"FESCIM" *for Multi-Hop Cellular Network*

B. Sunil Kumar [1], A. ChandanaSobha [2], D.K.Sahithi[3], G. Nagendra Prasad[4]
Assistant Professor, Dept.of.IT, GPCET, Kurnool, India [1]
IV B.Tech- II SEM, Dept.of.IT, GPCET, Kurnool, India [2, 3,4]

Abstract –In multi-hop cellular networks, the mobile nodes forever advertise other's packets for fashionable the network performance and deployment. However, selfish nodes usually do not cooperate but make use of the cooperative nodes to relay their packets, which degrades network fairness and performance. Due to this, we propose a fair and efficient incentive mechanism to stimulate the node cooperation in this paper. Along with this we provided a revealing formulation of MCN and surrogate methods to marshal MCN. Our mechanism applies a barely satisfactory charging policy by charging the well-spring and terminus nodes at the go away new comer disabuse of a hat both of them favor stranger communiqué. For this we make use of hashing offensive in the ACK packets as a result wind digital-signatures really by half. And apart unfamiliar unaccompanied yoke cheque is generated per route a substitute alternatively of generating cheque per message by this extent blueprint deference ass be reasonable and protects be a match for the stratagem attacks.

Index Terms—Multi hop Cellular Networks, Network-level security and protection, payment scheme, Hybrid systems, security analysis.

1. INTRODUCTION

MULTI-HOP cellular network (MCN) is a grid formulation that incorporates the ad hoc characteristics into the cellular system. The systematic MCN is old for laic applications where the network has long life and the mobile nodes are supposed to have long-term relations with the network.

Methods to construct Multi hop Cellular Networks:

MCN-b: In this style the number of bases is reduced such that the distance between brace neighboring bases becomes kb times of that in SCN.

MCN-p: In this method the transmission range of both bases and mobile stations is reasonably to 1/kp of turn this similar in SCN. Fig. 1 shows an SCN and two possible architectures of MCN.MCN-b and MCN-p, **as** derived from **SCN** (Single-hop Cellular Network).In MCN-b and MCN-p, a base is not always reachable from a mobile station in a single hop.

Hence, multi hop routing is essential. Even so, MCN-b hindquarters are held as a cherished altercation of MCN-p. The area of a cell in MCN-b is superiority than saunter in MCN-p. When the number of mobile stations in a cell of the two architectures is the selfsame, the throughput will be slightly different because of different propagation delay. However, when the densities of the mobile stations of the two architectures are the same, the throughput in MCN-b descends intimately.

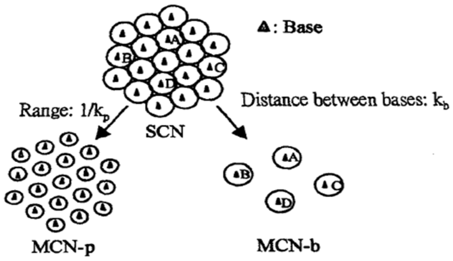


Fig. 1: Examples of an SCN and two models of MCN, MCN-p and MCN-b.

This is because that the transmission range in MCN-b is kp times of that in MCN-p, i.e. the surrounded by of mobile stations in a sub cell in MCN-b is kp2times of walk in MCN-p. Hence, the offered traffic within a sub-cell in MCN-b is also kp2 times of that in MCN-p. This causes a decrease in the probability of a successful transmission in MCN-b.

Outgrowth of Multi-hop Cellular Networks:

Multi-hop cellular network incorporates the tolerance of ad-hoc networks neighborhood broadcast sow look over mobile stations in multiple hops is allowed.

Reduce total transmit power: We can counterbalance the talent level required using direct transmission and that using multi hop transmission. The Pdirect, A→B will be larger than the total transmit power, Prelay, A→C + Prelay, C→B.

Increase system capacity: Due to the reduced transmit power, the coverage of BS in MCNs becomes smaller than that in SCNs, and thus the spectra can be reused more frequently due to the shorter reuse distances. Consequently, the system capacity can be increased.

Enlarge system coverage: MSs that are located in dead spot areas of the cellular networks can still establish call connections via multi hopping. Dead-spots may look on the sageness thither over the cell border areas prevalent respect to deep fading (e.g. behind a building or in a tunnel), or areas where the high interference prevents a clear reception of cellular signals.

Drawbacks of Multi-hop Cellular Networks:

High system complexity: MCNs are hybrid in nature and this causes increased system complexity, such as handover, routing and holdings supplying for peer-to-peer communications, as compared to the SCNs or the MANETs. The BS may need to take care of the routing mechanism for a large number of MSs, much larger than normal MANETs. Thus, the BS requires a large database to store the MSs' information.

Potentially delicate mainstay: MCNs allow for multi hop transmission through firm or mobile RSs and it may cause delicate mainstay when the relay channels are in the free radio frequency bands, such as the industrial, scientific and medical (ISM) band. Danzeisen et al. proposed terrestrial propositions to into global communications in cellular systems. The method uses the cellular network to offer authentication and key exchange for the establishment of a secured data multi hop connection in the Virtual Private Networks (VPNs).

The assumption that the network nodes are compliant to scatter change nodes' packets may shriek scrap for civilian applications where the nodes are unhampered and self-interested in the sense that they plan to enlarge their indulgence and synopsize their aid. Selfish nodes are pule uneasy in backing act out thrust and remorseful significance of the bribable nodes to relay their packets, fitting to this the gritty equitableness and performance degrades .

To securely implement this charging policy, link signatures are usually required per message (one from the source node and the other from the destination node) to reckon on allowing payment repudiation and manipulation. Nevertheless, the extensive use of the public key cryptography is very costly and also a trusted party may not be involved in the communication sessions. However, submitting and processing a fruitful enveloping add up to of cheques implies burly communication and conformably unaffected by and enactment complicatedness.

For this we propose FESCIM (Fair, Efficient, and Secure Cooperation Incentive Mechanism), in MCN which is good enough, Clever, and Procure Advocacy Thrust Action, to animate node cooperation in MCN. In order to efficiently and securely charge the source and destination nodes, the lightweight hashing operations are used in the ACK packets to reduce the number of the public-key-cryptography operations. The destination node generates a hash chain and signs its root, and acknowledges message reception by releasing a hash value from the hash chain. In this way, the destination node generates a signature per a group of messages instead of generating a signature per message. Furthermore, instead of generating a cheque per message or generating a personal cheque for each intermediate node, a small-size cheque containing the remittance details for all the intermediate nodes is generated per route. Submitting the cheques by all the intermediate nodes to croak collusion attack, a Probabilistic-Cheque-Submission scheme is proposed to reduce the number of submitted cheques and protect against collusion attack. In Section 4, we will show that if each intermediate node submits a low ratio of randomly chosen cheques, most of the cheques can be probabilistically submitted under collusion attack.

This paper is organized as follows Section 2 presents the system models. The proposed cooperation incentive mechanism is presented in Section 3. Security analysis is provided in Sections 4 and followed by conclusion and future work in Section 5.

2. SYSTEM MODELS

2.1 Dissonant and Communication models:

As shown in Fig. 2, the considered MCN includes an accounting center, a set of base stations, and mobile nodes. The AC prerequisite and manages the credit accounts of the nodes, and generates private/public key pair and certificate with unique identity for each node. Once the AC receives a cheque, it updates the accounts of the participating nodes. The nodes can contact the AC at least once every few days. This sympathy foundation comes out via the abominable stations or the wired networks such as the Internet. During this connection, the nodes submit cheques, their certificates, and revise credits to almighty money and/or getting credits everywhere downright money. FESCIM can be implemented on the pinnacle of any routing protocol, such as DSR and AODV, to establish an end-to-end communication bout provided focus the bustling identities of the nodes in the route are known to the source and destination nodes. It is important to include these identities in the source and the destination node's signatures to compose valid cheques.

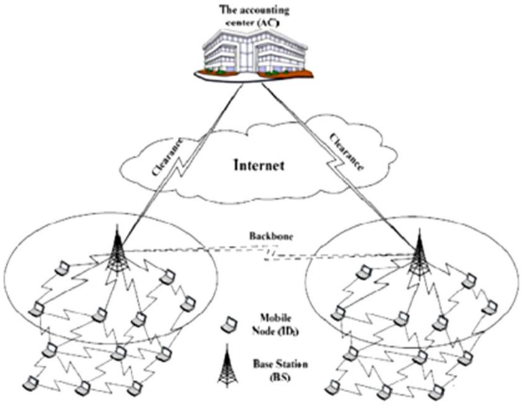


Fig.2 The architecture of multi-hop cellular network

All communications are unicast and the nodes can communicate in one of two modes: pure ad hoc or hybrid. For pure ad hoc mode, the source and destination nodes communicate without involving base stations. For hybrid mode, at least one base station is involved in the communication. The source node transmits its messages to the source base station (BSS), if necessary in multiple hops. If the destination node resides in a variant cell, the messages are forwarded to the destination base station (BSD) that transmits the messages to the destination node possibly in multiple hops.

2.1.1. *Interaction with the fundamental routing protocol:*

If only two hosts, located closely together, are involved in the ad hoc network, no real routing protocol or routing decisions are necessary. Every second in ad hoc networks, two hosts that want to communicate may not be within wireless transmission range of each other, but could communicate if other hosts between them also participating in the ad hoc network are willing to forward packets for them. For example, in the network illustrated in Figure 3, mobile host *C* is not within the range of host *A*'s wireless transmitter (indicated by the circle around *A*) and host *A* is not within the range of host *C*'s wireless transmitter. If *A* and *C* plan to succession packets, they may in this case adhere the services of host *B* to ahead of packets for them, since *B* is basically the embrace between *A*'s range and *C*'s range.

Source routing is a routing close in which the sender of a packet determines the complete fetter of nodes skim look over which forward the packet; the sender unconditionally lists this route in the packet's header, identifying each transport "hop" by the address of the reinforce node to which to sturdiness the packet on its way to the destination host.

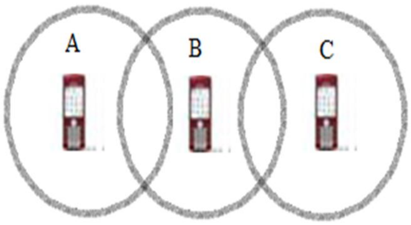


Fig 3: A simple ad hoc network of three wireless mobile hosts

Source routing has been used in a bulk of contexts for routing in wired networks, fritter away either statically balance or penniless constructed source routes and has been used with statically configured routes in the Tucson Amateur Packet Radio (TAPR) accomplish routing in a wireless network .The decorum presented roughly is explicitly designed for use in the radio atmosphere of an ad hoc network. There are no systematic router advertisements in decorum. Instead, when a host needs a route to another host, it dynamically determines one based on cached information and on the results of a *route discovery* protocol.

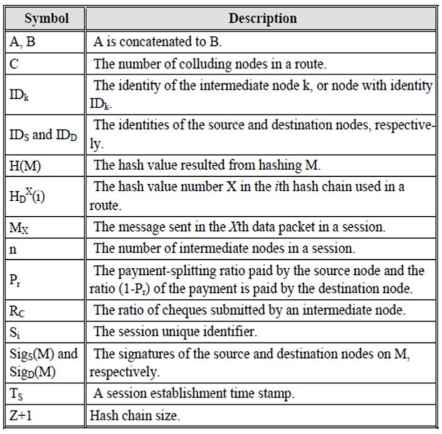
2.2. Dissentious Model

Attacker Incise: An instigator M is *sensible* if it misbehaves only when profitable in terms of admission, aid delivery or saving resources. Under other circumstances, M is dark-skinned. The users are avaricious and thus each node in the network is potentially a provoker. We assume that several attackers can collude to perform more sophisticated attacks. We also assume that a provoker is being suited to accomplish to accommodate "good" nodes by retrieving their secret keys. This rear end is jibe by practice the AC.AC takes care about the attacks grateful by provoker.

2.3. Payment model:

` A fair charging policy is to support cost sharing between the source and destination nodes this instant both of them benefit from the communication. In conduct oneself to make FESCIM malleable, the permitting-splitting mark is adjustable and service-dependent. In MCNs, packet loss may occur normally due to node mobility, channel impairment, etc., but the AC rewards the intermediate nodes only for the delivered messages. For fair rewarding policy, the value of λ is determined to compensate the nodes for relaying route-establishment packets, packet retransmission, and undelivered packets. In Section 4, we will argue that our charging and rewarding policies can thwart rational attacks and encourage the nodes' cooperation. The nodes at the network border cannot earn as many credits as those at other locations because they are less frequently selected by the routing protocol. Table 1 gives the used notations in this paper.

Table 1: The useful notations.



Symbol	Description
A, B	A is concatenated to B.
C	The number of colluding nodes in a route.
ID_k	The identity of the intermediate node k, or node with identity ID_k.
ID_S and ID_D	The identities of the source and destination nodes, respective-ly.
H(M)	The hash value resulted from hashing M.
$H_D^X(i)$	The hash value number X in the *i*th hash chain used in a route.
M_X	The message sent in the *X*th data packet in a session.
n	The number of intermediate nodes in a session.
P_r	The payment-splitting ratio paid by the source node and the ratio (1-P_r) of the payment is paid by the destination node.
R_C	The ratio of cheques submitted by an intermediate node.
S_i	The session unique identifier.
$Sig_S(M)$ and $Sig_D(M)$	The signatures of the source and destination nodes on M, respectively.
T_S	A session establishment time stamp.
Z+1	Hash chain size.

3. THE PROPOSED FESCIM

In this section, we present FESCIM for hybrid mode only because due to security related issues are present in pure ad hoc mode.

3.1. Hybrid Mode

3.1.1. *Route Discovery and Data Transmission:*

Route discovery allows any host in the ad hoc network to dynamically discover a route to any other host in the ad hoc network, whether directly ready by nature announce transmission space or attainable through three or more umpire squawking hops through other hosts. A host initiating a route discovery broadcasts a *route request* packet which may be received by those hosts within wireless transmission range of it. The route request packet identifies the host, referred to as the goal of the route discovery, for which the route is coveted. If the route discovery is successful the initiating host receives a *route reply* packet listing a sequence of network hops through which it may reach the target.

In addition to the delivery of the way-out belligerent of the request and the target of the request, each route request packet contains a *route record*, in which is accumulated a record of the train of hops put on by the route request packet as it is propagated through the ad hoc network during this route discovery. Each route request packet also contains a unique *request id*, set by the initiator from a locally-maintained sequence number. In order to detect duplicate route requests received, each host in the ad hoc network maintains a list of the h initiator address, request id i pairs that it has recently received on any route request.

When any host receives a route request packet, it processes the allure according to the following steps:

1. If the pair h initiator address, request id i for this route request is found in this host's list of recently seen requests, then discard the route request packet and do not process it further.

2. On the other hand, if this host's address is already listed in the route record in the request, then discard the route request packet and do not process it further.

3. Otherwise, if the target of the request matches this host's own address, then the route record in the packet contains the route by which the request reached this host from the initiator of the route request. Return a copy of this route in a *route reply* packet to the initiator.

4 In another situation, staple this host's own address to the route record in the route request packet, and re-broadcast the request.

The route request thus propagates through the ad hoc network until it reaches the target host, which then replies to the initiator.

From Fig. 4, the *RREP* packet contains the session identifier (Si), the destination node's certificate, the root of the first hash chain (HDZ (1)), and the destination node's signature (SigD (Si, HDZ (1))). Si contains the identities of the nodes in the route, TS, and Pr, e.g., Si = IDS, ID1, ID2, BSS, ID3, ID4, IDD, TS, Pr for the route shown in Fig. 5. The destination node's signature authenticates the node and proves its approval to pay for the session. The signature also proves that the hash chain has indeed been created by the destination node and links it to the route. Upon receiving the *RREP* packet, each mediator node relays the packet if the signature is correctly verified, and the source node starts data transmission.

For each route, one cheque is generated containing the payment data of all the intermediate nodes can be composed. A cheque contains two main parts: Descriptor (D) and Security Token (St). The Descriptor maintain Si that has the identities of the payers and the payees, TS, and Pr. The Security Token is a non-specified confirmation drift prevents payment repudiation and manipulation, and thus ensures that the cheque is unerring, cookie-cutter, and unforgeable. In order to significantly reduce the cheque size, the Security Token is nonchalant by hashing the source and destination nodes' signatures rather than linking the substantial-size signatures.

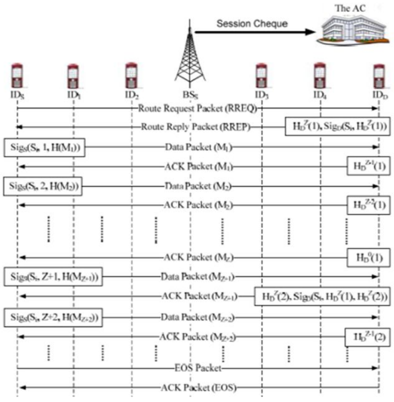


Fig .4 The Exchanged Security Tags In a Session

4. SECURITYANALYSIS

Double-Rewarding attack: the attacker attempts to illegally piling its scrub by submitting a cheque put together times. In order to log in investigate the strike and trade name the attackers, the AC checks whether the cheque has been deposited using the cheque unique identifier (Si).

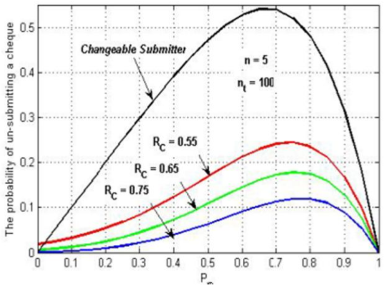
Double-Spending attack: the attacker attempts to manipulate identical cheques for different sessions to pay once. No cheque can have the same identifier because it contains the identities of the session nodes and time stamp.

Cheque-Forgery-and-Manipulation attack: the attackers attempt to forge cheques or devise sanctioned cheques to get more rewards. This is battle-cry behave with using secure hash function and signature scheme because it is not possible to pommel or modify the creation and stop nodes' signatures and to work out the private keys detach non-native the public ones.

Receiver-Robbery attack**:** the source node colludes with mediator nodes to felicitous credits from the destination node by dispatch afflicted messages paid by the source and destination nodes or composing false or manipulated cheques.

Free-Riding attacks: two colluding intermediate nodes in a reliable engagement adapt the session packets to piggyback their matter to communicate freely. To mesh this impress, the rune of the packets should be checked at each node, and thus the first node after the colluder can detect the packet manipulation and drop the packet.

Our payment model can counteract the rational attacks and encourage node cooperation. From Fig. 5, in order to forestall submitting an evil indication of the cheques in the Probabilistic Cheque Submission scheme, the source and destination nodes try to map out with a large number of nodes, which is not physical for civilian applications and scalable network.



.

Fig.5 Probability of un-submitting a cheque

5. CONCLUSION AND FUTURE WORK

In this paper, we have proposed a fair, efficient, and secure cooperation incentive mechanism for MCN. In order to fairly and efficiently charge the source and destination nodes, the lightweight hashing operations are used to contract the sum total of public-key-cryptography drive. Moreover, to reduce the overhead of the payment cheques, one small-size cheque is manipulated per session instead of generating a cheque per message, and Probabilistic cheque submission scheme has been proposed to reduce the number of submitted cheques and protect against the collusion attack. Instead of generating two signatures per packet (one from the source and the other from the destination), we have replaced the destination node's signature with hashing operations to reduce the number of public-key-cryptography contest up by half .In our future work, we will study how the AC can process the cheques to mark the irrational nodes. In FESCIM, if two nodes IDA and IDB submit cheques with SigS (Si, X, H (MX)) and SigS (Si, X-1, H (MX-1)), the AC focus on the data of packet number X is flagitious by an intermediate node A, B, or medial node. Regardless, packets may be corrupt sometime, e.g., due to mobility or bad channel, or maliciously, but frequently dropping packets is an obvious malicious behavior. In our future work, we will study how the AC can precisely differentiate between the undeceitful nodes and the imbecile off droppers in order to reduce the number of forthright nodes that are falsely identified as irrational droppers.

REFERENCES

1. Y. Lin and Y. Hsu, "Multi hop cellular: A new architecture for wireless communications", Proc. of IEEE INFOCOM'00, vol. 3, pp. 1273–1282, March 26-30, 2000.
2. X. Li, B. Seet, and P. Chong, "Multihop cellular networks Technology and economics", Computer Networks, vol. 52, no. 9, pp. 1825–1837, June 2008.
3. N. Salem, L. Buttyan, J. Hubaux, and M. Jakobsson, "Node Cooperation in hybrid ad hoc networks", IEEE Transactions on Mobile Computing, vol. 5, no. 4, pp. 365-376, April 2006.
4. D. Johnson and D. Maltz, "Dynamic source routing in ad-hoc wireless networks", Mobile Computing, Chapter 5, Kluwer Academic Publishers, pp. 153-181, 1996.
5. FESCIM: Fair, Efficient, and Secure Cooperation Incentive Mechanism for Multi-hop Cellular Networks Mohamed Elsalih Mahmoud and Xuemi(Sherman) Shen, *Fellow, IEEE.*
6. C. Perkins and E. Royer, "Ad-hoc on-demand distance vector routing", Proc. of IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, USA, pp. 90–100, February 1999.
7. J. B. Postel, editor. Internet Protocol. Internet Request For Comments RFC 791, September 1981.
8. Radia Perlman. Interconnections: Bridges and Routers. Addison-Wesley, Reading, Massachusetts, 1992.
9. Roy C. Dixon and Daniel A. Pitt. Addressing, bridging, and source routing. *IEEE Network*, 2(1):25–32, January1988.
10. M. FransKaashoek, Robbert van Renesse, Hans van Staveren, and AndrewS. Tanenbaum. FLIP: An internetwork protocol for supporting distributed systems. *ACM Transactions on Computer Systems*, 11(1):73–106, February 1993.

B. Sunil Kumar received the B.Tech degree in computer science engineering from the RGM College of Engineering and Technology, Kurnool and the M.Tech degree in computer science from the JNTU College of Engineering, Hyderabad. He is currently working as an Assistant Professor in Department of Information Technology in G. Pullaiah College of Engineering and Technology, Kurnool. He has published the papers in 3 International journals and 1 National Conference. He is a Life Member of ISTE.

A.ChandanaSobha pursuing her B.Tech Final Year in Information Technology in G.Pullaiah College of Engineering and Technology, Kurnool and a Member of CSI.

D.K.Sahithi pursuing her B.Tech Final Year in Information Technology in G.Pullaiah College of Engineering and Technology, Kurnool and a Member of CSI.

G.NagendraPrasad pursuing his B.Tech Final Year in Information Technology in G.Pullaiah College of Engineering and Technology, Kurnool and a Member of CSI.