Optimal Transmission in Multihop Cellular Networks by Detecting Irrational Nodes

Jashma Suresh P.P.*, Prof. V. Chandrasekar**

Department of Computer Science and Engineering
Dhanalakshmi Srinivasan Engineering College
Perambalur, India
*jashma.suresh@gmail.com

Abstract– In multihop cellular networks mobile nodes usually transmit packets through intermediate mobile nodes for enhancing performance. Selfish nodes usually do not cooperate which has a negative effect on the network fairness and performance. A fair, efficient and optimal incentive mechanism has been proposed to stimulate the mobile node's cooperation. Hashing operations are used in order to increase the security. Trivial Hash function has been used to improve end-to-end delay and throughput. In addition Cyclic Redundancy Check Mechanism has been employed to identify the irrational nodes that involve themselves in sessions with the intention of dropping the data packets. Moreover, to reduce the collision at the Accounting Center a Border node has been entrusted the task of submitting the checks using a digital signature.

***Index Terms*–**Border Node Mechanism, Cyclic Redundancy Check, Selfish nodes, Trivial Hash Function

I. Introduction

Reputation-based and incentive mechanisms have been proposed to avoid selfishness attacks. For reputation-based mechanisms the nodes usually monitor the transmissions of their neighbors to make sure that the neighbors relay other nodes' traffic, and thus, selfish nodes can be identified and punished. For incentive mechanisms, packet relay is a service not an obligation. The source and destination nodes pay credits (or virtual currency) to the intermediate nodes for relaying their packets. Credits can stimulate the nodes' cooperation by proving that it is more beneficial for the nodes to cooperate than behaving selfishly.

A fair and efficient incentive mechanism has been proposed to stimulate the node cooperation. Hashing operations are used in the ACK packets to reduce the number of public-key-cryptography operations.

Trivial Hash function has been used to reduce the number of public key cryptographic operations. In addition it also has the advantage that it can reduce the computation cost.

Cyclic Redundancy Check Mechanism has been employed to identify the irrational nodes that involve themselves in sessions with the intention of dropping the data packets to launch Denial-of-Service attacks.

Moreover, reducing the overhead of the payment checks is essential for the efficient implementation of the incentive mechanism due to the large number of payment transactions. To enable this, instead of allowing each of the intermediate nodes to submit checks individually for payment a Border node has been entrusted the task of submitting the checks using a digital signature. Extensive analysis and simulations demonstrate that the proposed system enables efficient data transfer by detecting irrational nodes .The network efficiency has been significantly improvised by reducing the overhead of check submission using Border node mechanism. Moreover Trivial Hash function has significantly reduced the cost of computing hash functions without compromising the message integrity.

II. Literature Review

A secure mechanism is presented [1] to stimulate end users to keep their devices turned on, to refrain from overloading the network, and to avoid tampering aimed at converting the device into a "selfish" one. A Locally Aware Reputation system has been proposed [2] that addresses selfish behavior by using locally available information. An overview of security problems [3] for mobile ad hoc networks distinguishing the threats on basic mechanisms and on security mechanisms is discussed. A micro-payment scheme has been proposed [4] for multi-hop cellular networks that encourage collaboration in packet forwarding by letting users benefit from relaying others' packets. A protocol [5] is presented for routing in ad hoc networks that uses *Dynamic Source Routing*. Multihop Cellular Network (MCN), for wireless communications [6] preserves the benefit of conventional Single Hop Cellular Networks (SCN) where the service infrastructure is constructed by fixed bases, and it also incorporates the flexibility of ad-hoc networks where wireless transmission through mobile stations in multiple hops is allowed. In multihop cellular networks, the mobile nodes usually relay others' packets [7] for enhancing the network performance and deployment. A fair and efficient incentive mechanism-FESCIM has been proposed to stimulate the node cooperation. Two techniques have been proposed that improve throughput in an Ad-hoc network [8] in the presence of nodes that agree to forward packets but fail to do so. There is a watchdog that identifies misbehaving nodes and there is a pathrater that helps routing protocols avoid these nodes. A simulation study is carried out [9] that identifies security issues that are specific to MANET and that illustrate the effects of those threats on network performance when the DSR routing protocol is used. A multi-party micropayment [10] scheme has been proposed that allows all parties involved in a call to be paid in real-time. Multi-hop cellular networks (also called hybrid networks) appear to be a promising combination of the dynamics of mobile ad hoc networks and the reliability of infrastructured wireless networks [11]. These hybrid networks offer several advantages for users as well as operators. A Cooperation And Accounting Strategy For Hybrid Networks called CASHnet has been proposed which stimulates cooperation among nodes by making it a rewarding alternative to selfishness. Our scheme incorporates security architecture, which is based on public key cryptography and uses digital signatures and certificates. Today’s public Wireless LANs are restricted to hotspots [12]. With the current technology, providers can only target a small audience and in turn charge high prices for their service to generate revenue. Also, providers cannot react appropriately to dynamic changes in the demand. Therefore, a cooperation and accounting scheme has been which introduces monetary rewards. CASHnet is compared with the Nuglet scheme using simulations under the criteria of network liveliness, overhead, and packet drop reasons as well as cash flow. CASHnet, uses a highly decentralized accounting and security architecture .It allows selfish nodes and supports cost sharing between sender and receivers located in different sub networks. Integrated Cellular And *Ad Hoc* Relaying Systems (iCAR) [13] is a new wireless system architecture based on the integration of cellular and modern *ad hoc* relaying technologies. It addresses the congestion problem due to unbalanced traffic in a cellular system and provides interoperability for heterogeneous networks. The proper functioning of mobile ad hoc networks depends on the hypothesis that each individual node is ready to forward packets for others [14].To address this problem, we propose a credit-based Secure Incentive Protocol (SIP) to stimulate cooperation among mobile nodes with individual interests. SIP can be implemented in a fully distributed way and does not require any pre-deployed infrastructure. Sprite [15], a simple, cheat-proof, credit based system is proposed for stimulating cooperation among selfish nodes in mobile ad hoc networks.

III. EXISTING SYSTEM

In multihop cellular networks, the mobile nodes usually relay other node’s packets for enhancing the network performance and deployment. As a first step to this process in FESCIM [7], a route is set up between source and destination by the Route Discovery Phase. During this the sender will send a Route Request Packet to its neighbors that contain the destination address. The neighbors in turn append their own address to the Route Request Packet and rebroadcast it. This process continues until the Route Request Packet reaches the destination. The destination will confirm this route by a Route Reply Packet. The data packet being sent will be encrypted by using hashing operation. In addition hashing process will also reduce the number of public-key-cryptographic operations. Upon receiving the Route Reply Packet, each intermediate node relays the packet. However, selfish nodes usually do not cooperate but make use of other nodes for relaying the packets. Such nodes are identified and punished. After successful data transfer the co-operating nodes will submit a check to the Accounting Center for reimbursement of resources. The Accounting Center will then distribute the credits to the co-operative nodes after verification of the checks.

IV. PROPOSED SYSTEM

From the studies conducted over the years it has been clear that during data transfer some delay still exists. Selfish behavior among nodes is found to be one important reason for this delay in data delivery. Various techniques have been adopted to reduce this selfish behavior and enhance cooperation among intermediate nodes but it has been found out that some misbehavior still exists due to the presence of irrational nodes in the network. The existing system can avoid selfishness attacks but it cannot identify the irrational nodes that involve themselves in sessions with the intention of dropping the data packets. Techniques could be adopted to find out such irrational nodes.

Previously hashing operations have been utilized to secure the data being transferred over the network. But however hashing operations also give rise to some computational delay.

This cost of computation could be reduced using better hashing techniques.

Moreover each of the cooperating nodes that have participated in successful data transfer submit checks to the Accounting Center for reimbursement of resources. This can result in congestion at the Accounting Center. Steps could be taken to reduce this traffic congestion.

The proposed system aims at overcoming all these draw backs.

- Reduces time delay involved in data transfer by identifying irrational nodes.
- Reduces the computational cost of hashing
- Reduces the traffic congestion at the Accounting Center

A. CRC- Cyclic Redundancy Check

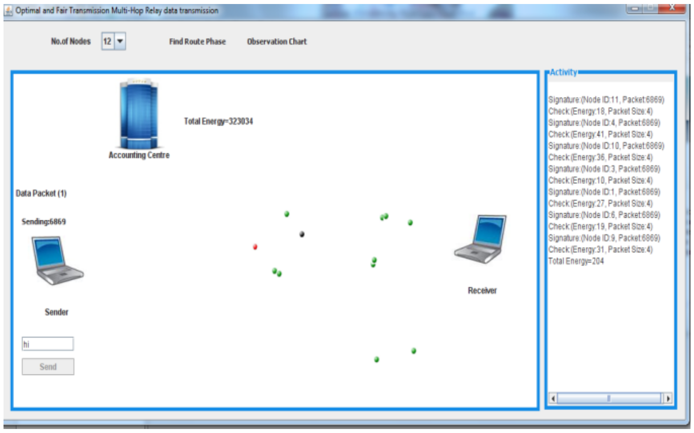
Cyclic Redundancy Check can be used for dealing with irrational nodes. Each data packet to be transmitted is appended with a checksum and this checksum is calculated at every hop of data transfer. If there is a difference in the checksum value there is a data loss so that particular node is found out and blocked. Such nodes are irrational nodes. This will help avoid data loss and ensure high throughput and reduce end to end delay.

B. Trivial Hash function

Trivial Hash function has been used to reduce the cost of computing the hash function. If the datum to be hashed is small enough, one can use the datum itself as the hashed value. The cost of computing this "trivial" hash function is effectively zero. This hash function is perfect, as it maps each input to a distinct hash value. An index table is maintained that gives alternate form of the character Invalid data values may be left undefined in the table, or mapped to some appropriate "null” value.

C. Border Node Mechanism

To deal with congestion at the Accounting Center a border node is entrusted the responsibility of check submission. All the intermediate cooperating nodes will hand over the checks to this Border Node. This Border Node will then generate a final check and secure it with a digital signature and send it to the Accounting Center. This will ensure less congestion at the Accounting Center and help deal with the bottleneck problem.



Total Energy=323034

Sending:6869

hi

```
Signature:(Node ID:11, Packet:6869)
Check:(Energy:18, Packet Size:4)
Signature:(Node ID:4, Packet:6869)
Check:(Energy:41, Packet Size:4)
Signature:(Node ID:10, Packet:6869)
Check:(Energy:36, Packet Size:4)
Signature:(Node ID:3, Packet:6869)
Check:(Energy:10, Packet Size:4)
Signature:(Node ID:1, Packet:6869)
Check:(Energy:27, Packet Size:4)
Signature:(Node ID:6, Packet:6869)
Check:(Energy:19, Packet Size:4)
Signature:(Node ID:9, Packet:6869)
Check:(Energy:31, Packet Size:4)
Total Energy=204
```

Figure 1: Data transmission secured using trivial hashing

V. RESULT AND DISCUSSION

Java Network Simulator (JNS) is used for simulation set up. JNS is a popular network simulation tool used for network lab experimentation and research. JNS provides network performance metrics at various abstraction levels such as Network, sub-network, Node and a detailed packet trace. Using JNS modeling and simulation services are provided in a variety of networking technologies and protocols. Results obtained are as shown below. Table I, II, III shows variation in throughput, end to end delay and packet loss for 12 nodes respectively. Similarly the graphs obtained for these variations are also shown below in Figures 2, 3, 4 respectively.

Performance of MANET with the nodes in mobility

Table I: Variation in throughput

Throughput(Kbps)	
FESCIM	**Optimal**
81.25	91.25
87.25	97.25
94.75	103.95
102.5	112.25
109.5	118.9
116.25	125.25
121.75	130.75

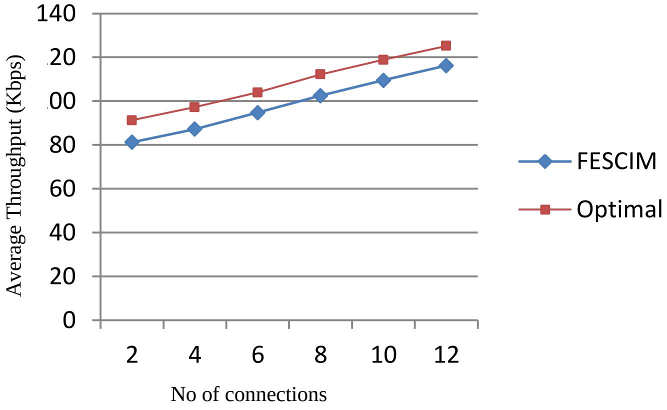


Figure 2: Comparison of throughput

Table II: Variation in end to end delay

End to end delay(ms)	
FESCIM	**Optimal**
98.5	96.25
100.25	99.5
101.5	100.25
102.75	100.75
104.25	103
105.25	103.75
107.5	105.25

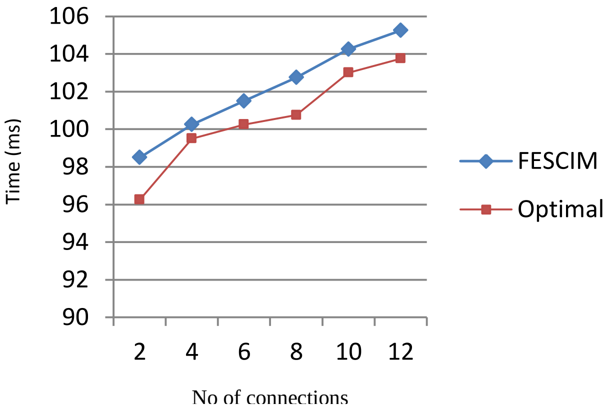


Figure 3 :Comparison of end to end delay

Table III: Variation in packet loss

Packet loss(no of packets per sec)	
FESCIM	**Optimal**
26.25	16.25
30.5	22.25

39.75	30.75
41.5	32.25
51.5	43.75
59.25	48.25
61.75	50.25

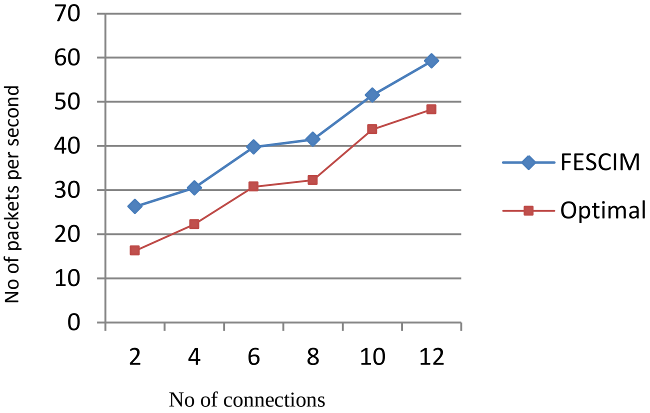


Figure 4: Comparison of packet loss

VI. CONCLUSION

An optimal and secure transmission mechanism has been proposed for Multihop Cellular Networks. Irrational nodes have been found out thereby increasing throughput by 9.4 % and reducing end to end delay by 1.6%. Extensive simulations show that the proposed mechanism achieves better transmission by reducing the packet loss by 9%.

REFERENCES

[1] L. Buttyan and J.Hubaux, “Enforcing service availability in Mobile Ad-Hoc Wans” Proc.ACM MobiHoc,pp.87-96,Aug.2000

[2] J.Hu, “Cooperation in Mobile Ad Hoc Networks” Technical Report TR-050111,Computer Science Dept.,Florida State Univ.,Jan.2005

[3] J. Hubaux, L. Buttya´n, and S. Capkun, “The quest for security in Mobile Ad Hoc Networks,” Proc. ACM Symp. Mobile Ad Hoc Networking and Computing, Oct. 2001.

[4] M. Jakobsson, J. Hubaux, and L. Buttyan, “A micro-payment scheme encouraging collaboration in Multi-Hop Cellular Networks,”Proc. Seventh Financial Cryptography (FC ’03), pp. 15-33,Jan. 2003.

[5] Johnson and D. Maltz, “Dynamic source routing in Ad Hoc Wireless Networks,” Mobile Computing, pp. 153-181, chapter 5, Kluwer Academic, 1996.

[6] Y.Lin and Y. Hsu, “Multihop Cellular: A new architecture for wireless communications ”Proc.IEEE INFOCOM, vol.3.pp-1273-1282, Mar.2000

[7] M. Mahmoud and X. Shen, “FESCIM: Fair, Efficient and Secure Cooperation Incentive Mechanism for Multihop Cellular Networks”, IEEE Trans.Mobile Computing, vol11, no5, pp-753-766, May 2012

[8] S. Marti, T.G. T. Giuili, K. Lai and M. Baker, “Mitigating routing misbehavior in Mobile Ad-Hoc Networks”, Proc.ACM MobCom, pp.255-265, Aug.2000

[9] P. Michiardi and R. Molva, “Simulation-based analysis of security exposures in Mobile Ad Hoc Networks” Proc.European Wireless Conf., Feb 2002

[10] M.Peirce and D. O’Mahony, “Micropayments for Mobile Networks,”technical report, Dept. of Computer Science, Trinity College, 1999.

[11] Weyland and T. Braun, “Cooperation and accounting strategy for Multi-HopCellular Networks,” Proc. IEEE Local and Metropolitan Area Networks (LANMAN ’04), pp. 193-198, Apr. 2004.

[12] W.Staub, and T. Braun, “Comparison of motivation-based cooperation mechanisms for Hybrid Wireless Networks,”J. Computer Comm., vol. 29, pp. 2661-2670, 2006.

[13] H. Wu, C. Qiao, S. De, and O. Tonguz,” Integrated Cellular And Ad HocRelaying Systems: Icar”, IEEE J. Selected Areas In Communications, vol. 19, no. 10,pp.2105-2115, October 2001

[14] Y. Zhang, W. Lou, and Y. Fang, “A secure incentive protocol for Mobile Ad Hoc Networks,” ACM Wireless Networks, vol. 13, no. 5,pp. 569-582, Oct. 2007.

[15] S. Zhong, J. Chen and R. Yang, ”Sprite: A Simple Cheat Proof Credit Based System for Mobile for Mobile Adhoc Networks”, IEEE Trans. Mobile Computing,vol5,no.4,pp.365-376,Apr.2006

AUTHORS

First Author – Jashma Suresh PP, ME CSE II, Dhanalakshmi Srinivasan Engineering College Perambalur, jashma.suresh@gmail.com

Second Author – Prof. V. Chandrasekar, Dhanalakshmi Srinivasan Engineering College Perambalur, India