www.ijsrnsc.org

Available online at www.ijsrnsc.org

IJSRNSC

Volume-1, Issue-1, Apr- 2013
Review Paper

Int. J. Sci. Res. in Network Security and Communication
ISSN: 2321-3256

Secured position based Grid Location Service for MANET Using SGF

M. Buvana*[1], M. Suganthi[2], K. Muthumayil[3]

*[1]PSNA College of Eng. &Tech, Kothandaraman nagar,Dindigul, Tamilnadu,INDIA, bhuvana_beula@yahoo.co.in
[2]Thiagarajar College of Engineering,Madurai, Tamilnadu INDIA, msece@tce.in
[3]PSNA College of Eng. &Tech, Kothandaraman nagar,Dindigul, Tamilnadu,INDIA, muthumayil@yahoo.com

Received: 15 Jan 2013 Revised: 05 Feb 2013 Accepted: 02 April 2013 Published: 30 Apr 2013

***Abstract*— Position based routing protocols can offer a significant performance increase over traditional ad hoc routing protocols. Correctness of location messages. These routing protocols use geographical information to make forwarding decisions, resulting in a significant reduction in the number of routing messages. However, current position aided routing protocols were not designed for use in high-risk environments, as position information is broadcasted in the clear allowing anyone within range, including the enemy, to receive. We introduce "Secure Position Based Grid Location for Ad hoc Routing" (SPBGLAR), a routing protocol designed to use protected position information to improve security, efficiency, and performance in MANET routing. We propose a secure geographic forwarding (SGF) mechanism, which provides source authentication, neighbour authentication, and message integrity by using both the shared key and the TIK protocol. By combining SGF with the Grid Location Service (GLS), we propose a Secure Grid Location Service (SGLS) where any receiver can verify the correctness of location messages.**

Keywords— Position Based, Geographic Location, Ad-hoc, Grid

I. INTRODUCTION

MANET is multi-hop infrastructure less network which is characterized by dynamic topology due to node mobility, limited channel bandwidth and limited battery power of nodes. Current research on Mobile Ad hoc Network (MANET) mainly focuses on topology-based routing protocols, including both proactive and reactive (on-demand) approaches [1]. When network topology changes frequently or the network size increases, some of these protocols may incur a significant amount of routing control overhead. Recent research has shown that position-based routing protocols can be good alternatives to topology-based routing protocols in large and dense MANETs [2]. By using Location Information (LI), position-based routing protocols avoid the flooding of control traffic. An intermediate node only needs to know its own position and the positions of its neighbouring nodes to make a message forwarding decision. The message is forwarded to a neighbor that is geographically closest to the destination [3–5]. To implement a position-based routing protocol, information about the geographical location of each destination must be available. Each node can determine its own position by using the Global Positioning System (GPS), or its relative position by using GPS free positioning methods [6]. A location service [7–9] is used by the sender to determine the location of the destination. Three major components of location service.

- ➢ Location update
- ➢ Location request
- ➢ Location response

Centralized Location server is not practical, because a single centralized server maintains locations of the entire participating node. So, Distributed approach is more suitable Each participating nodes normally manage locations of some other nodes. Every node has assigned a position server and must periodically report its position Retrieve the position of a destination node from the corresponding location server.

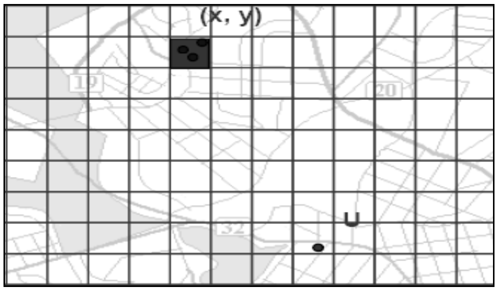

Fig. 1(a)

Geographical area divided into "grid squares". Node U's ID is hashed to produce (x location x, y) location. Every node has a table containing location server address.

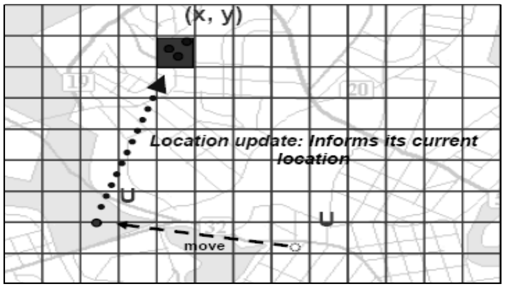

Fig. 1(b)

*[1]Corresponding Author: M Bhuvana

For example, Node U moves out of its current region and into a new one. Node informs its current location information to its location server by using location update (LU) message. (Unicasts).

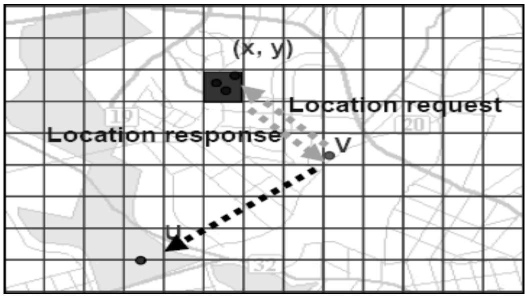

Fig.1(c)

Node V wishes to communicate with U. Node V determines LS from ID of U and hash and then unicast location request. The first node in LS responses to node V with node U's location unicasts towards U.

In position-based routing, the forwarding decision is based on LI contained in messages. Attackers can alter the LI in messages to disrupt the operation of a unicast forwarding scheme (i.e., message tampering attack). As shown in Fig. 2(a), assume two paths exist between B and A via C (i.e., path BCEA and path BCFDEA). When a node C receives a message m from B, it can modify the LI of A and forward modified message m' to other colluding node D via node F. When node D receives m', it will return re-modified message m'' to C again, and so on. This makes a routing loop where messages traverse nodes in a cycle without being relayed to the real destination A.

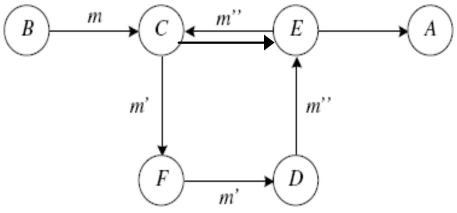

Fig:1.2(a)

The Grid Location Service (GLS) [7] is a distributed location service which calls for nodes to maintain location of specific subsets of the nodes based on the node's identifier (ID) as shown in Fig.1.2.(a) GLS divides the area that contains a MANET into a hierarchy of squares. Each node periodically broadcasts a list of neighbours using a HELLO message. Therefore, each node can maintain a table of immediate neighbours as well as each neighbour's neighbours. Each entry in the table includes the node's unique ID, location, speed, and a timestamp. Each node recruits nodes with IDs ''close'' to its own ID to serve as its Location Servers (LSs) (i.e., least ID greater than A) by sending Location Update (LU) messages. Any attacker may modify the location update (LU) message and generate a falsified message LU' with the latest timestamp (i.e., falsified message injection attack). As a result, even a single attacker can cause other nodes to fail to find a route to source if they are more than one hop away from source.

If position information can be safely protected, it can be used to improve the efficiency and security of MANET routing. We introduce "Secure Position Based Grid Location for Ad hoc Routing" (SPBGLAR) as a method to protect position information in a high-risk environment.

The objective of this paper is to provide security mechanisms for both data and control messages in position-based routing protocols. The main contributions of this paper are as follows.

We propose a secure geographic forwarding (SGF) mechanism that incorporates both the Hashed Message Authentication Code (MAC) and the Timed Efficient Stream Loss-tolerant Authentication (TESLA) with Instant Key disclosure (TIK) protocol. In combination with SGF, we propose a Secure Grid Location Service (SGLS) where any receiver can verify the correctness of location messages.

This paper is organized as follows, In Section 2 we discuss the target environment for SPBGLAR. Section 3 overviews related working secure routing and position aided routing. In Section 4 we present the details of SPBGLAR and with a brief discussion and conclusion, in Sections 5 and 6.

II. SPBGLAR ENVIRONMENT

Our goal is to satisfy the following set of security requirements,

1. Outgoing routing messages cannot be injected into network by malicious nodes
2. Routing messages cannot be altered in transit by malicious nodes.
3. No malicious routing loops can be formed
4. Routes cannot be redirected from the shortest path (or ideal path) by malicious nodes.
5. Unauthorized nodes should be excluded from route computation and discovery.
6. Network topology must not be exposed to adversaries or to unauthorized nodes by routing messages.

SPBGLAR protects a MANET from attacks by malicious nodes, while attempting to minimize the potential for damage by attacks originating from compromised nodes. Position-based routing brings two new threats:

- False location update attack:

An attacker may try to update the location of another node causing the server to maintain false location.

- False location response attack:

An attacker may try to alter the response from a server causing a node to receive wrong location of another node.

In order to defend against these attacks Authentication of the sender and authentication of update and response messages must be provided with self-signed locations.

III. RELATED WORK

3.1 Secure Routing Protocols

Ad hoc network research has produced numerous routing protocols, some of which are under consideration.

3.1.1 Secure Routing Protocol (SRP)

SRP requires a security association between the source and destination nodes. As shown in Figure 1, SRP uses a route field in LREQ and LREP packets. Each intermediate node appends its identifier to the route field as a routing packet propagates from the source to the destination.

In [11] & [12], Marshall points out a weakness in SRP and presents an attack. The premise of Marshall's attack is that a malicious node M may forward a LREQ without appending its address to the address field of the SRP header, effectively making itself invisible in the path returned to the source. As Figure 2 illustrates, the result is the source node erroneously believes that a path exists to a destination that is not dependant on M.

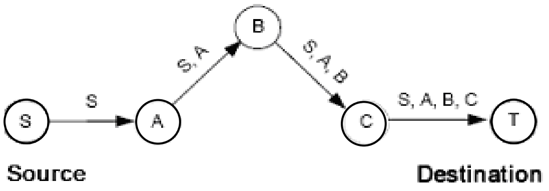

Fig (3.1)

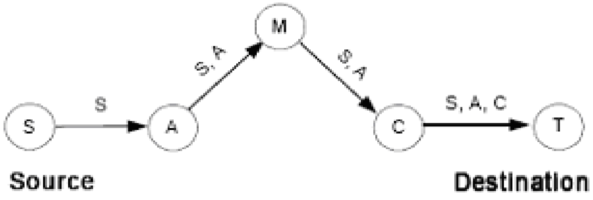

Fig (3.2)

Initially, one might question the significance of this "invisible node" attack. While [11] describes the attack in detail, little is mentioned of possible effects. One consequence of this attack could be fooling S into using a path that appears ideal, but may not have appeared ideal if the malicious node (or nodes) was visible. For example, suppose SRP was being used as and extension to a shortest path routing algorithm that measured path length as the number of hops. In this case, S may decide to use a path that appears to be the shortest, but in actuality is not because one or more hops are invisible in this path due to malicious nodes. This scenario is illustrated in Figure 3.

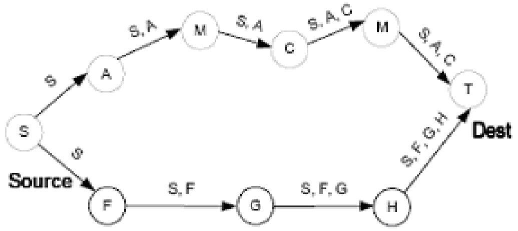

Fig (3.3)

In Figure 3.3, the true shortest path (SFGHT) requires four hops. However the source node will not choose this path because it believes in the false path of 3 hops (SACT). If S does choose this path, the malicious nodes could then negatively impact network performance by intentionally delaying packing or dropping packets. Despite the poor performance, the base protocol may continue to choose this path as ideal since it appears to be the shortest route.

IV. SECURE GEOGRAPHIC FORWARDING (SGF)

Our proposed secure protocols aim to protect the network layer from attackers. Our proposed schemes work under several assumptions as follows:

4.1 Network environments and assumptions:

Nodes are assumed to be located uniformly in the given network. The following notations are used in this paper:

TABLE I
NOTATIONS OF SECURITY ATTACKS

A	The identifier of node A
A PK	The public key of node A
A PR	The private key of node A
Sig A(msg)	A's signature on message M using
T AI	The timestamp representing the time APR was first generated.
T AC	the timestamp representing the current time generated by A.
pos A	A's geographical location (coordinate) obtained from GPS.
Loc A	The self-signed geographical location of node A. Loc A = Sig A(A||pos A || T AC|| T AI)

4.1.1 Secure geographic forwarding for unicast messages

We propose the use of MAC computed over the non-mutable part (e.g., LI of a destination) of unicast messages with the pair-wise shared secret key between the source and destination. Since intermediate nodes do not have the shared secret key with the source node, they cannot verify the non-mutable part of messages. This allows a compromised user to be able to modify the non-mutable part of messages to disrupt the operation of position-based routing protocol. To prevent this attack, source node can use the digital signature over the non-mutable part with its own private key instead of MAC. However, implementing a mechanism to sign the non-mutable parts of all data and control messages may introduce too much overhead. In our scheme, we propose the use of a reputation system (see Section4) to detect and isolate message tampering and drop-ping attackers instead of using expensive digital signatures.

V. PROPOSED PROTOCOL

In our scheme Nodes generate a public key pair and registers its public key in other nodes when it joins the network. If the majority of the nodes are honest, then this process will be sufficient to provide a safe public key environment. A node updates its position by sending its location digitally signed and a node receives this digitally signed location when requesting other node's location.

5.1 Secure grid location service

In this section, we describe our proposed SGLS protocol based on SGF. SGLS provides several security mechanisms to the original GLS.

Registration and Initialization:

We propose the following public announcement method

Step1. Generates a public key pair & Creates a self-signed certificate $Cert_A$=Sig_A (A, Apk, TAI)

Step2. Broadcast the following public key registration message

PK_init= [Type, Seq, width, $Cert_A$, Loc_A]

When a message is broadcasted there are two ways to process the message.

Method 1 A node receiving the message unconditionally stores the certificate.

Method2. A node receiving the message stores the certificate if source location is within certain boundary.

Location update

A node broadcast a location update message When it moves to a certain distance from the previous location or if a certain time has elapsed from the last update.

5.2 The Neighbor Table

In SPAAR, each node maintains a neighbor table that contains the identity and position information of each verified neighbor, along with the cryptographic keys required for secure communication with each neighbor. A node will only accept routing messages from a node in its neighbor table. Specifically, each node maintains two keys for each neighbor. The first is the public key of the neighbor that is acquired from its certificate. The second is the neighbor's group decryption key that is used to decrypt LREQs, table update messages, and other routing messages encrypted with a group encryption key.

The position information is in the form of the Neighbor's most recent location, represented as latitude, longitude coordinates, along with the neighbor's transmission range. Finally, each entry contains the neighbor's Table Update Sequence Number for use in the table update process.

5.2.1 Neighbor Table Creation

Step 1: A node N periodically broadcasts a "hello" message with its certificate. Nodes within range of N wishing to be recognized as neighbors decrypt N's certificate to verify and obtain N's public key. An entry for N is created in their neighbor table and N's public key is stored. Nodes respond with their certificate, coordinates, and transmission range encrypted under N's public key.

Upon receiving a hello response from a neighbor node X1, N verifies that X1 node is a one-hop neighbor. For all nodes that N verifies as one-hop neighbors, N stores the node's public key, most recent location, and transmission range in N's Neighbor Table.

Step 2: N generates a public/private key pair, which we call a Neighbor Group Key pair. The private part of N's neighbor group key pair is called N's group encryption key and denoted GEK_N. The public part of node N's neighbor group key pair is called N's group decryption key, denoted GDK_N. N distributes its group decryption key to each of his neighbors listed in the neighbor table.

The key is signed with N's private key to provide authentication, and encrypted under the neighbor's public key. Upon receiving the N's group decryption key, N's neighbors store it in their neighbor table. It is important to note that at this point, X1 and X2 have the capability to accept routing packets from N, however they will not do so until they have verified N as a neighbor. This will occur after X1 and X2 broadcast a "hello" message and the above steps take place. This table state will last, at most, the time between "hello" broadcasts of X1 and X2.

5.2.2 Neighbor table maintenance

5.2.2.1 Table update messages and TUSN

Each node periodically broadcasts a "table update" message to inform the neighbors of its new position coordinates and transmission range. Table update messages are encrypted with a nodes group encryption key. Neighbors of N decrypt the table update message, analyze the new position information to verify that the neighbor is still a one-hop neighbor, and update their neighbor table with the new position information. TUSN is a time stamped sequence number that is incremented each time N broadcasts a table update message or constructs a LREP containing its position information. Representing the "freshness" of location information, the TUSN prevents table update message replay attacks. In the LREQ a node uses the TUSN to inform its neighbors how fresh the coordinates are that it possesses for the destination. When a table update message is received, the TUSN is time stamped allowing the node to determine how much time has passed since it has received a table update from its neighbors. After a timeout period has elapsed without a table update from a neighbor, the link is assumed to be broken and the neighbor is deleted from the table.

The interval at which a node broadcasts a table update depends on its mobility rate. A node with a high mobility rate broadcasts table update messages more frequently inan effort to keep its neighbors up-to-date. To offset the overhead involved with such a proactive approach, table update messages are piggybacked on all routing messages encrypted with a node's neighbor group key (LREQ &location request messages).

5.2.2.2 Hello messages

All nodes broadcast periodic "hello" messages to add nodes to the neighbor table. A node receiving a "hello" message from N, checks to see if N is already in its neighbor table. If so, the node then checks to see if the "NGK" field has a value. If the node has a value for node N's NGK field, it is already in N's neighbor group and will ignore the "hello" message. If a node does not have N in its neighbor table, or has no value for N's NGK field in the neighbor table, it sends a "hello response" message as described above. As with table updates, the interval between hello messages is dependent on node mobility.

5.3 Location Discovery

5.3.1 Location Requests (LREQ)

Step 1: Node N broadcasts a LREQ with the LREQ sequence number, the destinations identifier, N's distance to D, D's coordinates and TUSN, all encrypted with its group encryption key. The LREQ sequence number is incremented each time a node initiates a LREQ. It is used to prevent replays of LREPs.

Step 2: LREQ recipients decrypt it with the appropriate group decryption key. Successful decryption implies that the sender of the LREQ is a one-hop neighbor. The identifier in the decrypted LREQ should match that of the neighbor whose group key was used to decrypt the LREQ.

Step 3: An intermediate node checks to see if it, or any of its neighbors, is closer to destination D. If an intermediate node has the destination's coordinates with a more recent TUSN, it uses those coordinates instead of the coordinates contained in the LREQ. If neither the intermediate node nor its neighbors are closer to the destination, the LREQ is dropped. If either is closer, the node forwards the LREQ with its identifier and distance to S, encrypted with its group encryption key. If the intermediate node had the destinations coordinates with a more recent TUSN, those coordinates replace the older coordinates in the LREQ. Intermediate nodes record in their route cache the address of the neighbor from which they received the LREQ, thereby establishing a reverse path. This process is repeated until the destination is reached.

Loc_request=[Type,Seq,A, LocB]

5.3.2 Route Replies (LREP)

Step 1: Upon receiving a LREQ, the destination constructs a LREP containing the LREQ sequence number, its coordinates, its velocity, and a TUSN. It then signs the LREP with its private key and encrypts it with the public key of the neighbor it received the LREQ from. The LREP propagates along the reverse path of the LREQ, being verified at each hop.

Step 2: Intermediate nodes, upon receiving a LREP, decrypt it with their private key and verify the signature with the public key of the neighbor node they received it from. Next, they setup forward entries in their route table that point to the node from which the LREP came. Intermediate nodes sign the LREP and encrypt it with the public key of the next node in the reverse route.

Step 3: The source node receives the LREP with the destinations location, velocity vector, and a TUSN. After successful decryption and signature verification, the source node verifies that the LREQ_SN matches the LREQ_SN from the initial LREQ. This prevents LREP replay attacks.If the LREQ_SN is correct, the node updates its destination table with the new destination position information. As with table update messages, the source node time stamps the TUSN as an update history. location response message in the form of

Loc_response=[Type,Seq, LocB, LocA, Locc]

5.4 Error Alarm :

When a node A receives a message, it verifies the signature included in the message in the following ways,

Policy 1. A message is verified every h hops.

Policy 2. Every node randomly determines by itself whether it will verify the message or not.

Policy 3. A node verifies a message only if it has the required certificate.

If the message is invalid invalid, it broadcasts the following message in the reverse direction:

Err_alarm=[msg, SigA (msg)], where msg

(Type,Seq,err_Type)

Nodes receiving this message must verify the validness of this message and perform necessary actions such as removing the previous location update and changing the reliability of a node.

VI. ANALYSIS OF PUBLIC KEY REGISTRATION

Nodes cannot determine whether the received certificate is valid or not, they accept the registration unconditionally.

In case this case, we have to consider the outcome of the following attacks.

Attack 1. Someone else has already register a public key using the same ID as the current one.

Attack 2. Someone else may later try to register a public key one using the same ID as the current one.

Attack 3. Someone may simultaneously send a registration message using the same ID as the current one in a different location.

Attack 4. Someone swaps the public key in the current message forwards message with another one and forwards the altered message.

Security against Attack Threat

If the PKI used in our protocol is secure, our new location service is robust against various attacks.

update False location attack/False response attack

we used self-signed locations. Therefore, without acquiring the private key of a certain node one cannot generate a false but valid self-signed location.

Replay attack:

Old replayed messages will be discarded using the timestamp included in that message.

Blackmail attack:

This kind of attack is related to false error alarm messages. Nodes receiving an error alarm message will verify that msg. Therefore nodes can detect a false error alarm.

Invisible node attack:

In assumption, all nodes should have a equal distance and speed factor. A message received at the end of destination node that verify the distance factor to identify the malicious node which is appear along the route path.

VII. CONCLUSIONS

In this paper, we have proposed SGLS, which is a security enhancement to the original GLS protocol. The security mechanisms added to GLS include TIK, TESLA, MAC, digital signature, and a reputation system. SGLS has the capability of preventing message tampering, dropping, falsified injection, invisible attack and replay attacks. For future work, we are planning to implement our algorithm on mobile devices, and study it in real world environments by taking into account the energy issues. Moreover, countermeasures against blackmail attacks will be investigated. The protected position information is used to reduce routing overhead and increase the security of routing, resulting in a protocol with performance comparable to that of traditional MANET routing protocols and secure enough for use in high-risk environments.

REFERENCES

[1]. X. Hong, K. Xu, M. Gerla, Scalable routing protocols for mobile ad hoc networks, IEEE Network 16 (4) (**2002**) **28–39**.

[2]. Shivlal Mewada, Umesh Kumar Singh and Pradeep Kumar Sharma, " Simulation Based Performance Evaluation of Routing Protocols for Mobile Ad-hoc Networks (MANET)", IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), Vol. 2, No. 4,August **2012**

[3]. E. Kranakis, H. Singh, J. Urrutia, Compass routing on geometric networks, in: Proc. Canadian Conference on Computational Geometry, Vancouver, BC, August **1999**.

[4]. G.G. Finn, Routing and addressing problems in large metropolitan-scale internetworks, Technical Report ISI/RR-87-180, Inst. for Scientific Information, March **1987**.

[5]. S. Basagni, I. Chlamtac, V.R. Syrotiuk, B.A. Woodward, A distance routing effect algorithm for mobility (DREAM), in:Proc. ACM MobiCom, Dallas, TX, October **1998**.

[6]. S. Capkun, J.-P. Hubaux, Secure positioning of wireless devices with application to sensor networks, in: IEEE Proc. IEEE Infocom, Miami, Florida, March **2005**.

[7]. Umesh Kumar Singh, Shivlal Mewada, Lokesh Laddhani & Kamal Bunkar,“an Overview & Study of Security Issues in Mobile Adhoc Networks”,Int. Journal of Computer Science and Information Security (IJCSIS) USA, Volume-9, No.4, pp (106-111), April **2011.**

[8]. Z.J. Haas, B. Liang, Ad hoc mobility management with uniform quorum systems, IEEE/ACM Transactions on Networking 7 (2) (**1999**).

[9]. L. Blazevic, L. Buttyan, S. Capkun, S. Giordaro, J.-P. Hubaux, J.-Y. Le Boudec, Self-organization in mobile ad hoc networks: the approach of terminodes, IEEE Communications Magazine (June) (**2001**).

[10]. John Marshall, An Analysis of SRP for Mobile Ad Hoc Networks, Proceedings of The 2002 International Multi-Conference in Computer Science, Las Vegas, USA, **2002**.

[11]. Y. Hu, A. Perrig, D. Johnson, “Wormhole Detection in Wireless Ad hoc Networks,” Rice University Department of Computer Science, Technical Report TR01-384, **2001**.

[12]. Jinyang Li, John Jannotti, Douglas S. J. De Couto, David R. Karger, and Robert Morris, A Scalable Location Service for Geographic Ad Hoc Routing, Proceedings of the 6th International Conference on Mobile Computing and Networking, Boston, USA, **2000, 120-130.**