SECURE COOPERATION FOR IMPROVING CONFIDENTIALITY IN MULTIHOP CELLULAR NETWORKS

Hariprasath M.E.,/Assistant Professor, Computer Science and Engineering,
Bharathiyar Institute of Engineering for Women, Salem,India.
hariprasath1989@gmail.com

ABSTRACT

A secure incentive security mechanism for data delivery in Multihop cellular networks(MCN) which provides data confidentiality and provide incentive mechanisms by charging the source and which have limited power supply and intermediate or the mobile relay nodes computation power will drop the packets as they selfishly want to save their stance. The proposed mechanism applies a fair charging policy by charging the source and destination nodes where both of them benefit from the communication. The AC is used to credit the intermediate nodes to encourage them in participating transmission and charge the communicating nodes. Intermediate nodes are credited which makes them to cooperate the entire data transmission.

INTRODUCTION

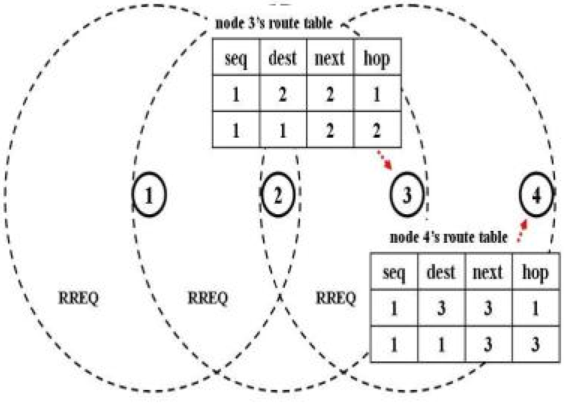
The main aim of the project “Secure Co- operation for improving confidentiality in multihop cellular networks” is to send data securely with co-operation from intermediate nodes. The charging and crediting nodes has been initiated for efficient data transmission.In recent years, research has been performed in the area of multihop cellular networks due to their potential for higher capacity, lower energy consumption, and wider coverage.Multihop Cellular Network (MCN) (Lin Y, 2000) isa network architecture that incorporates the ad hoc characteristics into the cellular system. A node’s traffic is usually relayed through other nodes to the destination. The network nodes commit bandwidth, data storage, CPU cycles, battery power, etc., forming a pool of resources

The utility that the nodes can obtain from the pooled resources is much higher than that they can obtain on their own. The considered MCN is used for civilian applications where the network has long life and the mobile nodes are supposed to have long-term relations with the network. Multihop packet relay can reduce the dead areas by extending the communication range of the base stations without additional costs. It can also reduce the energy consumption because packets are transmitted over shorter distances, and improve the area spectral efficiency and the network throughput and capacity(Chong P, 2008).

EXISTING SYSTEM

The existing system has two communicating nodes which are the sender and the receiver. The sender sends the data which is to be received by the destination node. This is achieved by sending the data through intermediate nodes using Multi hoping technique. The communication between the sender and intermediate nodes inside the same network uses the sender's base station. If the destination node is under another home station the receiver's base station is involved in base station to base station communication. An Accounting center (AC) is involved in crediting accounts and charging the intermediate nodes and communicating nodes respectively. Christo Ananth et al. [2] discussed about Reconstruction of Objects with VSN. By this object reconstruction with feature distribution scheme, efficient processing has to be done on the images received from nodes to reconstruct the image and respond to user query. Object matching methods form the foundation of many state- of-the-art algorithms. Therefore, this feature distribution scheme can be directly applied to several state-of- the-art matching methods with little or no adaptation. The future challenge lies in mapping state-of-the-art matching and reconstruction methods to such a distributed framework. The reconstructed scenes can be converted into a video file format to be displayed as a video, when the user submits the query. This work can be brought into real time by implementing the code on the server side/mobile phone and communicate with several nodes to collect images/objects. This work can be tested in real time with user query results.

An intermediate node may send aroute_reply on behalf of a destination only if its highest sequencenumber for the destination is at least as high as theone in the route_request and it has recently used the routeto forward traffic. If the route_reply is sent by the destination, it is tagged with a sequence number reflecting the lasttopology change known to the destination.



seq	dest	next	hop
1	2	2	1
1	1	2	2

seq	dest	next	hop
1	3	3	1
1	1	3	3

Fig .1: Scenario of general Multihop Cellular Networks

AUTHENTICATION METHOD

To securely credit and charge the intermediate and communicating nodes respectively authentication schemes is introduced to find the contribution of the intermediate nodes in the system. The sender using digital signature scheme signs the data for every packet. The packets which are received by the destination node verify the signature and release a hash from its chain of hash. The digital signature scheme is used to overcome the issues of using the costly time consuming public key cryptographic scheme which degrades the system of mobile nodes. The receiver sends or releases hash per group of messages to overcome the attacks of malicious node.

DISADVANTAGES

1. Packet routing process suffers from new security challenges that endanger the practical implementation of MCN.
2. Nodes' resources such as energy and computing power do not provide direct benefits.
3. The mechanisms suffer from unreliable detection of the selfish nodes and false accusation of the honest nodes.
4. AODV suffers from delay and routing overload.
5. AODV can gather only a limited amount of routing information, route learning is limited only to source node.

PROPOSED SYSTEM

The proposed scheme is an efficient secure charging and cooperation incentive mechanism for the multihop cellular network overcomes and introduces some novel techniques to perform the operation well.Proposed IAODV is defined as "Limited Source Routing up to two hops with Backup route between Source node and Destination node". IAODV protocol combines routing mechanism of DSR and AOMDV protocol in to basic AODV protocol. The proposed IAODV (Improved AODV) protocol can ensures giving timely and accurate information to nodes in data dissemination compare to AODV protocol in city scenario. Proposed method is divided into two sub parts as change in route discovery mechanism and route maintenance mechanism. During the route discovery mechanism of IAODV protocol route request phase is modified for limited source routing up to two hops and route reply phase is modified to create backup route between source and destination node. Route maintenance mechanism is modified such a way that if primary route is failed then source node uses the backup route for transmission of data and if backup route itself failed then new route discovery procedure is performed. The packets are signed and encrypted using the RSA scheme. The receiver verifies the signature, decrypted and accepts the packets.

SECURITY MECHANISM

Existing system doesn't provide data security and confidentiality. The proposed public key cryptography encryption scheme using RSA provides security and confidentiality. The traditional RSA has long computation time and it over rides the mobile systems computation time and power. The implemented security by incorporating a secure and fast RSA scheme in which the encryption and decryption of the data is faster than the earlier system. The FAST RSA system works faster in mobile nodes by efficiently utilizing system resource and processing power.

ADVANTAGES OF PROPOSED SYSTEM

1.Improved Routing protocol IAODV reduces Avg. End-to-End delay, Packet dropping which occurs in AODV protocol.

2.Fast RSA scheme is fast and it reduces the computation overhead and secures the data in the system.

3. It works faster in mobile nodes by efficiently utilizing system resource and processing power

4. The AC encourages the intermediate nodes in participating transmission of packets.

5. RSA is more than 31 and 45 times faster than those of the 168-bit ECDSA and 1,024-

bit DSA.

ARCHITECTURE

The system architecture consists of sender which sends the data which is to be received by the destination node. The sender finds the route in route discovery using proposed reactive routing protocol. The protocol finds the efficient route for the unicast discovery of best forwarding candidates in the system to send the data. Intermediate nodes are mobile nodes which relay the data using their knowledge from the routing system to forward the data to next hop node. The destination node receives the data by checking the signature of the sender and verifying it. Thus this system is combination of Ad-hoc and infrastructure network. Thus at least one base station is involved in Hand- off scheme. Base stations also submit the checks submitted by the intermediate nodes in the system is shown in figure.

ROUTE DISCOVERY AND DATA GENERATION

In this module using routing algorithm i.e., Improved AODV. Discover the efficient route to establish a path which to send data. Since it is unicast cannot flood messages as in AODV broadcast. By use the routes information update the senders routing table. Updating the nodes tables gives the best and shortest route to send the data to the destination and gives the efficient transmission. During discovery of route the sender sends its ID and destination ID along with timestamp hence to check the time of transmission. Generate data to be send to Data that to be send are destination is prepared and ordered in the sender node.

2.MESSAGE SIGNING AND FORWARDING

Based on the route information generate DATA and sign the data with the user's signature and send the data to the next node. In this signing phase sign the data with RSA algorithm in which sign by creating a message digest and adding it to the data and send to the destination. RSA signature scheme is used to sign the packets with Fast RSA to encrypt the messages to provide the confidentiality of the message to overcome.The authentication and message verification overcomes the attacks. The forwarding node thus with the updated table forwards to the next hop node. The intermediate nodes thus forwards and also submit there checks to update their credit which they can exchange for real money or increase the credit balance. After receiving the data packets the source node attaches a signature in each data packet to ensure the payment no repudiation and to verify the message integrity at each intermediate node to thwart Free- Riding attacks as shown in figure 3. Thus the receiver releases hashes for group of messages to notify that the receiver received the packets from the sender.

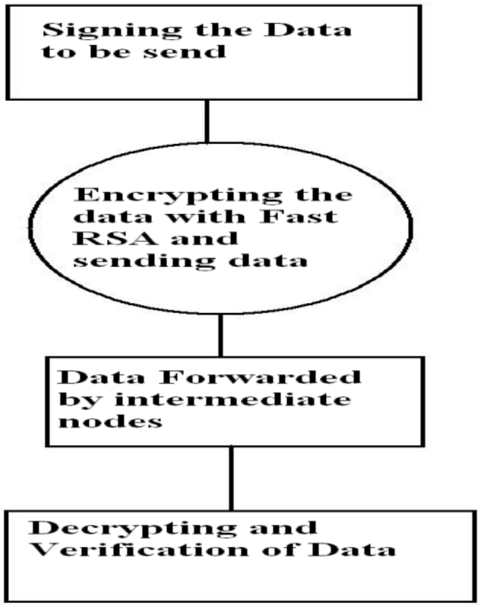

Signing the Data to be send
Encrypting the data with Fast RSA and sending data
Data Forwarded by intermediate nodes
Decrypting and Verification of Data

Fig.3 :Process showing Signing and Verification

PAYMENT SCHEME

A fair charging policy is to support cost sharing between the source and destination nodes when both of them benefit from the communication. Thus to increase the communication and participation of the intermediate nodes in the data transmission use checks which are nothing but a charging policy where the intermediate nodes use the checks to increase their balance. Some malicious nodes send bogus messages to attack the transmission. So each checks are attached with other nodes checks and finally all the checks are sent to the AC for clearance as shown in figure 4.

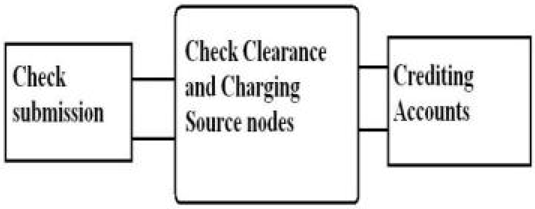


Fig.4: Payment Scheme Method

COMPOSITION AND CLEARANCE

In Check Composition phase a check which contains the payment data has to be composed for all intermediate routes to identify the nodes and payers and payees. The Accounting center charges the Communicating nodes such as Sender and receiver and credits to the intermediate nodes.Based on the data level, rate and transmission time the sender and receiver are charged. In Check Clearance phase the base station submits the check to the AC for redemption but the nodes submit the check if the base station belongs to a different operator . The AC clears the checks submitted by the intermediate nodes and communicating nodes as shown in figure5.

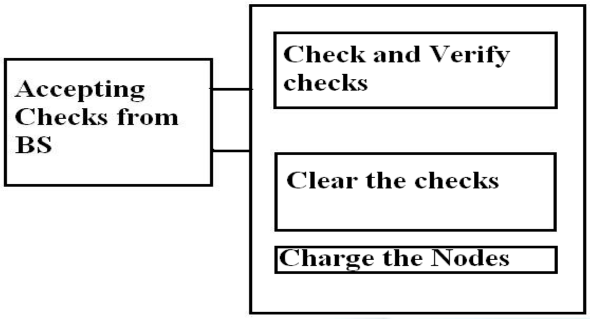


Fig.5: Composition and Clearance phase

CONCLUSION

The efficient secure charging and cooperation incentive mechanism for the multihop cellular network efficiently charge the source and destination node to perform the operation well. The FAST RSA system works faster in mobile nodes by efficiently utilizing system resource and processing power. This system uses payment scheme by accepting the checks from the base station submitted by the intermediate nodes and checks the submitted checks for clearance. After clearance the AC will credit the accounts of the nodes. The AC also charges the sender and receiver based on the amount of data and total time for the transmission.

REFERENCES

[1] Butty´an L. and Hubaux J.P. (2003) " Stimulating Cooperation in Self-Organizing Mobile AdHoc Networks".ACM Mobile Networks & Applications,8(5).

[2] Christo Ananth, M.Priscilla, B.Nandhini, S.Manju, S.Shafiqa Shalaysha, "Reconstruction of Objects with VSN", International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST), Vol. 1, Issue 1, April 2015, pp:17-20

[3] Feeney L. (2001) "An Energy-Consumption Model for Performance

Analysis of Routing Protocols for Mobile Ad Hoc Networks," Mobile Networks and Applications, vol. 3, no. 6, pp. 239-249.

[4]Gomes C. and Galtier J.(2009) "Optimal and Fair Transmission Rate Allocation Problemin Multi-Hop Cellular Networks," Proc. Int'l Conf. Ad-Hoc, Mobile and Wireless Networks, pp. 327-340.

[5]Gomes C. and Galtier J.(2009) "Optimal and Fair Transmission Rate Allocation Problemin Multi-Hop Cellular Networks," Proc. Int'l Conf. Ad-Hoc, Mobile and Wireless Networks, pp. 327-340.