Live Bandwidth Allotment LBA-MAC protocol for MANETs

M.MALA KALAIARASI , S.SEEDHANA DEVI

Lecturer , Department of Computer Engg., V S V N Polytechnic college, Virudhunagar.

Asst. Professor, Department of Computer Engg., Sri Vidya College of Engg. and Tech., Virudhunagar.

ABSTRACT

In this paper we considered the necessity to achieve a capable medium access control protocol subject to bandwidth constraints. As medium access control has a important role on the bandwidth allotment, bandwidth efficiency is one of the main concept in the design of medium access control (MAC) protocols for MANETs. Nodes are placed in an ad hoc manner, when transmitting the packets nodes will be inactive for more time, and when it becomes an active state, some characteristics of MANETs and applications motivate a MAC that is different from IEEE 802.11 in some ways like live Bandwidth allotment and self-organization are the targets. We took The significance routing protocol that makes security as wanted by providing a broad architecture of Secured PPEM Mechanism based Multi-Hop Strong Path Geographic Routing protocol (SMHSP) with effective key management, secure neighbor detection, secure routing data's, finding malicious nodes, and eliminating these nodes from routing table.. In this paper, we would implement the LBA-MAC protocol under SMHSP routing protocol and compare the performance parameters by varying number of nodes in the MANETs.

Keyword: Index Security, Routing Protocol, Mac Protocol, MANETs

1. INTRODUCTION

Many algorithms are finding the problem of fairness among senders and receivers in MANETs. Some of the algorithms, despite solving the fairness problem, suffer a significant reduction of the channel throughput, increase delay or reduce packet delivery ratio. In this paper, we proposed a new approach to solve the fairness problem in MANETs without degrading the parameter metrics. Throughput and fairness in wireless channels are inversely related, for instance, some research maximizes the throughput [1] but keeps the CW constant, while other research modifies the CW with respect to the size of the region and the state of the channel. Yet, others modify the CW with respect to the conditions of the network load. The quality of service (QoS) of the IEEE 802.11 protocol is a critical issue for some applications such as multimedia. Therefore, a key element is that we preserve the bandwidth, packet loss rate, and delay for such applications to achieve an acceptable performance in wirless networks.

The classification of the MAC protocol is into two categories. One is single and the other one is multi-channel MAC design. In single channel MAC protocols, a channel is shared by a number of nodes located in close proximity [2]. Typical examples include 802.11 DCF [3], MACAW [4], and MARCH [5]. Single channel MAC protocols are commonly used in MANET. It can achieve high bit rate. Collision avoidance is a big issue for single channel protocols since collision increases with the number of nodes. Throughput is affected if too much collision happens due to lack of bandwidth.

2. Literature Survey/Related Works

The term of contact channels and resource sharing is a necessary task for the harmonization of access among network nodes. This practice is simply managed in a central design due to the central trusted entity, which satisfies the coordination function. However, this can potentially be an issue in mobile ad-hoc networks (MANETs), where the topology lacks a central management entity. On the other hand, security is cared as the main standard in maintaining efficient communication. Therefore, designing a secure MAC protocol is essential to networks, to ensure the provision of secure communication among network nodes. There have been a more number of studies

into crentral security mechanisms in the literature. These studies tested protection, detection and authentication methods. For example, Zhu and Mao [6] looked at the issue of authentication, proposing a secure system that authenticates through a base station that grants access and provides a third party for network validation. Another technique was suggested in [7], in which the base stations of both primary and secondary nodes are utilized to provide the nodes that are connected to the base stations using a wired link. Other studies used a trust value technique of the user in previous communication, calculating the value to determine whether or not the user utilizes the channel [8] [9]. Their mechanism is applied when a genuine user has requested a new hidden channel that was not included in the Free Channel List. The legitimate user then applies the puzzle system to detect the suspicious behavior among nodes. A timing parameter technique has also been proposed [10] for the detection of malicious nodes during the negotiation stage. In this approach, if the sender is asked to locate time parameters to follow and does not obey by sending frequent packets, the legitimate user will then stop the communication and simultaneously broadcast the information about the malicious node to other nodes.

3. SMHSP Mechanism:

Our main focuses are to introduce SMHSP to protect data transmission and to construct a secured Geographic Routing protocol. Our SMHSP approach uses an ad hoc security approach so that it satisfies the main security requirement and guarantees the discovery of a proper and secure path. The security approaches that the protocol uses are the hash function, Certificates/Signatures, time synchronization and path discovery request.
SMHSP works as a group and has four stages:

- Route/Path Request Process
- Find and Remove the Attackers from The Routing table Process:
- Distribution of Certificate
- Packet Transfer Process

3.1 Route/path Request Process:

The MMD5 (modified message-digest algorithm with 256 bits) hash function is used to encrypt and update the Request packet needed for the routing process in order to secure the data request, which in this case is the first path and time to find a right unique destination, whose information uses hash chains. SMHSP uses hash chains in order to protect the mutable packet request of the first path and Td, the maximum time to find a destination, for any node in the network, including an intermediate node and the destination node, which when it receives the data can verify that the mutable data request has not been decremented by any attacker. SMHSP forms a hash chain by applying it one way. A hash function is the action whereby a node makes an RREQ and a hash function frequently to begin. The MMD5 Hash function functionality is explained briefly in next headings. Using these Request data's is being encrypted and sending to the source. The source node will have the symmetric/private key to decrypt this message to read the proper request data.

3.1.1 Working Principle of MMD5 (modified message-digest algorithm):

"MMD5 message-digest algorithm takes as input a data of random length and gives as output a 256-bit "fingerprint" or "message digest" of the input. It is conjectured that it is computationally infeasible to produce two data having the same message digest, or to produce any data having a given pre specified target message digest. The MMD5 algorithm is proposed for digital signature applications, where a big file must be "compressed" in a secure method before being encrypted with a private key under a public-key cryptosystem such as RSA. MMD5 is considered one of the most efficient algorithms. MMD5 algorithm uses four iterations, each applying one of four non-linear functions to each sixteen 32-bit segments of a 256-bit block source text. The result is a 256-bit digest. Below is a graph that illustrates the structure of the MMD5 algorithm.

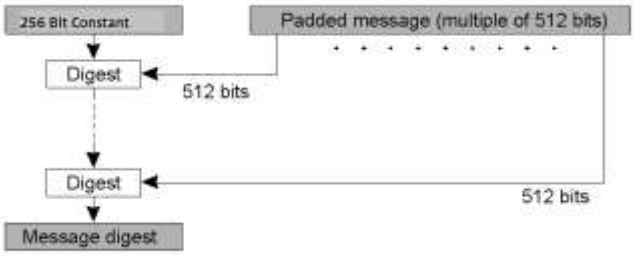

Figure 3.1.1 - Structure of MMD5 algorithm

- Join padding bits
- Join length
- Initialize MD buffer
- Process data in 16-word blocks

3.2 Find and Remove the Attackers from The Routing table:

Using the above process sender node can easily find the correct destination. And it could easily find the attacker/malicious nodes by receiving duplicate requests. It would be the strongest way to find the attackers and remove from the network by removing these nodes from routing table.

3.3 Certificates/Signatures Distribution to all the authenticated nodes:

SMHSP adopts the sender node create Certificate/Signature approach because of its power in distributing keys and achieving integrity and non-repudiation. The network uses symmetric/private and public keys. The symmetric key is used to sign the certificate/signature and the public key of all the nodes, while the public key is used to renew certificates/signatures that are issued by sender/source node. All nodes must to have verified certificates/signatures. The public keys and the corresponding symmetric keys of all nodes are created by the sender node, which also issue the public-key certificates of all nodes. Each node has its own public/Symmetric key pair. Public keys can be distributed to another node in the secure route stage, while Symmetric keys should be kept confidential to individual nodes.

Each node in SMHSP method receives exactly one certificate/signature after securely authenticating its identity to the Source node. Each node will hold its certificate in the Node Databases. The main structure of node certificates, it contains the identifier of the node, its public key, the name of the sender giving this certificate, the certificate issue and expiry dates, and the public key of the node. Finally, the contents of the certificate will be attached to the signature of the sender node. All nodes in a network should maintain fresh certificates with the sender node. At the secure route stage, nodes use their certificates to authenticate themselves to other nodes in the network.

3.4 Packet Transfer Process:

SMHSP approach is to use a PPEM algorithm to launch secure data between nodes. The Secure route Stage is found in the first process and is based on the requirement for all nodes to have a protected path with other nodes before sending any route request packet. Any node receiving an RREQ from the sender node or another node without a protected path should discard the request. In our approach, each node is given the system public key in order for any node to be able to send a Secure route Request to another node the first time the certified public keys are exchanged/distributed. The authenticity of the certificate can be confirmed as the nodes have the system public

key. The first objective is the exchange of the certified public keys and their confirmation, while its second objective is to ensure the identity of the sender before acceptance of the RREQ.

3.4.1 Working principle of PPEM (Packet Protection Encryption mechanism) Algorithm:

PPEM (Packet Protection Encryption mechanism) calculation utilizes Symmetric-keys that are a class of calculations for cryptography that utilize the same cryptographic keys for both encryption of plaintext and decoding of figure content. The keys may be indistinguishable or there may be a straightforward change to go between the two keys. The keys, in practice, speak to an imparted mystery between two or more hubs that can be utilized to keep up a private data join. Both the hubs have the right to gain entrance to the mystery key. The key size utilized for a PPEM figure details the quantity of reiterations of change adjusts that change over the data, called the plaintext, into the last yield, called the figure content.

128-Bit Key Avalanche
Plaintext Avalanche
Plaintext/Cipher text Correlation
Cipher Block Chaining Mode
Random Plaintext/Random 128-Bit Keys
Low Density Plaintext
Low Density 128-Bit Keys

Table 3.4.1 Categories of Data

The quantities of cycles of redundancy are as per the following:

10 cycles of redundancy for 128-bit keys.
12 cycles of reiteration for 192-bit keys.
14 cycles of reiteration for 256-bit keys.
16 cycles of reiteration for 128-bit keys.

Each round comprises of a few preparing steps, each one containing four comparative however diverse stages, including one that relies on upon the encryption key itself. A set of opposite rounds are connected to change cipher text go into the first plaintext utilizing the same encryption key.

3.5 LBA-MAC PROTOCOL FOR MANETS

The main objective of the proposed LBA-MAC is to allocate bandwidth to the Network users in a more dynamic manner. To this end, we propose two modifications to the MAC: one is Dynamic Bandwidth allo tment (DBA) and other one is Transmission Interval Setting. Through the proposed designs, LBA-MAC not only can support more complicated network cases, but can also further utilize the spectrum holes in a more effective way. In first phase the LBA-MAC, we proposed a DBA such that the Network users are not limited to transmit only pre-defined packets. To this end, we defined several new variations of packets, namely MAX PACKET, bandwidth demand of Network sender (NS) and bandwidth demand of Network receiver (NR). Similarly, the MAX PACKET is a pre-defined network parameter. However, instead of representing the number of packets that can be transmitted by each user/node, it refers to the maximum number of packets that is allowable to be transmitted by a user/no de pair when both Network users are on the data channel. On the other hand, the NS and NR refer to the number of

packets to be transmitted by the Network sender and Network receiver, respectively. Considering that a Network may carry asymmetric traffic flows between a user/node pair, the values of NS and NR are dynamically decided during the BNP on the control channel. These values are carried in the control packets, i.e., REQ and GRANT. To this end, we extend the REQ and GRANT with a 5-bit field of NS or NR. With the allocation of this 5-bit field, each user/node can request up to a maximum of 31 transmission opportunities. The remaining three bits are left unused for possible future extension. The DBA of LBA-MAC operates in the following way. Firstly, we assume that a Network sender maintains a separate queue for every Network receiver. Before sending an REQ, the Network sender gets the number of packets to be transmitted to a specified Network receiver by retrieving the current size of the corresponding queue. This information is treated as the value of NS in the REQ and shall be set using the following equation:

$$NS = \begin{cases} CQs, \text{ if } CQs \leq MP \\ MP, \text{ if } CQs > MP \end{cases} \quad (1)$$

Where CQs denotes the current queue size of the Network sender (for the specified Network receiver) and MP denotes the pre-defined and fixed network parameter MAX PACKET. Upon receiving the REQCR, the Network receiver checks the corresponding queue that contains packets to be sent to the Network sender and then decides the value of NR using Eq. 2. At the same time, the Network receiver also records the value of NS as the number of packets to be received from the sender (NPRs) using Eq. 3. After that, it replies a GRANT to the Network sender.

$$MR = \begin{cases} 0, \text{ if } Qr = 0 \\ MP - NS, \text{ if } CQr \geq \lfloor A \rfloor \text{ and } NS \leq \lceil A \rceil \\ \lfloor A \rfloor, \text{ if } CQr \geq \lfloor A \rfloor \text{ and } BDs \geq \lceil A \rceil \\ CQr, \text{ if } CQr \leq \lfloor A \rfloor \end{cases} \quad (2)$$

Where NR denotes the size of the queue containing packets to be sent to the Network sender and A denotes M/2.

Where BSF denotes the finalized value of NS at the end of the BNP. Using our proposed DBA, the LBA-MAC can offer very high flexibility in allocating bandwidth to the user/node pair regardless of their traffic condition. Through maintaining the NS, NR, NPRs and NPRr, LBA-MAC can support (1) a uni-directional traffic flow from the Network sender to the Network receiver, (2) a bidirectional traffic flow where both the user/node sender and the Network receiver have the same number of packets to send in their queues, and (3) a bi-directional traffic flow where the user/node sender and the Network receiver have unequal numbers of packets to send in their queues. In case (3), the user/node pair will swap their sender/receiver identities on the data channel when the Network sender has transmitted all packets in its queue but the Network receiver still has packets to send in its queue. At this moment, the bi-directional traffic flow temporarily degenerates to a unidirectional traffic flow.

In phase two of the LBA-MAC, we proposed STIS such that the TI to be carried in the control packets can provide the neighboring PUs with the correct timing information when bi-directional bandwidth reservation is needed. In a typical 802.11 network, a two-way handshake of RTS/CTS is adopted for bandwidth reservation. In the process of handshaking, the TI is carried in the RTS packet to indicate how long a sender wants to hold the medium. In return, the receiver replies with a CTS packet echoing the expected duration of transmission. Through the exchange of RTS and CTS control packets, all the nodes within the hearing distance of either the sender or receiver or both will set their Network Allocation Vector (NAV) according to the TI in the overheard packets. In the presence of bi-directional traffic flow, we further proposed a conditional transmission of RTSe by the Network sender after receiving a CTS. As a result, the Network sender can effectively update all of its neighboring PUs with its latest TI whenever bi-directional bandwidth reservation is required.

To sum up, through the proposed DBA, the LBA-MAC can maximize the achievable throughputs in a Network by minimizing the frequency and overhead of Network users switching from the control channel to the data channel and vice versa in presence of bi-directional flows. Also, through the STIS, the LBA-MAC can broadcast correct information of TI to all neighboring nodes of a user/node pair to avoid unnecessary packet collisions.

3.6 SIMULATION PARAMETERS AND PERFORMANCE ANALYSIS

Network simulator (NS2) is used to simulate all types of network. It is a discrete event driven simulator and start packet sending for specified time. Results are generated in the form of graph. Performance metrics are evaluated to check QoS of a presented protocol.

Channel	Channel/Wireless
Network Interface	Wireless
NS Version	NS-2
CBR Packet Size	512 bytes
MAC	LBA-MAC
Routing Protocol	SMHSP
Interface Queue	Priority Queue
Queue Length	100
No. of Nodes	50
Simulation Area Size	800x800
Simulation Duration	20sec
Packet Rate	1000k

Packet delivery ratio is the percentage of ratio between the number of packets sent by sources and the number of received packets at the sink or destination. Higher the packet delivery ratio better is the performance of the network

Throughput is the average rate of successful message delivery over a communication channel which is measured in bits per second i.e. bps.

End to end delay is a time required for packets to reach to destination node from source node. Lower the end-to-end delay better is the performance of the network.

3.6.1 Simulation Result

In this phase, the performance data of four routing protocols (TORA, ARIADNE, TESLA and SRAAA) are collected. A scenario is set up for data collection. This scenario is run 11 times with 11 different values of the mobility pause time ranging from 0 to 100 seconds. The data is collected according to two metrics – Packet Delivery Fraction and Normalized Routing Load. In general, the actual values of the performance metrics in a given scenario are affected by many factors, such as node speed, moving direction of the nodes, the destination of the traffic, data flow, congestion at a specific node, etc. It is therefore difficult to evaluate the performance of a protocol by directly comparing the acquired metrics from individual scenarios. In order to obtain representative values for the performance metrics, we decided to take the average values of multiple simulation runs. The average values of these 11 simulation runs are then calculated for the two metrics and used as a baseline to evaluate the performance of routing protocols in malicious environments.

The Graph Shown in comprises the results of Throughput with no of node taking Throughput along Y-axis and No of node along X-axis. This graph shown in Figure indicates the throughput values for different number of nodes. We are comparing the proposed protocol SRAAA with the Existing protocol TELSA, TORA and ARIADNE.

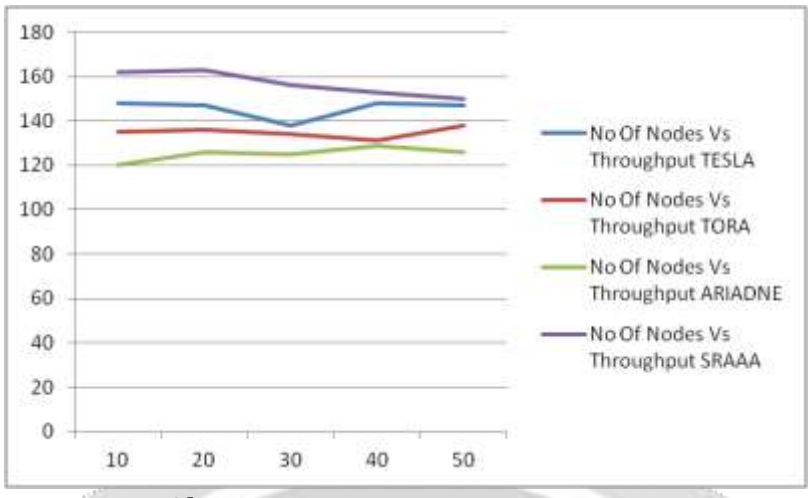

Chart 1 Simulation Result of Node Vs Throughput

The throughput outcome is good when compare with all other protocol. We obtained the transmission range of TX Range and the carrier-sensing range by similar approaches. We fixed the information table of each node and set the distance between successive nodes with the help of smart secured route using SRAAA.

SRAAA improves 11% of the throughput in terms of Number of nodes when compared with all other protocols.

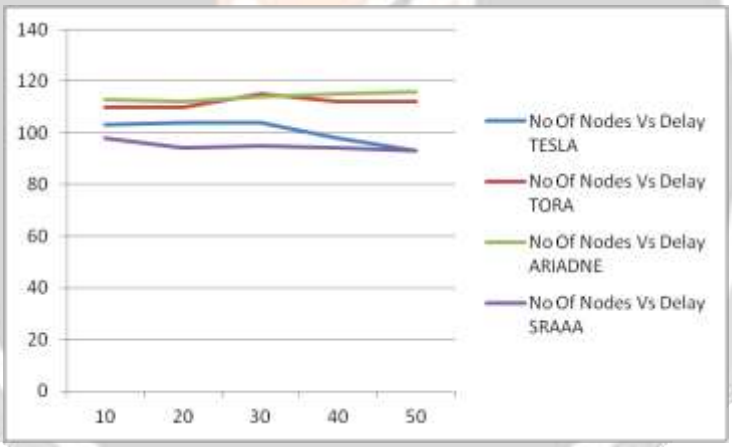

Chart 2 Simulation Result of Node Vs Delay

The Graph Shown in comprises the results of delay with No of node, taking node along X-axis and Delay along Y-axis. Graph indicates the Delay values for different number of nodes.

We are comparing the proposed protocol SRAAA with the Existing protocol TELSA, TORA and ARIADNE. The Delay outcome is good when compare with all other protocol we measure the effect of change in number of nodes on packet delay. Each experiment is executed for 10ms. Delay from initial transmission of packet from source until packet is received at destination.

We can speculate that the reason is in the fact that small frame size results in larger number of frames, which in turn results in more dequeue attempts and more collisions and bakeoffs.

Smart secured route is used to reduce the delay with avoiding the waiting time Graph demonstrates the above point by measuring pure network delay (which excludes delay at the buffer). The buffer delay is the major factor in causing packet delay, while network delay is the minor factor.

SRAAA improves 10.6% of the delay in terms of Number of nodes when compared with all other protocols.

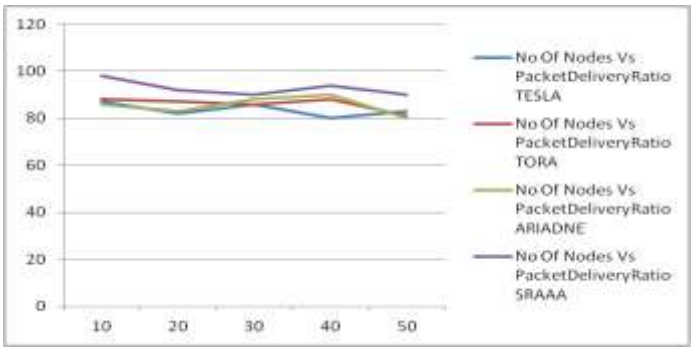

Chart 3 Simulation Result of Node Vs Packet Delivery Ratio

The Graph Shown in comprises the results of Packet Delivery with No of node, taking node along X-axis and PDR along Y-axis This graph indicates the PDR values for different number of nodes. We are comparing the proposed protocol SRAAA with the Existing protocol TELSA, TORA and ARIADNE. The PDR outcome is good when compare with all other protocol. Graphs show the fraction of data packets that are successfully delivered during simulations time versus the number of nodes. Performance of the ARIADNE is reducing regularly while the PDR is increasing in the case of TORA and TELSA. SRAAA is better among the three protocols. SRAAA improves 9.5% of the Packet delivery ratio in terms of Number of nodes when compared with all other protocols.

4. CONCLUSION

In this paper, we proposed LBA-MAC protocol for Networks over 802.11 networks. The proposed LBA-MAC can reserve bandwidth dynamically to further utilize the spectrum holes of the authorized bandwidth. In addition, the LBA-MAC can support asymmetric two-way traffic flows with variable packet sizes. Simulation results show that our proposed LBA-MAC can significantly enhance the aggregate throughputs of Nodes in a Network and dramatically improve the spectrum efficiency without degrading the performance in SMHSP routing.

5. REFERENCES

[1] SachinGarg, Martin Kappes, and A. S. Krishnakumar, "On the Effect of Contention- Window sizes in IEEE 802.11b Networks,"Technical report, Avaya Labs Research, June 2002.

[2] Z. J. Haas and J. Deng , "Dual Busy Tone Multiple Access (DBTMA)-A Multiple Access Control Scheme for Ad Hoc Networks," IEEE Trans.on Communications, vol. 50, no.6 pp. 975 – 985, June 2002.

[3] LAN/MAN Standards of the IEEE Computer Society, Wireless LAN medium access control (MAC) and physical layer (PHY) specification. IEEE standard 802.11, 1999 Edition, 1999.

[4] V. Bharghavan, A. Demers, S. Shenker and L. Zhang, "MACAW: A Medium Access Protocol for Wireless LANs, Proc. of ACM SIGCOMM 1994, pp. 212-225, Aug. 1994.

[5] C. K. Toh, V. Vassiliou, G. Guichal and C. H. Shih, "MARCH: A Medium Access Control Protocol for MultiHop Wireless Ad Hoc Networks," Proc. of IEEE MILCOM 2000, vol.1, pp. 512-516, Oct. 2000.

[6] L, Zhu., and H, Mao. (2010) "Research on authentication mechanism of cognitive radio networks based on certification authority", in Computational Intelligence and Software Engineering (CiSE), 2010 International Conference on, 2010, pp.1-5

[7] S, Parvin., and F, Hussain. (2011) "Digital signature-based secure communication in cognitive radio networks", in Broadband and Wireless Computing, Communication and Applications (BWCCA), 2011 International Conference on

[8] S, Parvin., S, Han., B, Tian., and F, Hussain. (2010) "Trust-based authentication for secure communication in cognitive radio networks", in Embedded and Ubiquitous Computing (EUC), 2010 IEEE/IFIP 8th International Conference on, 2010,

[9] S, Parvin., S, Han., F, Hussain., and M, Al Faruque. (2010) "Trust based security for cognitive radio networks" in IiWAS '10 Proceedings of the 12th International Conference on Information Integration and Web- Based & Services, 2010, pp. 743-748

[10] R, Shaukat., S, Khan., and A, Ahmed. (2008) "Augmented security in IEEE 802.22 MAC layer protocol", in Wireless Communications, Networking and Mobile Computing, 2008. WiCOM '08. 4th International Conference, pp. 1-4