loss are some collision on network immediately to inform the server to stop the data and maintaining source node information and header information of message. It checks the users using those details whether they are attackers or normal user.

3.3 Energy Consumption

They used power adaptive broadcasting by reducing the transmission range of mobile nodes to save energy. The range buffer based approach is proposed to further enhance the stability of the forwarding nodes. In NDD techniques determine stable connected dominating set based node velocities. Their algorithm prefers slow moving nodes with lower velocity rather than the usual approach of preferring nodes with a larger number of uncovered neighbors.



3.4 Neighbor discovery techniques and Key distributor

Step 1: The source nodes have the every node key and his address.

Step 2: If source node wish to send data

Step 3: To check the neighbors' node has key means to transfer the data in that node.

Else

Thus not send data**,** again to check the key

Step 4: The node to collect the information and key

Step 5: To checking the all node key, finally to send data means the key will be automatically exchange.

Step 6: Using this key the data will be sending in efficient manner as well as without any loss data.

4. Performance analysis

Aim of our simulation to analyze the performance of the AODV by using meshes Networks. The replication surroundings are produced in NS-2, in that provides maintain for a wireless networks. NS-2 was using C++ language and it has used for an Object Oriented Tool Command Language. It came as an extension of Tool Command Language (TCL). The execution 20 wireless mobile nodes rootless over a simulation area of 1000 meters x 1000 meters level gap in service for 10 seconds of simulation time [8]. The MAC layer models were used. The network based data processing or most expensive and data communication level on their performance on the network. Hence, the simulation experiments do not account for the overhead produced when a multicast members leaves a group. Multiple sources create and end sending packets; each data has a steady size of 512 bytes. Each mobile node to move randomly on their network, it's more and most expectable on their networks.

4.1 Performance results

Experimental simulations are conducted with NS-2 to evaluate the control packet, message delivery rate and end to end delay of the bootstrapping security mechanism applied. The simulation used a random way point model, area 1000 * 1000, maximum velocity 20 m/s, wireless range 250 m, nodes 50, and data transfer rates 4packets/s for our simulation topology scenarios. Each run of the simulator accepts a scenario file as input that describes the exact motion of each node and the exact sequence of packets originated by each

Parameters	Value
version	**Ns-allinone 2.28**
Protocols	**AODV**
Area	**1000m x 1000m**
Broadcast Area	**250 m**
Transfer model	**UDP,CBR**
Data size	**512 bytes**

4.2 Simulation result

4.2.1 Throughput performance

The ratio of throughput performance overall network performance improve network performance and packet delivery ratio and minimize packet delay.

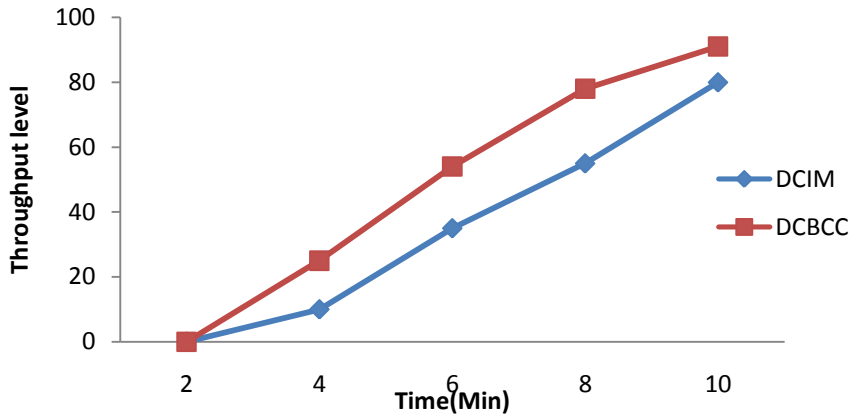


Figure 1: Performance of throughput

4.2.2 The data delivery fraction:

The packets are delivered from source to destination on their network. It is calculated by dividing the number of data received by ending state through the quantity package originated from starting point on network.
PDF = (Pr/Ps)*100
Where Pr is total Data received & Ps is the total data sending on their network.

4.2.3 The Query delay:

It calculate a average number of query delay on network, it includes all possible delay caused by through route detection latency, simulation value shows that the DCIM method is more update delay compare with proposal model DCBCC in varies with number of nodes and query request rate.

$$D = (Tr - Ts)$$

Where Tr is receive Time and Ts is sent Time.

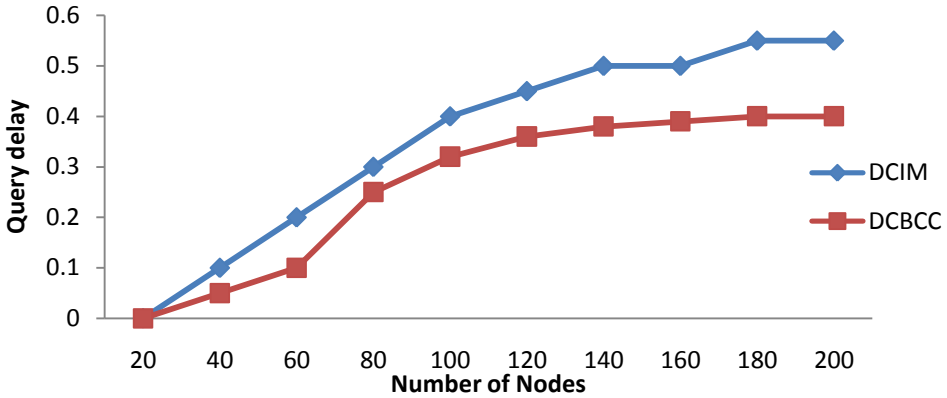


Figure 2: Performance of delay ratio

4.2.4 Energy Consumption:

The energy level on the network is must and most important one of the quick data transmission on their network. its calculated from their each node energy consumption is must of the network. if any node none to data transmit that node to save the energy on the network.

Energy consumption = no of packets * initial energy level

Remained energy = energy consumption – no of packets in node

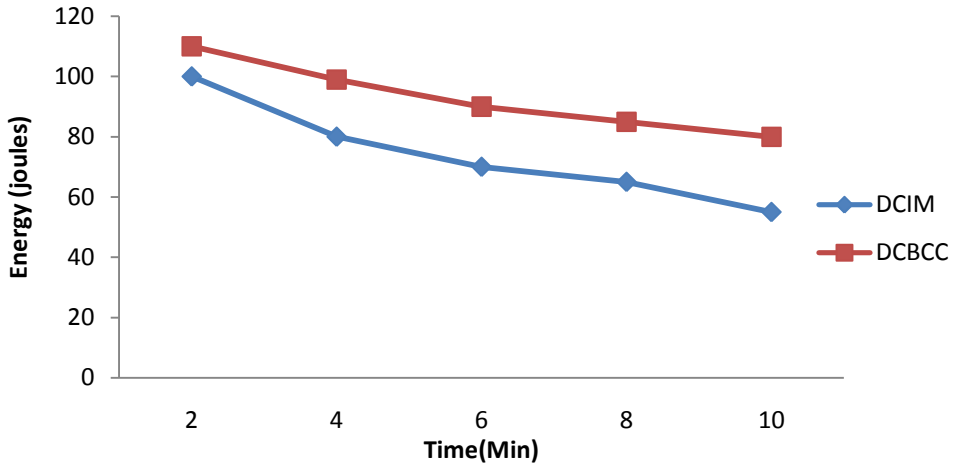


Figure 3: Energy consumption on network

Conclusion

In this study, we proposed a Dynamic cluster Based cache consistency maintenance in mobile environment using Agent Technique (DCBCC), key features as stated earlier are low cost for communication, energy consumption is very low and easy to maintain the cache consistency ,increase the local cache hit ratio, avoiding every request send to server so the network traffic reduces. Simulation results show that may suffer from some security attack in our proposed method used NDD neighbor discovery distance method to improve the network. The experimentation is conducted with NS-2 simulator and showed improved attack resistance rate, false positive rate, Bandwidth and Response time.

References

[1]. Shalini Jain, Dr.Satbir Jain, "Detection and prevention of wormhole attack in mobile adhoc networks", 2010.
[2]. Kimaya Sanzgiri, "A Secure Routing Protocol for Ad Hoc Networks".
[3]. Monika ,"Priority based protocol for different attacks in mobile ad hoc network", 2011.
[4]. Shyaam Sundhar, "Attacks and Countermeasures in Sensor Networks: A Survey".
[5]. Yanhong Li and Le Gruenwald , "A Caching Model for Real-Time Databases in Mobile Ad-Hoc Networks".
[6]. Peter H. Yu and Udo W. Pooch. "Security and Dynamic Encryption System in Mobile Ad-Hoc Network".
[7]. Sarvesh Tanwar, Prema, "Threats & Security Issues in Ad hoc network: A Survey Report", 2013.
[8]. Nithya preya, "Feasible mechanism for boosting the data Access by push based consistency & Efficient replication technique in manet", 2013.
[9]. K.P.Manikandan, "A Survey on Attacks and Defense Metrics of Routing Mechanism in Mobile Ad hoc Networks", 2011.
[10]. Yih-Chun Hu, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols".