PEUC-WiN: Privacy Enhancement by User Cooperation in Wireless Networks

Karim El Defrawy and Claudio Soriente
University of California, Irvine
{keldefra,csorient}(at)uci.edu

Abstract

Location awareness capabilities of today's wireless networks provide position tailored services but, at the same time, impose serious privacy implications for the wireless users. Interface identifiers allow an adversary to trace a user's movement and location over time in a wireless environment. This causes a significant privacy threat to users, since an adversary could learn a lot of information about them from their locations. Current proposed location privacy mechanisms suffer from a high rate of network disruption and degraded throughput. In this paper, we introduce a new scheme to improve the location privacy of wireless users while minimizing network disruption. The proposed scheme achieves its goals by exploiting the collaboration among users in the same coverage area of an access point in a wireless system.

1. Introduction

IEEE802.11 has become a popular standard for implementing wireless local area networks (WLANs). Such networks can be found in malls, airports, campuses and factories around the world [14]. While communication confidentiality issues in wireless networks can be efficiently solved with means similar to those used in their wired counterparts, user mobility raises new location privacy risks that must be addressed at each layer of the protocol stack. Several technologies, such as the one proposed by Bahl and Padmanabhan, [3], allow detection of the location of a wireless user based on the transmitted signal strength and the received signal to noise ratio. Such attacks are very difficult to thwart because they utilize mechanisms needed by the physical layer of wireless systems for correct operation. On the other hand, signal to noise ratio computation and triangulation can only be performed with special hardware. Going up the stack, less sophisticated attacks are feasible with less capabilities, allowing an adversary to learn information about the users. Layer two, three and four identifiers allow linkage of different communication sessions to the same user and facilitate user traceability over time. One drawback of currently proposed schemes [7], [9] is that they represent impractical trade-offs between performance and privacy. These schemes require, for a user to prevent being traced, shutting down all active TCP connections, remaining silent for a random amount of time and then setting up all the connections again. As the reassociation process with the access point (AP) may take up to 2.5 seconds [10], this process is not pursuable with applications characterized by a high traffic volume such as file transfers or with other applications that require the connection to be kept alive for the duration of the session, such as remote logins or real time applications such as voice over IP. In this paper, we introduce PEUC – WiN a new scheme that prevents user traceability with minimal network disruption. PEUC – WiN takes advantage of features derived from Mobile IP [16] and utilizes cooperation between users in the same coverage area of an untrusted AP. The rest of the paper is organized as follows. Section II reviews related work. Section III introduces the details of PEUC – WiN and section IV provides its security analysis. Simulation results comparing PEUC – WiN to other schemes are presented in Section V while section VI gives the future directions and our conclusion.

2. Related Work

In [7] a scheme is introduced that uses frequent disposal of the client's interface identifiers to enhance location privacy. This scheme requires each user to use short-lived, disposable MAC addresses generated by a hash chain on a random seed. The user should re-associate with the AP each time he wants to change his MAC address, thus getting a new IP address alongside. It is shown that this scheme reduces the time during which an adversary will be capable of tracking the location of a user based on his MAC and IP addresses. Issues like duplicate address detection

1-4244-0773-7/06/$20.00

at the link layer are addressed and an ARP [17] based approach that does not reveal the relation between the old and the new MAC address is proposed. An attack based on signal strength collected at the physical layer at the AP is considered and it is shown that it increases the probability of tracking down a user. Attacks based on traffic analysis alone or combined with signal strength are not considered. As reassociation is required each time the MAC address is changed, the scheme affects continuous user connectivity as well as their throughput. In [8] a preliminary framework and methodology for identifying, comparing and evaluating the significance of location privacy risks in wireless networks is presented. A case study is conducted by applying the proposed methodology to IEEE802.11b WLAN hotspots. Finally, research issues to address the identified privacy challenges are discussed and a methodology consisting of three major steps for doing that is proposed. The first step is locating the user, the second is identifying the users, and the third is data collection and correlation from different entities. In the case study of IEEE802.11b WLAN hotspots, it is shown that attacks on different layers of the protocol stack could be used to identify and locate the user. It is pointed out that the equipment necessary for carrying such attacks are inexpensive and easily available. The authors in [8] conclude stating that the multi-faced issue of location privacy must be addressed through a variety of means encompassing legislative, self-regulative and technological approaches. A scheme that allows a user to take advantage of location based services (LSB), while keeping his identity and location hidden is proposed in [6]. All users send their requests to the LSB server through a cloaking proxy. The cloaking server will collect several requests from different users originating within the same area and approximately at the same time, and will issue one single request to the LSB server. If *K* requests are cloaked under one common request issued by the cloaking server, each of the users that has issued a request will be part of a *K* anonymity set, i.e. will not be identifiable within a set of *K* subjects. The area and the time interval where requests are collected can be adjusted to provide a minimum cardinality of the anonymity set, and to be able to achieve different degrees of anonymity. Even though a user pseudonym can be disposed, an attacker can still trace a user based on several other information like the user's direction, his speed, his behavior, etc. The authors in [9] identify and provide a solution to a new wireless location privacy attack based on spatial and temporal characteristics of transmitted messages. In a scenario like the one described in [7] an eavesdropper *E* may be able to track a user down, even though the user changes his pseudonym, using correlation attacks based on the time it took the user to switch to the new pseudonym, and the speed/direction the user had before switching. To address this issue, *The Silent Period* was introduced in [9]. *The Silent Period* is a variable length transition period in which a user is not allowed to disclose either the old or the new pseudonyms. Simulation results show that traceability time is decreased by a factor of 0.5 when using the silent period. In [20] an addressing scheme called *Spatio-Temporal Addressing* (STA) for mobile ad hoc networks is proposed. STA takes advantage of the latest improvement in location detection to avoid duplicate addressing while minimizing the overhead that a *Duplicate Address Detection* (DAD) protocol may imply. In STA, a station computes its address as a function of its position in the systems and the actual time. Using an injective function, as two stations cannot be in the same place at the same time, duplicate addressing is not likely to happen. Due to the accuracy limitation of location detection techniques, duplicate addresses may occur. A DAD protocol based on ARP is introduced to solve this problem. As duplicate addresses may only be assigned to stations that are close to each other, the DAD protocol has to be executed only locally, minimizing network disturbance. In [4] *The Mix Zone* is used to take advantage of LBS while protecting the location privacy of the users. A Mix Zone for a set of users, is defined as a connected spatial region of maximum size in which none of those users has registered for an application callback. If users change their addresses when entering a Mix Zone, LBS providers will not be able to link a user that previously entered the Mix Zone with one that is coming out of it. The anonymity level of a user is function of the number of users in the Mix Zone over a time interval, and can used as a threshold to decide whether enough anonymity is achieved to register for an application callback or not.

3. PEUC-WiN

We use the following notation throughout our description. We define $E_k(m)$ as the encryption with key k of message m and $S_k(m)$ as the signature with key k of message m. We consider the scenario in which a group of K users $G_j = \{u_1, ..., u_k\}$ registered with the same access point AP_j, considered to be malicious, cooperate with a Privacy Enhancer (PE) to prevent AP_j from discovering their identities and tracking their locations over time. One PE can separately manage several groups at the same time. A user can move from one group to another, simply leaving the old group and joining the new one. The adversary, i.e the AP, can listen to the incoming and outgoing traffic of all users. Each user u_i has a public/private key pair (PK_{u_i}, SK_{u_i}). A group key GK_{G_j} is given to each user when he joins a group and thus is known to all users in the same group. Each user has also a permanent IP address IP_i^* that will not change as the user moves from one WLAN to another. The PE has a public/private key pair (PK_{PE}, SK_{PE}) and knows all the group keys of all the groups it man-

ages. Moreover the PE and all users in G_j have a common hash function $H_j()$. Time is divided into slots of variable length. During each time slot, each user uses an (IP, MAC) pair chosen from a table T_j known to all users in the same group (also given to a user when he joins the group). If $|G_j| = k$, then the table will contain the pairs of addresses $(IP_1, MAC_1), ..., (IP_k, MAC_k)$. Clearly, when there's only one user, Tb_j will have only one pair and it will not help the user to protect his privacy. Nevertheless, as well as any other scheme $PEUC - WiN$ is effective only if the cardinality of the group inside the coverage area of the malicious AP is larger than one. When a user u_i enters the coverage area of AP_j and acquires an IP address IP_i, a requests to register with IP_i and MAC_i as his IP address and MAC address respectively is sent to the PE. The the following message is sent to the PE in order to join the group G_j (the group inside the coverage area of AP_j):

$E_{PK_{PE}}(join||G_j||ID_i||IP_i||MAC_i||TS||$
$S_{SK_{u_i}}(join||G_j||ID_i||IP_i||MAC_i||TS))$

where G_j is the group identifier, ID_i the user identity, IP_i and MAC_i the IP and MAC addresses of u_i and TS is a timestamp. The PE will answer with the following message, to provide the the new user the group key:

$E_{PK_{u_i}}(join||G_j||ID_i||GK_{G_j}||TS||$
$S_{SK_{PE}}(join||G_j||ID_i||GK_{G_j}||TS))$

After verifying the signature and the timestamp of the join message, the PE will add u_i to the group G_j and will add (IP_i, MAC_i) to the table Tb_j, increase K_j (the size of the group) by one and send an update message to all the users in the group G_j containing the updated table Tb_j:

$E_{GK_{G_j}}(update||G_j||K_j||Tb_j||S_j||T_j||TS||$
$S_{SK_{PE}}(update||G_j||K_j||Tb_j||S_j||T_j||TS))$

where G_j is the group identifier, K_j the size of the group G_j, Tb_j is the table of the address pairs (IP, MAC) in use in G_j, S_j the seed used for calculating the hash chain and TS is a timestamp.

When the cardinality of the group changes an update message is sent to all users. This message will cause users to reset their clocks, and to learn the necessary information to properly synchronize with other users in the same group and to be able to switch addresses at the same time (to a certain precision). At the beginning of a time slot t each user $u_i \in G_j$ will compute $H_j^t = H_j(H^{t-1}j)$ where $H_j^0 = S_j$ and will use the resulting value to compute the pair of addresses (IP, MAC) that he will use during that slot, as well as the length of the slot. $(H_j^t \bmod K_j)+i$ will be used as an index in Tb_j to retrieve the (IP, MAC) pair to be used. The length of the time slot will be set to $T_j + F(H_j^t)$, where F() is a function that outputs a variable time interval that will be used to prevent a timing attack based on the constant length of time slots. This also ensures that no collisions will happen when changing address and hence no duplicate address detection (DAD) protocol will be needed. Before $u_i \in G_j$ moves away from the coverage area of AP_j, it sends the following message to PE:

$E_{PK_{PE}}(leave||G_j||ID_i||IP_i||MAC_i||TS||$
$S_{SK_{u_i}}(leave||G_j||ID_i||IP_i||MAC_i||TS))$

This message will remove u_i from G_j. After verifying the signature and the timestamp, the PE will remove (IP_i, MAC_i) from Tb_j, decrease K_j, compute a new seed S_j and will send an update message to the users in G_j. To deal with cases where a user suddenly leaves a group without notifying the PE, perhaps due to a sudden shutdown, the PE should keep timers for each user. The timer is reset each time a packet is received from that user. When the timer expires, the PE will send a message to the user to check whether it is still within the coverage area of AP_j or not. If not, it will infer that the user has left and will send an update message to all users in the group. Update messages are sent only when a user joins or leaves a group and this happens infrequent. The average time that users remain associated to a certain AP is about 20 minute [2]. As in Mobile IP with reverse tunneling [16], [15], each user will communicate with the outside world through the PE which will route traffic which originated from (or is destined to) the user. To minimize network disruption, the PE will perform all the necessary operations to allow a user to keep his TCP connections running after an addresses change. Suppose that a user $u_i \in G_j$, who is using the pair (IP_i, MAC_i), wants to set up a TCP connection with a correspondent node CN with IP address IP_{CN}. u_i will establish a TCP connection with the PE using IP_i as the source IP address and the PE will establish a TCP connection with CN using IP_i^* as source IP address. A datagram from u_i to CN will be sent from u_i to the PE using IP_i and IP_{PE} as source and destination addresses respectively. The PE will keep track of all connections established with users of each group and their communicating partners. It will be able to forward the datagram to CN using IP_i^* and IP_{CN} as source and destination addresses respectively. Datagrams from CN to u_i will follow the reverse path, that is, CN will send the datagram to IP_i^*, the PE will receive and will forward it to u_i using IP_{PE} as source address and IP_i as destination address. Thus, the PE will act as a proxy for all communications. Moreover, a correspondent node will communicate with u_i using IP_i^* therefore learning nothing about the actual subnetwork where u_i is located. This is very similar to the operations performed in Mobile IP. Suppose that at time slot t $u_i \in G_j$ with (IP_p, MAC_p) is communicating with a correspondent node CN_i and $u_h \in G_j$ with (IP_q, MAC_q) is communicating with a correspondent node CN_h. The following connection will be established:

1. $(IP_p, port_a, IP_{PE}, port_b)$ from u_i to the PE
2. $(IP_{PE}, port_c, IP_{CN_i}, port_d)$ from the PE to CN_i
3. $(IP_q, port_e, IP_{PE}, port_b)$ from u_h to the PE

4. $(IP_{PE}, port_e, IP_{CN_h}, port_f)$ from the PE to CN_h

The PE will forward traffic between connection 1 and connection 2 to allow communication between u_i and CN_i and will also forward traffic between connection 3 and connection 4 to allow communication between u_h and CN_h. Suppose that at slot $t+1$, u_i is supposed to use (IP_q, MAC_q) while u_h is supposed to use (IP_p, MAC_p). The new set of connections will be:

1. $(IP_q, port_a, IP_{PE}, port_b)$ from u_i to the PE
2. $(IP_{PE}, port_c, IP_{CN_i}, port_d)$ from the PE to CN_i
3. $(IP_p, port_e, IP_{PE}, port_b)$ from u_h to the PE
4. $(IP_{PE}, port_e, IP_{CN_h}, port_f)$ from the PE to CN_h

No connection will be torn down and no new connection will be established. The PE will simply forward traffic between connections 1 and 2 and between connections 3 and 4 after switching IP_p and IP_q. While IP addresses change, port numbers remain fixed because even though u_i can easily compute the IP address IP_{t+1} it is going to use during time slot $t+1$, it might not be able to learn the port used by the user that was using IP_{t+1} at time t. Assuming that all communication are encrypted at the IP layer using IPsec [1], an adversary cannot trace users by looking at ports numbers of TCP connections. In addition to changing the IP addresses of the connections, the PE must manage sequence numbers, ack numbers and window sizes of each connection, in order to minimize network disruption.

4. Security Analysis

In our scheme, as well as in [7], physical layer attacks on user privacy are not considered. This is based on the assumption that the required equipment and technical knowledge to perform such attacks are not as common and as the ones needed to carry attacks on higher layers of the protocols stack. Despite this assumption a determined powerful adversary can use physical layer attacks to trace the location of a certain user, even if location privacy schemes are implemented in the upper layers of the protocol stack. Another problem with addressing attacks on the physical layer is that it is very hard to combat such attacks without modifying the underlying transmission technologies and standards so that they take the issue of location privacy and security into account. Using the schemes based on disposing MAC and IP addresses, an adversary will not be able to track a user's communication if he relies on attacks on higher layers of the protocol stack (layer 2 and above). The degree of anonymity that a user can have is proportional to the cardinality of the group, the bigger it is, the higher the degree of anonymity will be. The time interval during which a user can be tracked is proportional to the minimum duration of a time slot: small values will result in higher anonymity but in more overhead caused by frequent switches of addresses, whereas large values will decrease the overhead but will allow an adversary to track users for a longer time. In our system the PE is responsible for adding and deleting users, as well as sending update messages. As update messages are encrypted with a key known by all the users in a group, previous group members can learn sensitive group information such as it's actual size and the random seed. To avoid information leakage to previous group members, a key distribution scheme such as [13] can be used in order to achieve perfect forward secrecy. Nevertheless, key distribution schemes are beyond the scope of this paper. Because we require users to register with the PE and log on to receive the necessary information to join a group, the possibility of an attacker impersonating a member of a group is not considered. If an attacker manages to join a group or to compromise a member of a group, it will be possible to know the sequence of addresses used by each group member and to track them down. Other means, should be used at registration time, to avoid impersonation attacks. Since a connection to the PE could be identified by layer 3 addresses (e.g. source and destination IP addresses), an attacker could still determine the affiliation of a certain user to a certain group by observing the IP addresses in the packets sent by this user. To thwart this attack one possibility might be to use a PE that jumps between several IP addresses based on the hash of a certain seed known to the group members. Even though the pool of IP addresses that the PE will use in this case will most likely belong to the same organization and will all be located in the same network, changing the IP address of the PE will prevent an adversary from locating it with a fine granularity. This enhancement will be considered in future work. Another solution could be to use onion routing mechanisms [18] to prevent an attacker from identifying the destination of the packets but the delay will increase in this case.

5. Performance Evaluation

An important issue that affects the performance of the PE is the cardinality of the groups. More users will increase the degree of anonymity but will also result in a heavier load on the PE. Although this may seem problematic, we point out that the PE can be implemented as a standalone server which has enough processing power to perform the required tasks. To avoid having a single point of failure in the system, one could replicate the functionality of the PE among several servers. Techniques for addressing this issue are orthogonal to the design of the system and already developed solutions for similar problems in other fields, such as webservers and databases, could be

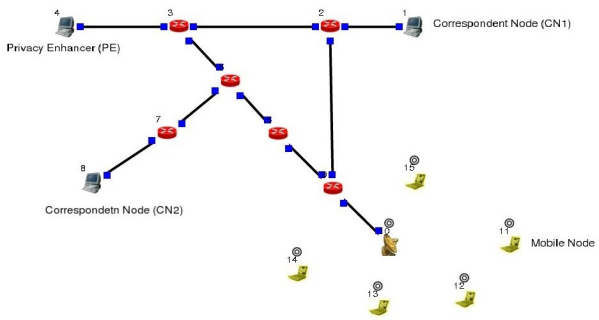

Figure 1. Topology of the network used for simulation of $PEUC - WiN$.

used. Since the users in our scenarios are wireless, and it is known that the performance of TCP is degraded anyway in wireless environments because of high error rates [5], UDP could be used for most traffic and the reliability could be implemented at the application layer. Another solution could be to tunnel TCP in UDP. This will mean that the congestion control mechanisms in TCP have to be turned off, which makes TCP only add the in order delivery, on top of the service provided by UDP. Because all data follows the route from the user to the PE to the correspondent node, the path from the WLAN where the group is located and the PE might become a bottleneck. Also, the performance can be affected by the triangular routing problem between the PE, the WLAN and the correspondent nodes. In the worst case a user will communicate with a correspondent node inside the same WLAN, while the PE is far away and connected through high delay links. Clearly, anonymity cannot be achieved without paying a cost. In this case performance degradation must be seen as a sacrifice for increasing user privacy. Moreover, several PEs could be deployed throughout the Internet to make sure that one PE will be close enough to each of the WLANs from where a user might want to use $PEUC - WiN$. In order to allow users to change their IP addresses during a TCP connection, a shim layer between the network layer and the MAC layer can be used, as in [12].

Simulations of our scheme were performed using NCTUns 3.0 [19]. We resided to simulate the scheme instead of implementing it because of a practical issue related the IEEE802.11 cards available today. If a user u_i switches to (MAC_j, IP_j) pair used by u_j, the former will need to send frames with a sequence number close to the last one used by u_j while he was using (MAC_j, IP_j) pair. A user can precompute which addresses he will switch to and listen to sequence numbers of this address pair and record it, so that when the switch occurs, he would use the proper sequence number. One problem we encountered when trying to implement this is that current wireless drivers do not allow the user to select the sequence number used in the IEEE802.11 frame. Changing MAC address implies turning down the network interface, assigning a new MAC address and turning it up again: the whole operation, depending on the processor, operating system, interface drivers, might typically take less than 200 msec. We measured the time it takes to do this on several laptops running different Linux flavors. On the other hand, the time to reassociate with the AP could typically be between several hundred msec and two seconds [10]. Thus it is evident that a scheme which requires reassociation each time an interface address is changed will experience longer disruptions. Fig.1 shows the topology for our simulations: five users within a WLAN are cooperating with the PE. To show the performance in different settings, we consider communication with a correspondent node ($CN1$) that has a low delay path between itself and the PE as well as communication with a correspondent node ($CN2$) that has a high delay path to the PE. We simulate a TCP connection between a wireless user and a correspondent node. Fig.2 compares the throughput of a normal user, a user using the scheme proposed in [7] and a user using our scheme. The graphs in Fig.2 (a), (b) and (c) correspond to the communication with $CN1$ while (d), (e) and (f) correspond to the communication with $CN2$. As shown in the results, a user who keeps his MAC and IP address achieves the highest throughput (y-axis) but, on the other hand, has no location privacy and can be easily traced. The scheme in [7] improves user privacy but will force the user to reassiociate periodically with the AP. More precisely, the user will have to terminate his TCP connections, turn down his wireless interface, change his MAC address, turn his interface up, reassociate to get a new IP address and finally reestablish the TCP connections going through new three way handshakes and new slow start periods [11]. Our scheme forces a user to change his MAC and IP address but does not require him to reassociate, nor to tear down/reestablish any TCP connections. In the case of communication with $CN2$ the high delay of the path between PE and $CN2$ results in a longer time for a connection to achieve its maximum throughput.

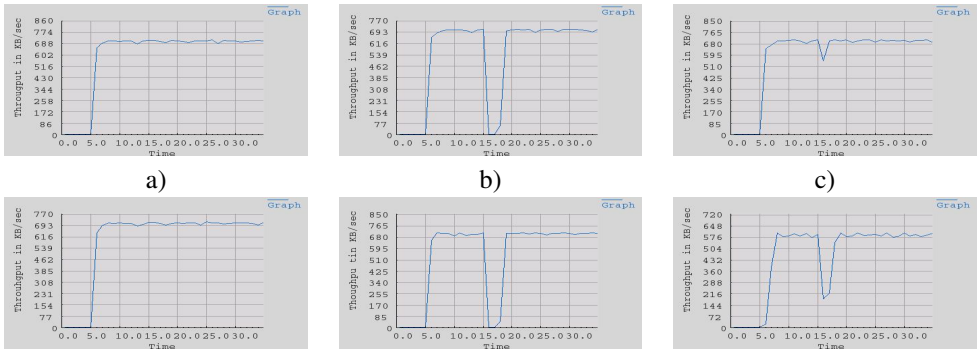

Figure 2. Average throughput of a normal user without any privacy mechanism (a ,d), of one using the scheme in [7] (b, e) and of one using PEUC-WiN (c, f).

6. Conclusion and Future Work

In this paper we have introduced a new scheme to address some of the privacy issues in IEEE802.11 based WLANs. The proposed scheme relies on the collaboration between users and a trusted third party which we call the Privacy Enhancer (PE) to implement location privacy for these users and prevent their traceability. The scheme causes minimal network disruption compared to other schemes that have been proposed so far. Future work will focus on developing a scheme that does not require the presence of a trusted third party and in which one of the users could act as the PE.

References

[1] Ipsec. *http://www.ietf.org/ids.by.wg/ipsec.html*.

[2] P. B. A. Balachandran, G.M. Voelker and P. Rangan. Characterizing user behavior and network performance in a public wireless lan. *Proceedings of the ACM SIGMETRICS Conference on Measurement and Modeling of Computer Systems*, 2002.

[3] P. Bahl and V. Padmanabhan. RADAR: An in-building RF-based user location and tracking system. *Proceedings of IEEE INFOCOM*, 2000.

[4] A. R. Beresford and F. Stajano. Location privacy in pervasive computing. *IEEE Pervasive Computing*, 2003.

[5] P. M. G. Xylomenos, G.C. Polyzos and M. Saaranen. Tcp performance issues over wireless links. *IEEE Communications Magazine*, 2001.

[6] M. Gruteser and D. Grunwald. Anonymous usage of location-based services through spatial and temporal cloaking. *Proceedings of ACM MobiSys*, 2003.

[7] M. Gruteser and D. Grunwald. Enhancing location privacy in wireless lan through disposable interface identifiers: a quantitative analysis. *Proc. of 1st ACM international workshop on Wireless mobile applications and services on WLAN hotspots*, 2003.

[8] M. Gruteser and D. Grunwald. A methodological assessment of location privacy risks in wireless hotspot networks. *Security in Pervasive Computing*, 2004.

[9] L. Huang and H. Yamaneet. Enhancing wireless location privacy using silent period. *5th Workshop on Privacy Enhancing Technologies*, 2005.

[10] J. S. I. Herwono, S. Goebbels and R. Keller. Evaluation of mobility-aware personalized services in wireless broadband hotspots. *In Proceedings of Communications Networks and Distributed Systems Modeling and Simulation*, 2004.

[11] W. S. M. Allman, V. Paxson. Rfc2581 - tcp congestion control. 1999.

[12] K. S. M. Buddhikot, A. Hari and S. Miller. Mobilenat: A new technique for mobility across heterogeneous address spaces. *ACM/Kluwer Journal on Mobile Networks and Applications*, 2005.

[13] G. T. M. Steiner and M. Waidner. Key agreement in dynamic peer groups. *IEEE Transactions on Parallel and Distributed Systems*, 2000.

[14] R. Minch. Privacy issues in location-aware mobile devices. *Proceedings of 37th Hawaii International Conference on System Sciences*, 2004.

[15] G. Montenegro. Rfc2344 - reverse tunneling for mobile ip. 1998.

[16] C. Perkins. Mobile networking through mobile ip. *IEEE Internet Computing*, 1998.

[17] D. Plummer. Rfc826 - ethernet address resolution protocol. 1998.

[18] D. K. S. Katti and K. Puchala. Slicing the onion:anonymous routing without pki. *MIT CSAIL Technical Report, http://nms.lcs.mit.edu/sachin/slicing.html*, 2005.

[19] S. Wang and Y. Lin. Nctuns network simulation and emulation for wireless resource management. *Wiley Wireless Communications and Mobile Computing*, 2005.

[20] K. Yamazaki and K. Sezaki. Spatio-temporal addressing scheme for mobile ad hoc networks. *Proceedings of IEEE TENCON*, 2004.