A Secure Group Key Management Scheme for Wireless Cellular Networks

by H. Um and E. J. Delp

Center for Education and Research in
Information Assurance and Security,
Purdue University, West Lafayette, IN 47907-2086

A Secure Group Key Management Scheme for Wireless Cellular Networks

Hwayoung Um and Edward J. Delp
Video and Image Processing Laboratory (VIPER)
School of Electrical and Computer Engineering
Purdue University
West Lafayette, Indiana, USA

***Abstract*— In wireless networks, secure multicast protocols are difficult to implement efficiently due to the dynamic nature of the multicast group and scarcity of bandwidth at the receiving and transmitting ends. Mobility is one of the most distinct features to be considered in a wireless network. Moving users onto the key tree causes extra key management resources even though they are still in service. To take care of frequent handoff between wireless access networks, it is necessary to reduce the number of rekeying messages and the size of the messages. In this paper, we design a key management tree such that neighbors on the key tree are also physical neighbors on the cellular network. By tracking the user location, we localize the delivery of rekeying messages to the users who need them. This lessens the amount of traffic in wireless and wired intervals of the network. The group key management scheme uses a pre-positioned secret sharing scheme.**

I. Introduction

As the technology and popularity of cellular networks such as 3G and cdma2000 [1] grows, there has been considerable progress in the area of multimedia streaming over wireless networks. Many applications, such as video conferencing, video-on-demand, stock-quote distribution, and software updates, have been developed for streaming digital multimedia contents to a set of clients [2]. In such applications, the multicast protocol plays an important role because it can deliver data efficiently from a source to multiple receivers. It reduces the bandwidth of the wireless network and the computational overhead of the mobile device. This makes multicast an ideal technology for communication among a large group of users. An important issue is how to provide security to these applications. Security could involve a number of issues, such as authentication of clients, secure data transmission and copyright protection. For each of these security needs, a number of security protocols (especially for multicast) have been developed and a great deal of research continues in this area. The problem then is how to flexibly integrate security protocols into multimedia streaming applications even though these applications are usually developed without security.

Multicast protocols require an access control mechanism such that only authorized members can access group communications. Access control is usually achieved by encrypting the content with an encryption key. This key is known as the session key (SK) that is shared by all valid group members. Access control typically employs a tree of encryption keys to update and maintain the SK. Tree-based schemes [3][4] have advantages that include computation, communication, and storage resources for the user and the group manager. In such schemes, the group key should be changed periodically or after a user leaves or joins the service to prevent the leaving/joining user from accessing future/prior communication. This is known as "forward message secrecy" and "backward message secrecy," respectively. Key management schemes in multicasting should also be "scalable." By scalable we mean that the overhead involved in key exchange, updates, data transmission, and encryption must not be dependent on the size of the multicast group. Moreover, addition or removal of a host from the group should not affect the other members. This is known as the "1 affects n" scalability rule.

The multicast protocol used in wired networks does not perform well in wireless networks because multicast structures are fragile as the mobile nodes move and connectivity changes. When we choose a key management scheme, the structure of the wireless network should be considered very carefully. For example, the wireless cellular network has a unique hierarchy structure such that a key management scheme should be easy to deploy. Some methods have been proposed to address access control in wireless networks. In [5], topology matching key management trees (TKMK) are described. By matching the key tree to the network topology, the communication traffic is reduced by 33% - 45% compared to the conventional key trees that are independent of the network. In [6], baseline, immediate, delayed and periodic re-keying schemes are proposed a wireless local area network (WLAN). We believe, this is the first method that describes the handoff impact of a centralized key management scheme for a real wireless cellular network.

In this paper, we design a key management tree such that the neighbors on the key tree are also physical neighbors in the cellular network. By tracking the user location, we localize the delivery of re-keying messages to the users who need them. This lessens the amount of traffic in the wireless and wired intervals of network. The group key management scheme uses a pre-positioned secret sharing scheme.

II. Handoff Schemes

We describe a soft handoff scheme and a hard handoff scheme based on the location of a user instead of the use of the strength of a pilot signal from the user to the Base station (BS),

0-7695-2497-4/06 $20.00 © 2006 IEEE

as shown in Figure 1. There are two important parameters, L_ADD and L_DROP. L_ADD and L_DROP indicate the beginning of handoff and the termination of handoff based on the location of the user. In general, the system administrator decides the values of the two parameters. In our work, a 30% soft handoff area is used. That is, the L_ADD is the boundary of overlapping area of two BSs and the L_DROP is the middle of two BSs as shown in Figure 1. In this example, a Mobile Station (MS) moves from A of BS1 to B of BS2. The moving MS requests a handoff to the neighboring BS when the location of the neighboring BS exceeds the handoff threshold L_ADD. If the handoff request is accepted in the neighboring BS, BS2, the MS maintains two traffic channels assigned by the serving BS, BS1 and the neighboring BS. As the MS moves away from the serving BS and approaches the neighboring BS, the location of MS falls below the handoff drop threshold L_DROP for the servicing BS. If the location of the MS is close to the neighboring BS during the specific time interval, the traffic channel assigned by the serving BS is released, and the handoff is terminated.

In the case of hard handoff, MS requests a handoff to the neighboring BS immediately after exceeding the handoff threshold L_DROP. The moving MS does not maintain 2 traffic links in the handoff region. The handoff-add threshold can be thought of as the "largest" distance between a MS and a BS such that the MS can reliably transmit information through the given BS. The handoff-drop threshold is the distance where the MS cannot communicate with the servicing BS any more. In general, the system administrator determines L_ADD and L_DROP to optimize wireless channel utilization. Each serving BS broadcasts this information.

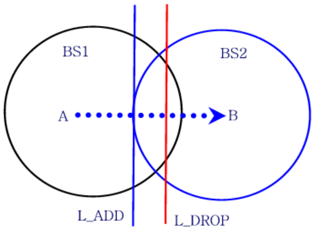

Fig. 1. An Example of L_DROP and L_ADD

We propose a new handoff scheme to reduce the traffic of key updating during a handoff call. In the revised handoff scheme, two links are maintained during the handoff for data transmission while the key update is only performed after completing the handoff. That is, the key updating does not occur when a call enters the handoff region. The connection to the new BS is established without rekeying to prepare for the new connection. We reduce the traffic for key update in handoff region. This is a variation of the soft handoff scheme.

III. Location Tracking

In this section, we describe briefly the determination of the location of a user in Code Division Multiple Access (CDMA) cellular system [7] . The forward link transmission timing of all CDMA2000 base stations worldwide is synchronized within a few microseconds. Base station synchronization can be achieved through several techniques including self-synchronization, radio beacons, or through satellite-based systems such as the Global Positioning System (GPS). Reverse link timing is based on the received timing derived from the first multipath component used by the terminal [8].

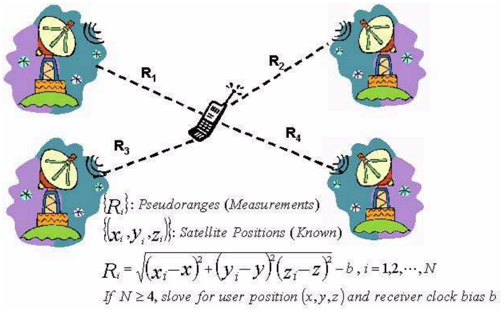
R_1
R_2
R_3
R_4
$\{R_i\}$: Pseudoranges (Measurements)
$\{(x_i, y_i, z_i)\}$: Satellite Positions (Known)
$R_i = \sqrt{(x_i - x)^2 + (y_i - y)^2 (z_i - z)^2} - b,\ i = 1,2,\cdots,N$
If $N \geq 4$, slove for user position (x,y,z) and receiver clock bias b

Fig. 2. The Principle of Location Tracking

GPS is a satellite-based pseudo-ranging location system. The idea behind GPS is that one's position is determined from the distance from three known satellites by triangulation. The distance is measured in terms of delay, where an accurate clock at the receiver measures the time delay between the signal transmitted from the satellite and arriving at the receiver. Four simultaneous delay measurements from four satellites are required to solve for the three position coordinates and the user's clock offset as shown in Figure 2. Proposals for positioning, using one or two satellites, were presented in [9] based on newly proposed mobile satellite systems.

IV. Pre-Positioned Secret Sharing (PSS)

We propose to use secret sharing techniques for the construction of the key trees. Secret sharing methods have been used for various security applications requiring users to share keys. We use the Pre-Positioned Secret Sharing (PSS) scheme described in [10][11]. We showed in previous work [12][13] that PSS-based schemes are comparable to Tree-based schemes [3][4] with respect to communications cost, rekeying time cost, and memory cost in wired networks.

To generalize Shamir's secret sharing scheme [14], we construct a (n, t) secret sharing scheme using a $(t-1)$ degree polynomial:

$$f(x) = a_0 + a_1 x + \cdots + a_{t-1} x^{t-1} \mod (q) \qquad (1)$$

To reconstruct the secret from each subset of t shares out of n shares, we use the interpolation property with Lagrange interpolation [15]. Given t distinct pairs consisting of $(i, f(i))$, there is a unique polynomial $f(x)$ of degree $t-1$, passing through all the points. This polynomial can be effectively constructed from the pairs $(i, f(i))$. Without loss of generality we will use this subset:$f(1), \cdots, f(t)$ and Lagrange interpolation to find the unique polynomial $f(x)$ such that

$degree f(x) < t$ and $f(j) = share_j(s)$ for $j = 1, 2, \cdots, t$, where $share_j(s) = (x_i, f(x_i))$, $i = 1, 2, \cdots, n$.

$$f(x) = \sum_{j=1}^{t} f(x_j) \times L_j(x), L_j(x) = \prod_{i \neq j, 1 \leq i \leq t} \frac{(x - x_i)}{(x_j - x_i)} \quad (2)$$

where, $L_i(x)$ is the Lagrange polynomial which has value 1 at x_i, and 0 at every other x_j. Then we reconstruct the secret to be $f(0)$.

PSS uses a polynomial of order $(m-1)$ to generate shares. The shares will be used to generate the keys for the key tree. PSS is an interpolating scheme based on polynomial interpolation similar to Shamir's secret sharing scheme [14]. An $(m-1)$-degree polynomial over the finite field $GF(q)$

$$F(x) = a_0 + a_1 x + \cdots + a_{m-1} x^{m-1} \mod (q) \quad (3)$$

is constructed such that the coefficient a_0 is the secret and all other coefficients are random elements in the field. Each of the n shares is a point (x_i, y_i) on the curve defined by the polynomial, where x_i is not equal to 0. Given any m shares, the polynomial is determined uniquely and hence the secret a_0 is obtained. However, given $m-1$ or fewer shares, the secret is any element in the field. Therefore, PSS is a perfect secret sharing scheme. PSS uses a tree structure, which is composed of user nodes, subgroup-manager nodes, and the group-manager node in a bottom-up order. In PSS, $(m-1)$ shares are assigned to each node while the m^{th} share is broadcast as public information. The $(m-1)$ shares of a node, which are secret, are referred to as the pre-positioned shares, while the broadcast share, is referred to as the activation share (AS). In PSS, the AS helps determine the symmetric keys for each node. Once a node obtains the AS, the original polynomial of order m is reconstructed and hence the keys are recovered, using the AS along with the private $(m-1)$ shares owned by the node.

V. Group Key Management

We design a key management tree such that the key tree matches the cellular network topology. We match the multicast users to the MSs, subgroup managers to the BSs and the group manager to the mobile switching exchanger (MX). We localize the delivery of rekeying messages to small regions of the cellular network, each base station, by transmitting the key update messages only to the users who need them. This lessens the amount of traffic in the wireless and wired intervals.

We describe the group key management operations, join, leave and handoff, using the example shown in Figure 3 and Figure 4. In our scheme, each node has (n-1) shares if the secret is generated by n^{th} order polynomials. The shares are used to generate the keys for the key tree when each node receives a share, AS. For each join, leave, and handoff, the shares will be changed to prevent the joining user from accessing past/future communications. After each join or leave, a new secure group is formed. The key server has to update the group's key graph by replacing the keys of some existing k-nodes, deleting some k-nodes and adding some k-nodes. Only one activating share is multicast by the key server, and it is used together with the pre-positioned information to generate three simultaneous keys.

In this example, 1 Group Manager (GM), 2 Subgroup Managers (SGM) and 6 users are considered. In Handoff operations, a 2 inter-BS handoff scheme is used for simplicity even though there are many handoff schemes [7].

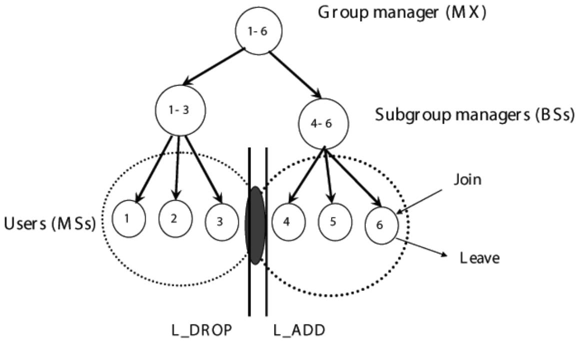

Fig. 3. Hierachical Tree for Join/Leave

A. Joining a Group via BS1

To illustrate the above, suppose user 6 wants to join the secure group (see Figure 3). To prevent the joining user from accessing past communications, all keys along the path from the joining point to the root node need to be changed.

User 6 sends a join request message to the key server. After granting the new user, the key server associates s_6 with the new member and creates a new node and a new set node. The key server attaches the set node to the existing joining point. After changing s_{1-5} to s_{1-6} and s_{4-5} to s_{4-6}, the key server constructs the following two messages:

1) AS,$\{\mathrm{s}_{1-6}\}_{k1-5}$, $\{\mathrm{s}_{4-6}\}_{k4-5}$
2) AS,$\{\mathrm{s}_{1-6}, \mathrm{s}_{4-6}\}_{k1-6}$

where AS is the activating share, the fresh keys k_{1-5}, k_{4-5} and k_6 are obtained by AS and the sets s_{1-5}, s_{4-5}, and s_6, respectively. The key server multicasts the first message to the existing members, through $1-5$, while it unicast the second to the new member, 6. The members construct the new set of group keys, $k_{1-6}^{'}$, when the new AS is multicast with the encrypted content.

B. Leaving a Group via BS1

Now suppose user 6 wants to leave the secure group, as shown in Figure 3. To keep the leaving user from accessing future communications, all keys along the path from the leaving point to the root node need to be changed.

User 6 sends a leaving request message to the key server. After granting the leaving user, the key server deletes the member node and the set node from the key tree. The key server replaces s_{4-6} by s_{4-5} and s_{1-6} by s_{1-5}. Then it constructs the following messages and multicast to the remaining members:

1) $\{s_{1-5}\}_{k1-3}, \{s_{1-5}\}_{k4-5}$
2) $\{\mathrm{s}_{4-5}\}_{k4}$, $\{\mathrm{s}_{4-5}\}_{k5}$
3) AS

C. Handoff

As shown in Figure 4, user 4 is moving from BS2 to BS1 while the user is in the group service. The serving subgroup manager, BS2, requests a new connection to the neighboring BS, BS1, when the moving user exceeds the handoff add threshold, L_ADD. The key server associates s_4 with the new member of BS1, and creates a temporary node and a new set node. These sets are used within the handoff area. The key server attaches the set node to the existing joining point. After changing s_{1-3} to s_{1-4}, it constructs the following two messages:

1) AS, $\{\mathrm{s}_{1-4}\}_{k1-3}$
2) AS, $\{\mathrm{s}_{1-4}\}_{k1-6}$

The key server multicasts the first message to the existing member of BS1 while it unicasts the second message to the handoff member. Thus the handoff user keeps two links until it exceeds the handoff drop threshold, L_DROP. Immediately after the handoff user exceeds the L_DROP, the key server performs the leave procedure for BS2 and the add procedure for BS1.

The key server deletes the member node, here 4, and the set node from the key tree. The key server replaces s_{4-6} by s_{5-6}. Then it constructs the following messages and multicasts it to the remaining members:

1) $\{\mathrm{s}_{1-6}\}_{k1-4}$, $\{\mathrm{s}_{1-6}\}_{k4-5}$
2) $\{\mathrm{s}_{4-5}\}_{k4}$, $\{\mathrm{s}_{4-5}\}_{k5}$
3) AS

In the case of hard handoff, the leave and join operations are performed immediately after the moving user exceeds the boundary of the serving BS. That is, we consider the hard handoff user as a leaving and a joining user to the group service. In this case, the handoff user does not keep two links in the handoff region. This is the main difference between the soft handoff and the hard handoff operations.

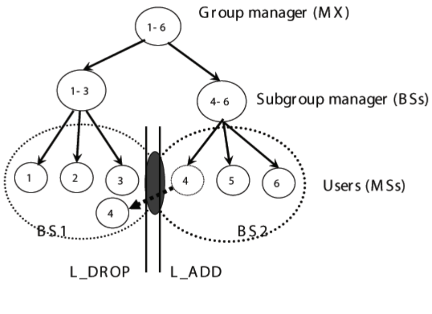

Fig. 4. Hierachical Tree for Handoff

Neither handoff schemes are practical for cellular networks with frequent handoffs because the extra communication cost is too high if the system does not limit the number of group members. Thus the system manager uses a resource management scheme such as the call admission control (CAC) function in a real system. We describe a simple CAC function below.

VI. Simulations and Results

Three measures are used to compare Tree-Based schemes (TBC) [3] and PSS[12]: Storage cost, communication cost and computational cost where both schemes use the logical key hierarchy. The observations are summarized in the following Tables. The group key tree is assumed full and balanced. The height h of the tree is the length of the longest directed path in the tree, and the degree d of the tree is the maximum number of incoming edges of a node in the tree.

TABLE I
Comparison of TBC and PSS schemes: Storage Cost

	TBC	PSS
# of keys held by server	$dn/(n-1)$	-
# of keys held by each member	h	-
# of share sets held by server	-	$dn/(n-1)$
# of share sets held by each member	-	h

The number of encryptions and decryptions required by join/leave operations are the same in both schemes. In the PSS scheme, however, neither the server nor the members need to store the node keys generated after each rekeying. They are deleted as soon as they are used in the decryption process. The sets (both the group set and the auxiliary set), however, need to be kept until they are replaced. There is a 1-1 correspondence between the number of keys generated for each member and the number of sets held by each member.

TABLE II
Comparison of TBC and PSS schemes: Communication Cost

	TBC	PSS
Join	$O(log_d(n))$	$O(log_d(n))$ and $O(1)$
Leave	$O(dlog_d(n))$	$O(dlog_d(n))$ and $O(1)$
Periodic rekeying	$O(d)$	$O(1)$

The size of the messages sent for join/leave operations are the same in both schemes. An additional communication cost in the PSS scheme for join/leave operations is the delivery of the activating share. The two schemes have different requirements in periodic rekeying. The communication cost for the PSS scheme is the delivery of the activating share and the communication cost for the TBC scheme is the delivery of d encrypted messages.

An additional computational cost in the PSS scheme for join/leave operations is the processing needed for the construction of the polynomials. There is a 1-1 correspondence between the number of polynomials constructed by the server and the number of encryptions performed by the server. There

TABLE III

TBC Computation Cost

	Server	Requesting member	Non-requesting member
Join	$2(h-1)$	$h-1$	$d/(d-1)$
Leave	0	$d/(d-1)$	$d(h-1)$
Periodic	d	1	

TABLE IV

PSS Computation Cost

	Server	Requesting member	Non-requesting member
Join	$2(h-1)$	$h-1$	$d/(d-1)$
Leave	$d(h-1)$	0	$d/(d-1)$
Periodic	0	0	

is also a 1-1 correspondence between the number of polynomials constructed by each member and the number of decryptions performed by each member. The two schemes have different computational requirements to recover the group key in periodic rekeying. The PSS scheme needs one polynomial construction for the server and one polynomial construction for each member whereas the TBC scheme needs d encryptions for the server and one decryption for each member.

TABLE V

Polynomial Construction Cost

	Server	Requesting member	Non-requesting member
Join	$2(h-1)$	$h-1$	$d/(d-1)$
Leave	$d(h-1)$	0	$d/(d-1)$
Periodic	1	1	

Now we test our new group key management scheme based on pre-positioned secret sharing in a wireless cellular network. We employ a wireless cellular network that consists of 16 concatenated cells with 1 Mobile switching eXchanger (MX). We use 4 mobility models: $0 \sim 1$ km/hr for walking, $2 \sim 5$ km/hr for running, $6 \sim 25$ km/hr for a low speed vehicle, and $26 \sim 100$ km/hr for a high speed vehicle. The arrival process of the new calls and the call duration are assumed to a Poisson distribution with rate λ and a Exponential distribution with mean $1/\mu$, respectively. Table VI shows the range of values and the constants for the parameters.

Including the handoff users and the new users, each BS is able to accommodate up to 100 group service users. Users are uniformly distributed in each BS. The CAC function, which is located in BS, counts the number of users to decide whether to accept new users or handoff users. We reserve some channels, here 30%, to give a priority to handoff users.

A call may have 3 key transactions during the call duration: call generation, handoffs, and call termination. A handoff call requires 2 key update transactions: (1) adding a new channel when a call enters handoff region and (2) deleting a serving channel after completing handoff.

Thus the number of key transactions during call duration, N, is equal to

TABLE VI

Simulation Parameters

Parameter	Value
# of MX	1
# of BS	16
# of MS	Up to 100 per BS
Call generation	Poisson with λ (calls/sec)
Call duration	Exponential with $1/\mu$ (1/sec)
User mobility	0-1 km/h (walking) 2-5 km/h (running) 6-25 km/h (low speed vehicle) 26-100 km/h (high speed vehicle)
Cell radius	1Km
Service	Voice, Data, Video
L_ADD	30% of BS coverage area
L_DROP	Boundary of BS

$$N = 1 \times (callgeneration) + 1 \times (calltermination) + 2 \times (\#ofHandoff) \tag{4}$$

We ran our simulation 10 times and obtained the average handoff attempts per user according to the mobility models. Each call has $3 \sim 8$ handoffs during the call service time. In Figure 5, we show the number of handoff attempts as a function of the number of new calls. Without CAC, the number of handoff attempts increases linearly as the number of new calls increases.

The handoff may be the largest inefficiency in a wireless cellular network. To reduce the number of handoffs, we increase the radius of the cell. However, as the radius of the cell increases, the system capacity decreases. That is, the total number of users in the system will be decreased if the radius of the cell is increased. So we need an alternative method.

We do not take into account call admission control (CAC). That is, we do not restrict the number of users for each BS. The CAC function determines whether to accept a new call and a handoff call. We use the CAC function presented in [16]. The CAC function uses the number of voice and data calls based on the signal to noise ratio.

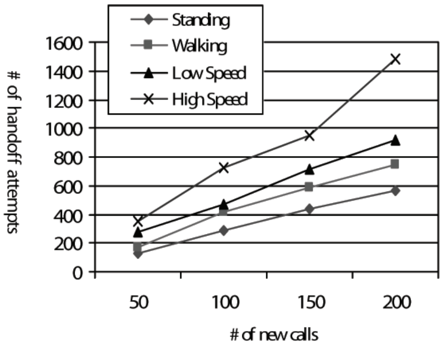

Fig. 5. The Number of Handoff Attempts vs. The Number of New Calls without a CAC.

With the CAC and a revised handoff scheme, the number of handoffs per call is reduced by almost 20% compared to the results of Figure 5 until the threshold of the CAC is reached, here 100 users per BS. Above the threshold, the handoff attempts stay at a certain level since the CAC limited the number of new calls. In Figure 6, we show the number of handoff attempts as a function of the number of new calls with the CAC and a revised handoff scheme. We find that the number of handoff attempts do not increase after 100 users. Because of the CAC, only 100 users are accepted in each BS.

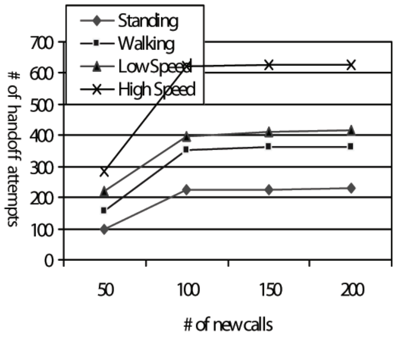

Fig. 6. The Number of Handoff Attempts vs. The Number of New Calls with a CAC.

VII. Conclusion

We designed a group key management tree such that the neighbors on the key tree are also physical neighbors on the cellular network. The group key management scheme uses the pre-positioned secret sharing scheme. By tracking the user location, we localized the delivery of rekeying messages to the nodes that need them. This lessens the amount of traffic in the cellular network. We find that each call undergoes an average of $3 \sim 8$ handoffs during a call duration according to the user mobility model. We proposed a new handoff scheme to minimize the key updating transactions. This new handoff scheme reduces one of the two key update transactions in the handoff region - adding a new channel when a call enters the handoff region. In the handoff area, only a new traffic channel is added to minimize the interruption time of the data transmission. With a the revised handoff scheme, the number of handoffs per call is reduced by almost 20% compared to that of the soft handoff. Also a simple CAC function is used to maintain key updating transactions to a level defined by the system manager.

References

[1] CDMA Technology Group, "http://www.cdg.org/technology/3g/," 2001.

[2] E. Lin, A. Eskicioglu, R. Lagendijk, and E. Delp, "Advances in digital video content protection," *Proceedings of the IEEE*, vol. 93, pp. 171–183, 2005.

[3] C. Wong, M.Gouda, and S. Lam, "Secure group communication using key graphs," *IEEE/ACM Transaction on Networking*, vol. 8, pp. 16–30, Febuary 2000.

[4] S. Mitta, "Iolus: A framework for the scalable secure multicasting," in *Proceedings of the ACM SIGCOMM'97*, September 1997, pp. 277–288.

[5] Y. Sun, W. Trappe, and K. J. R. Liu, "An efficient key management scheme for secure wireless multicast," in *Proceedings of the IEEE International Conference on Communication (ICC'02)*, 2002, pp. 1236–1240.

[6] D. BT *et al.*, "Secure group communications for wireless networks," in *Proceedings of the IEEE MILCOM 2001*, Mclean, VA, October 2001.

[7] *TIA/EIA Interim Standard (IS-95), Mobile Station - Base Station Compatibility Standards For Dual Mode Wideband Spread Spectrum Cellular System*, TIA/EIA Std., July 1993.

[8] N. Levanon, "Quick positioning determination using 1 or 2 LEO satellites," *IEEE Transactions On Aerospace and Electronic systems*, vol. 34, July 1998.

[9] K. Narenthiran, R. Tafazolli, and B. G. Evans, "Simple positioning method for location tracking in mobile satellite communications," in *Proceedings of the 18th AIAA International Communication Satellite Systems Conference*, Oakland USA, April 2000.

[10] G. J. Simmons, "How to (really) share a secret," *Proceedings of the Advances in Cryptology - CRYPTO'88 , Springer-Verlag*, pp. 390–448, 1990.

[11] ——, "Prepositioned shared secret and/or shared control schemes," *Proceedings of the Advances in Cryptology - EUROCRYPT'89, Springer-Verlag*, pp. 436–467, 1990.

[12] A. M. Eskicioglu and M. R. Eskicioglu, "Multicast security using key graphs and secret sharing," in *Proceedings of the Joint International Conference on Wireless LANs and Home Networks ICWLHN 2002 and Networking ICN 2002*, Atlanta, GA, August 26-29 2002, pp. 228–241.

[13] A. M. Eskicioglu, S. Dexter, and E. J. Delp, "Protection of multicast scalable video by secret sharing: Simulation results," in *Proceedings of the IEEE MILCOM 2001*, Santa Clara, CA, January 2003.

[14] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 11, pp. 612–613, November 1979.

[15] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*. New York: Dover Publications, 1974.

[16] H. Um, "Access control schemes for DS-CDMA cellular system supporting an integrated voice/data traffic," in *Proceedings of the SBT/IEEE International Telecommunications Symposium 1998*, August 1998, pp. 72–77.