Maintaining Security In Wirless Mobile Networks

Sudhakar. D[1]
Vanusha. D[2]
[1]M.Tech Department of Computer Science & Engineering
SRM University
[2] Assistant Professor Department of Computer Science & Engineering
SRM University
Chennai -603 203

***Abstract* -The trend toward wireless communications and advances in mobile technologies are increasingconsumer demand for ubiquitous access to Internet-based information and services. However, due to battery power limitations, users often must disconnect mobile devices from the networkto conserve energy. Moreover, wireless links have lower capacity than wired links and wireless channels are less stable, resulting in higher network congestion and packet loss. These challenges make mobile communication unreliable; emphasizing the need for efficient information-access mechanisms so, in this paper of the proposed work is fully client side approach using Time-to-Live (TTL) and achieving superior availability, delay and traffic performance. Then we create the security server for the purpose of stores all the ids of the mobile users.Whenever the client gives the request to the Query DB, It redirects to the security server (SS) andit checks the id of the requested node. If it is authenticated node, the request passes to Query DB (QDB) to get the data. Second we reduces the data loss while transferring the data items update to the Primary Storage Node (PSN), so to improve the security in the network we are proposing RSA algorithm for message encryption as well as decryption.**

Keywords: Ttl, Rsa, Psn,Qdb, Encryption, Decryption

I. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) consist self governing MNs (Mobile Nodes) with dynamic infrastructure and multi-hop wireless links. The previous researches have primarily focused on routingand MAC protocols in MANET.

Although routing andMAC protocols having important issue such as efficientdata access in MANET. Moreover, the MANETcontains some limitations like battery energy constraint,limited bandwidth, unpredictable signal propagation,mobility and unreliable wireless links. This causesfrequent disconnection in the network that makes issuesin data availability and accessibility. Cooperativecaching is an efficient way to tackle these issues andimprove the system performance in terms of energy,query latency, data delivery and overhead. MNs arecooperating with each other to share the data thatreduces remote server's workload and communicationchannel bandwidth. Due to rapid progress in wirelessnetwork, MANETs are not only used in militaryoperations and also used in commercial and industrialapplications like news, traffic information, cricket scoreupdates and stock market. In cooperative caching, theaccessing shared data is widely cached in the Primary Storagenodes. The shared cache copy is not a static, it ismodified and updated in the server during its lifetime.The modified and/or updated data in the server must bereplicated to cache copy in the caching node. Since datahave cached in many Primary Storage nodes.Thus maintaining cache reliability is a challenging issue in the mobile environment.

The novel consistency approach is predominantly proposed to handle the reliability among the cache copy in PS node and server.

1.1 MOTIVATION

In rapid development of the mobile communication, the MN [Mobile Nodes] retrieves the required data from the remote located source node. The MNs frequently change its location during its datatransmission due to network dynamism and mobility. MNs cannot retrieve the required data from the remote source at all time in the huge network. Hence, MNs caches the accessed data from remote server to share with its neighbors. This cache copy improves data availability in the network. But, the query latency and overhead have decreased drastically in the huge network due to numerous Primary Storage nodes and also invalidation of data takes long time to update the cachecopies in Primary Storage nodes from the server. The server also must ensure the reliability of cache copies in the Primary Storage nodes. It motivates the researcher to make exploration on maintain the reliability among server and caching node over huge Wireless Mobile Networks. Improve the security in the network to propose RSA algorithm for message encryption and decryption. Then for verification the connected nodes are asked to send the values that they have received it from the source. These values when sent back to source, is been encrypted using public key of the source. After receiving the values, the source node decrypts it and substitutes it in the polynomial and check whether it arrives to the super key or not. Thus with the help of this mechanism we can identify the malicious nodes that are present in the network.

1.2 PROBLEM IDENTIFICATION AND PROPOSED SOLUTION

The main problem in the existing system is security. The unauthorized user can give many requests to the server. So that, the server get overload. For this purpose query handling process is maintained by the Query Database [QDB] and the security server is implemented in this process. So the QDB reduces the transmission time and SS allows only authenticated user. Another problem is the authorized user can sometimes hack the data, while the server updates the message and forwards to the Primary Storage Node (PSN). So to improve the security in the network we are proposing RSA algorithm for message encryption as well as decryption.

OUR CONTRIBUTIONS ARE SUMMARIZED IN THREEFOLD

- When Requested Node (RN) request for the data to the Query Database (QDB), it will checks the PS node to send the data. When all PS nodes do not have the requested data, the request will send to the server. Then the servers will response to the requested data. Then that requested node will become the Primary Storage Node (PSN) for the data and it is updated in Query Database (QDB).
- To empower the encryption and decryption used in the network while transmitting: the data's and this is accomplished by using RSA algorithm.
- With the help of Secure Key Distribution Mechanism we can identify the malicious nodes that are present in the Wireless Mobile network.

This paper is framed as follows: Related works are explored in section II. Proposed works are discussed in section III. Result and Discussion are discussed in section IV and the section V discuss about the conclusion and further research.

II. RELATED WORK REVIEW

In this study [1] cooperation based database caching system. In this method query delay and bandwidth utilization more. In this approach [2] middle server between main server and client. But more workload on server. In this study [3] queuing model approachreduce the traffic but still more work load on server. In this method [4] is used to reduce the bandwidth requirement, the server transmits in one of the three modes slow, fast and super-fast. Drawback of this method, if the mode changes to slow, so the client has to wait for long time to utilize cached data. This study [5] Flexible combination of push and pull algorithm. Drawback of this method is latency more.Previous work on server invalidation [6], explored server invalidation by propagating resource changes to all clients that accessed a resource since its previous modification. While this was to guarantee strong cache coherency. It required the server to maintain a client list for each resource, which could become out-of-date as clients may no longer have previously accessed resources in their cache. In addition, invalidations are sent as separate messages, thus generating more network traffic.

The work on push-based mechanisms mainly uses invalidation reports (IRs). The original IR approach was proposed in [7], but since then several algorithms have been proposed. They include stateless schemes where the server stores no information about the client caches [7], [8], [9],and[10] Stateful approaches where the server maintains state information, as in the case of the AS scheme [11]. Many optimizations and hybrid approaches were proposed to reduce traffic and latency, like SSUM, and the SACCS scheme in [12] where the server has partial knowledge about the mobile node caches, and flag bits are used both at the server and the mobile nodes to indicate data updates. Such mechanisms necessitate server side modifications and overhead processing.

III. PROPOSED DESIGN FRAMEWORK

This section describes the design of Proposed Scheme and the interactions between its different components.

3.1 Basic Operations Construction Of The Network

First create the server and plot all primary storage nodes. Create the security server. And then create the one query database it has the query about the primary storage node. Security server used to check the authentication of the client node.

AUTHENTICATION OF CLIENTS AND OPERATION

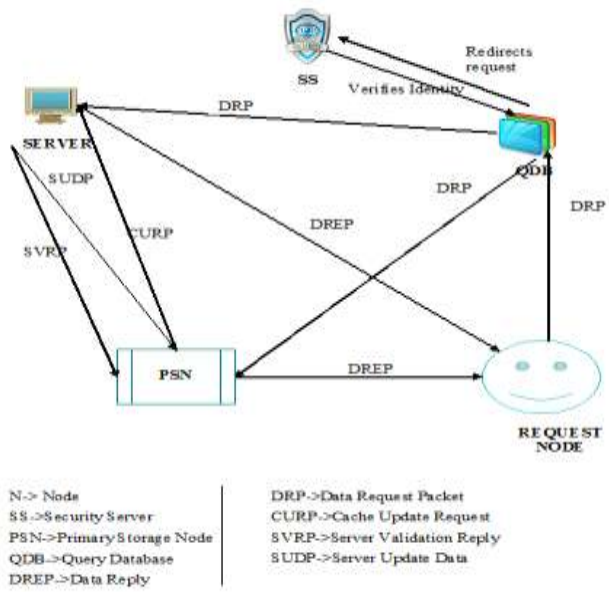
If the node wants the data, that node sends the request to the QDB. Then the request sends to the security server. Here check the authentication of the requested node. If it's valid, the request passes to the QDB .the QDB checks the request. If it has the query, the data can be retrieved using the PSN. Suppose the PSN does not have requested data items of the Request Node or not available in the network, then that the request passes to the server then finally the server sends the data to the requested node. So the requested node will be act as a primary storage node.

QDB AND PSN PROCESSING

Initially, the RN is submitting a Data Request Packet (DRP) for a query indexed in the Query Database (QDB), which forwards the DRP to the PSNPrimary Storage Node, suppose if the data item is expired at PSN, In the PSN, the requested item will be in the waiting list at the moment, the primary storage node will check whether the data item will expired or not and then the PSN to contact the server to update the data item using CURP message is forward to the server. (I.e. In the data item contains a timestamp, prefetch bit, and expired bit).

SERVER PROCESSING

When the server receives a CURP message from the PSN, it checks if all items have been changed by comparing their last modified times with those included in the request. After that, TTL value is calculated, if the item has changed on the server, the Last Updated time and the prefetch bit not set then the server update the data items then forwards to the PSN using SUDP packets and also the packet is encrypted using public key. Suppose if the item did not change on the server and the TTL did not expire on the PSN, so the TTL will not be modified. Also if the item expired on the PSN, but did not change on the server, the PSN increases the TTL value by considering the current time as the update time, without changing the timestamp value it stores finally, the server replies the request to PSN by using SVRP packet. At last the PSN decrypt the packet by using private key and releases the request from the waiting list and sends the updated cached response to the RN via DREP message.



ARCHITECTURE DIAGRAM

3.2 Rsa Mechanism

Actually in our proposed work is mentioning technique for encryption and decryption.In the RSA Algorithm only we are generating key as well as encryption and decryption process.

Operation

The RSA algorithm involves three steps: key generation, encryption and decryption.

Key generation

RSA involves a **public key** and a **private key.** The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key.

The keys for the RSA algorithm are generated the following way:

1. Choose two distinct prime numbers*p* and *q*.

❖ For security purposes, the integers*p* and *q* should be chosen at random, and should be of similar bit-length. Prime integers can be efficiently found using a primality test.

2. Compute $n = pq$.

❖ *n* is used as the modulus for both the public and private keys

3. Compute $\varphi(n) = (p-1)(q-1)$, where φ is Euler's totient function.

4. Choose an integer *e* such that 1 <*e*<φ(*n*) and greatest common divisor of (*e*, φ(*n*)) = 1; i.e., *e* and φ(*n*) are co-prime.

❖ *e* is released as the public key exponent.

❖ *e* having a short bit-length and small Hamming weight results in more efficient encryption - most commonly 0x10001 = 65,537. However, small values of *e* (such as 3) have been shown to be less secure in some settings.

5. Determine *d* as:

$$d \equiv e^{-1} \pmod{\varphi(n)}$$

i.e., *d* is the multiplicative inverse of *e* mod φ(*n*).

❖ This is more clearly stated as solve for d given (de) mod φ(*n*) = 1

❖ This is often computed using the extended Euclidean algorithm.

❖ *d* is kept as the private key exponent.

So, d*e= 1 mod φ(*n*) The **public key** consists of the modulus *n* and the public (or encryption) exponent *e*. The **private key** consists of the modulus *n* and the private (or decryption) exponent *d* which must be kept secret. (*p*, *q*, and φ(*n*) must also be kept secret because they can be used to calculate *d*.). Then, after that, the receiver decrypts the encrypted message with its private key. Then for verification the connected nodes are asked to send the values that they have received it from the source.The source node decrypts it and substitutes it in the polynomial and check whether it arrives to the super key or not. If the source arrives to the super key then all the nodes that have sent the values are genuine nodes. If the super key is not arrived, then any of the nodes is considered to be adversary's nodes.

3.3 Secure Key Distribution Mechanism

In proposed system, the main aim is to avoid the presence of hackers in the network. So that, secure key distribution mechanism is utilized for the process of identification of malicious nodes among mobile nodes.

PROCEDURE:

The source generates a polynomial *q(x)* and assumes the value of p and D. Here, the constant value in the polynomial is considered as "D" and this value is the super key. After the polynomial generation by source, then the source substitutes random values into the polynomial and gets number of corresponding outputs and sends to the each node connected to it. These values are encrypted using the public key of the nodes which has been generated using RSA algorithm. The receiver decrypts the encrypted message with its private key. Then for verification the connected nodes are asked to send the values that they have received it from the source. These values when sent back to source, is been encrypted using public key of the source. After receiving the values, the source node decrypts it and substitutes it in the polynomial and check whether it arrives to the super key or not. If the source arrives to the super key then all the nodes that have sent the values are genuine nodes. If the super key is not arrived, then any of the nodes is considered to be malicious nodes. Thus with the help of this mechanism we can identify the malicious nodes that are present in the network.

IV. RESULTS AND DISCUSSIONS

In the above discussions, it represents clearly that the proposed methods of this paper. In wireless mobile networks, data caching is essential as it reduces contention in the network, increases the probability of nodes getting desired data, and improves system performance. Also enable the security on nodes among them.In figure 1 it shows security performance of previous approaches that is DCIM and SSUM. Comparison of Proposed approach gives more security than existing approaches.

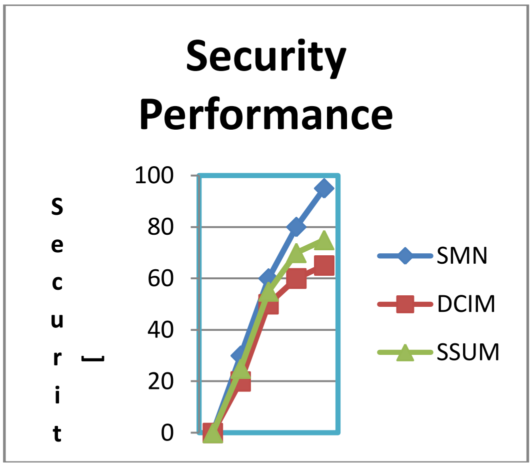


Figure 1Performance of Security

In figure 2 it shows results proved that the proposed approach RSA Mechanism provides better security than the existing approaches. The comparison graphs are shown illustrates below.

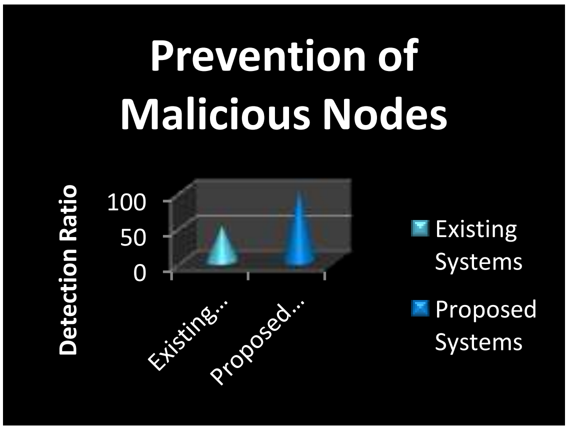


Figure 2Comparisons between Existing and Proposed Systems

V. CONCLUSIONS

In this paper, we presented a novel mechanism for maintaining more security in a wireless Mobile Network.In a wireless mobile network, data caching is essential as it reduces contention in the network, increases the probability of nodes getting desired data, and improves the overall performance. A PSN scheme based on a previously proposed architecture for caching database data in Communication Environments. The original scheme for data caching stores the queries that are submitted by requesting nodes in special nodes, called query Database (Query-Database), and uses these queries to locate the data (responses) that are stored in the nodes that requested them, called PSN (Primary Storage Node).In order to avoid this proposed system implements a client-based Primary storage scheme for Mobile Networks that relies on estimating the inter update intervals of data items to set their expiry time. So that, its increases the accuracy of its estimation also to reduce both traffic and query delays. In this proposed method mainly used the RSA algorithm is implemented for to secure the network in the mobile environments.In the mobile wireless computing environment of the future, a large number of users, equipped with low-powered palmtop machines, will query databases over wireless communication channels.

VI. REFERENCES

1) Artail, H., H. Safa, K. Mershad, Z. Abou-Atme and N. Sulieman., "COACS: A cooperative and adaptive caching system for MANETs", 2008.
2) Shanmugarathinam, G. and K. Vivekandan., "Recent research issues and methodology to improve the performance in mobile computing", 2011.
3) Shanmugarathinam, G. and K. Vivekandan., "Multiple servers-queue model for agent based technology in cache consistence maintenance of mobile environment", 2013.
4) Madhukar, A. and R. Alhajj.,"An adaptive energy efficient cache invalidation scheme for mobile databases", 2006.
5) Huang, Y., J. Cao, B. Jin and X. Tao., "Flexible cache consistency maintence over wireless adhocnetworks", 2010.
6) C. Liu and P. Cao., "Maintaining strong cache consistency in the World-Wide Web", May 1997.http://www.cs.wisc.edu/~cao/papers/icache.html.
7) D. Barbara and T. Imielinski, "Sleepers and Workaholics: Caching Strategies for Mobile Environments", May 1994.
8) G. Cao, "A Scalable Low-Latency Cache Invalidation Strategy for Mobile Environments," IEEE Trans. Knowledge and Data Eng., Sept/Oct. 2003.
9) Z. Wang, S. Das, H. Che, and M. Kumar, "A Scalable Asynchronous Cache Consistency Scheme (SACCS) for Mobile Environments", Nov. 2004.
10) S. Lim, W.C. Lee, G. Cao, and C. Das, "Cache Invalidation Strategies for Internet-Based Mobile Ad Hoc Networks," 2007.