

A FRAUD DETECTION METHOD USING IS-41C PROTOCOLS AND ITS APPLICATION TO THE THIRD GENERATION WIRELESS SYSTEMS*

D. G. Park^{1,2}, M. N. Oh¹, M. Looi²

¹ Wireless Communications Research Laboratory
Korea Telecom
park@isrc.qut.edu.au
omn@kt.co.kr

² Information Security Research Centre
Queensland University of Technology
mlooi@fit.qut.edu.au

ABSTRACT

Wireless fraud, in particular that caused by cloning, has become a global problem in public wireless mobile communications services. To overcome this problem, many kinds of detection technologies such as profiling, RF fingerprinting, PIN, and call history counter have been proposed. However, these still do not provide a high degree of fraud detection. The proposed detection mechanism in this paper is based on a challenge-response protocol, and can detect the occurrence of mobile cloning with a high degree of confidence while requiring minimal system resources.

INTRODUCTION

Over the last decade, wireless fraud, in particular that caused by cloning, has become a global problem in public wireless mobile communications services. According to an estimate by the Cellular Telecommunications Industry Association, nearly 90 % of cellular fraud in North America in 1995 was due to the cloning of cellular handsets (Figure 1) and more than 75,000 subscribers' handsets were cloned each month in the year [1].

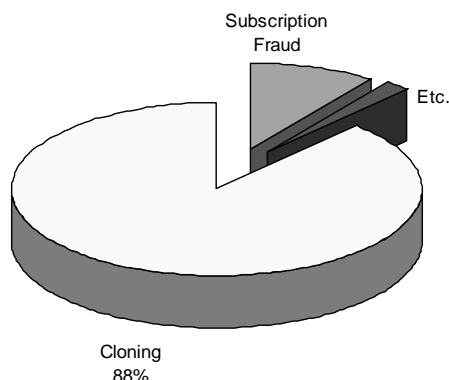


Figure 1 : Types of cellular fraud

To cope with cloning fraud, many kinds of detection technologies have been proposed. These include the use of PIN, profiling, RF fingerprinting, and call history counters. Most of these mechanisms were at first considered as add-on security solutions for the first generation analog cellular systems which have no inherent authentication protocols.

The current second generation systems and the proposed third generation systems have built-in authentication capabilities. However, these may still not be free from cloning fraud. Although made more difficult, copying or cloning of user/terminal data cannot be eradicated. Attackers will have to devise more sophisticated methods than just radio-scanning the mobile identity and the electronic serial number of a legitimate user's terminal because the secret information for authentication will never be transmitted over the air. One of the most common cloning methods is terminal-to-terminal copying which is believed to be one of the major sources of cloning fraud. Another method is getting secret authentication data from employees of wireless operators or certificate authorities. Authentication data could also be obtained from attacking the route for distributing secret authentication keys to subscribers, especially in the case of mail delivery and over-the-air activation. Finally, although rare, a cryptographic attack against authentication protocols and their corresponding algorithms may result in cloning being possible.

ALTERNATIVE SOLUTIONS FOR FRAUD DETECTION

Analysis of Usage Pattern

The most prominent among existing fraud detection methods is based on the analysis of the usage patterns of mobile users. This type of detection mechanism can be implemented through "rule-based approach" or "neural network approach"[2]. User profile analysis and Call

* This work was funded by Korea Telecom

Detail Records (CDRs) analysis are other names for this type of detection mechanisms. At first, it was conceived as an add-on solution for the first generation cellular systems without inherent authentication functions and protocols. However, even the third generation wireless systems such as UMTS (Universal Mobile Telecommunications System) are expected to use this kind of fraud detection methodologies [2] because of the reasons discussed above.

This approach for clone detection uses a profile analyzer (profiler) which gathers and analyses all the relevant usage data such as calling time, geographic position of mobiles, call duration, and call frequency. If the profiler finds an extraordinary discrepancy between the current call pattern and well-established usage pattern of the user, it reports that the call is "likely" to have been made by a cloned terminal.

However, there are some significant shortfalls of this mechanism. This mechanism entails having to install a profiler system separate from an authentication system, provide proper message transmission between the profiler and the other network elements, e.g. a mobile switch, and manage a considerable amount of data. Furthermore, the analysis of usage patterns of users - e.g. tracking of user's location, is an infringement on the privacy of users. Most of all, what this detection system gives out is not a fact but a probability of the occurrence of cloning fraud.

RF Fingerprinting

More recently, a new method called "RF fingerprinting" [3] has been developed and tried in the AMPS services. This can be thought of as a "mobile" version of profile analysis method. This RF fingerprint is the unique signal pattern emitted by a mobile terminal. This scheme needs to accumulate signal patterns of new users over initialization periods, and then compare the stored pattern with the incoming pattern of a mobile terminal on subsequent calls. As such, it requires an extra control system which maintains and updates the central database for the fingerprint of each mobile terminal. Furthermore, it entails quite a large investment in equipment for every base stations.

PIN

The oldest method of fraud control is using a personal identification number (PIN). Each user is given a secret PIN hopefully known only to the user and the authentication center. It requires users to enter their PIN when making calls. However, this is often an annoyance and can be easily defeated because the PIN itself is transmitted over the air.

Call History Count (COUNT)

North American second generation digital cellular sys-

tems based on IS-41C use a call history parameter, COUNT which has been introduced to detect cloning [4] . For every instance of mobile authentication, the network checks whether the received values of authentication response (AUTHR) and COUNT are equal to its own values of AUTHR' and COUNT' respectively (see Figure 2). If the values of both sides match, the mobile is given the access to the network. In the case of AUTHR match but COUNT mismatch, the subsequent action to handle the mismatch is not defined in the standard, and hence is up to the operators.

The value of COUNT is a modulo 64 binary number and is incremented by one under the control of the network, at intervals defined by the network operator. Once the value of COUNT is updated for a terminal that has been cloned, the value of COUNT within the Authentication Center (AC) will match only one of either the original terminal or the cloned terminal.

In the case that the Shared Secret Data (SSD) value of a particular mobile has been cloned, as soon as a COUNT mismatch has been detected, the network can update the SSD of the terminal (refer to Figure 3 and Figure 5). Therefore the cloned terminal will operate no longer. However, if the cloned terminal includes a true copy of the authentication key (A-key), the cloned terminal is able to respond correctly to the SSD update. Hence, using the call history count by itself for fraud detection and management is insufficient.

Furthermore, the possibility of COUNT mismatch between a legitimate terminal and the AC cannot be ruled out, which may be a result of failure within the terminal or network or over the radio interface. After all, the final step in fraud management will need some enquiry to the mobile customer whose terminal is believed to have been used by fraudsters to make another illegal copy. Such a process might annoy the customer, especially if the suspicion has been found to be mistaken. Therefore, IS-41C network operators will need a more accurate clone detection method which enables them to be confident in their decision that cloning has been done for a particular mobile.

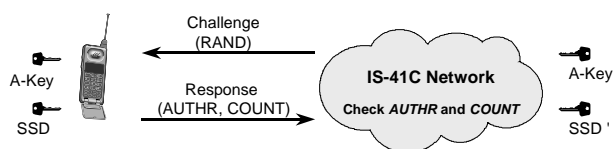


Figure 2: Authentication mechanism of IS41-C

SSD: IS-41C'S HIDDEN FRAUD DETECTION METHOD

The Shared Secret Data (SSD) parameter mentioned above was originally introduced to share the load of authentication processing and signalling between the home Authentication Center (AC) and the visited system's Visiting Location Register (VLR). With SSD shared, the VLR can calculate the authentication response AUTHR and compare it with that received from the corresponding mobile terminal. The home AC does not need to authenticate the mobile. Of course, this secret data may or may not be shared, and it is up to the operators.

The SSD in this paper, however, is used as another kind of security measure. We propose to use the SSD for clone detection as well.

Security Data in IS-41C

The security mechanism of IS-41C has more types of security related data than its European counterpart, GSM. Above all, it has one more key level which is composed of SSD-A and SSD-B. The former is for authentication purposes and the latter for ciphering services (Figure 3). This will add up to stronger security for the master key, A-key because it is not the A-Key itself but the SSD that is used to derive the authentication response, AUTHR. SSD can be viewed as a temporary copy of the A-Key. The AC can decide the SSD update period and change the SSD value of a particular mobile anytime when it wants to do.

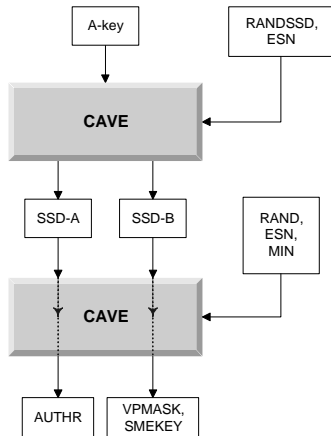


Figure 3 : Security related data and their relations in IS-41C

Authentication Response Handling and Local Administration Procedures

Authentication success for a particular mobile station means that both of the values of AUTHR and COUNT sent from it equal the corresponding values stored within

the Authentication Center. On the other hand, a mismatch in one or both of the authentication parameters is regarded as authentication failure. The standard does not specify how to handle the authentication failures. The required handling capability or logic is treated as a black box and just called "local administration procedures" within the standard documentation [4] .

IS-41C provides too many optional security measures compared to the simple features of European GSM system. These are call history count parameter (COUNT), temporary secret key (SSD) and two kinds of challenge-response protocols: global challenge and unique challenge. The local administration procedures may use some or all of the above security measures appropriately. In this paper, we only focus on SSD, COUNT and their update protocols in the viewpoint of their use for cloning detection.

The COUNT parameter is described in a previous section, and we describe the SSD update procedure in the following section.

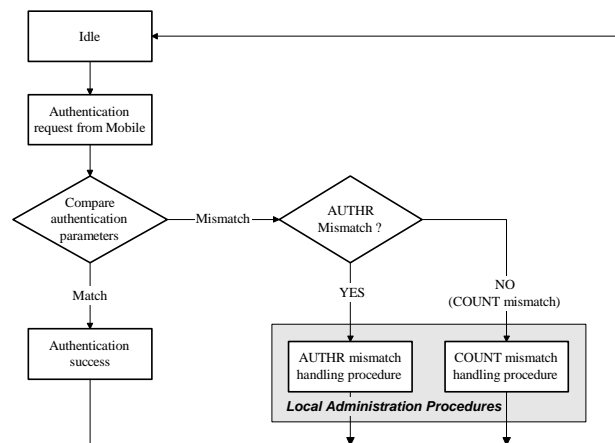


Figure 4 : Local administration procedures for handling "authentication failure"

SSD Update Procedure

This procedure(see Figure 5) is the most powerful response to any kind of security problem detected. It provides a feature of restart or reset of security data to both the mobile station and the AC. It can be used to handle any kind of security violations such as AUTHR mismatch, COUNT mismatch, etc. The SSD Update procedure, however, should be used sparingly because it is the most resource consuming method amongst several procedures provided by IS-41C security protocol. The following figure provides a simplified view of this procedure.

In the following section, we show that this SSD Update procedure is a built-in security bullet for cloning detection in IS-41C networks.

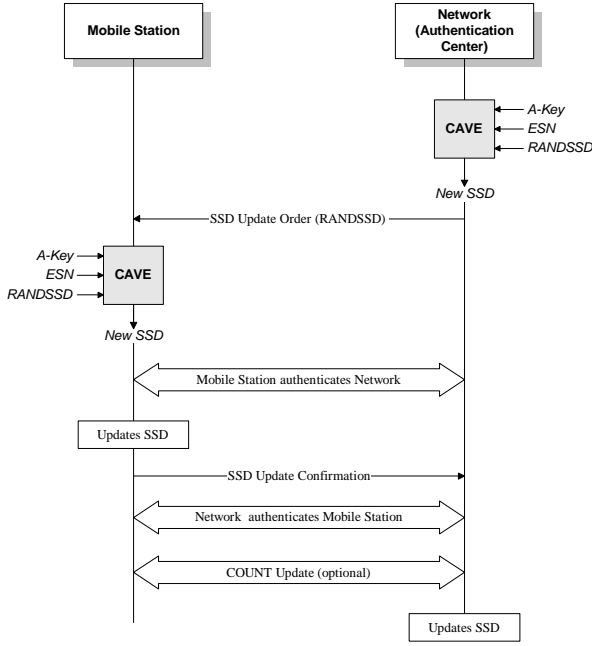


Figure 5: SSD Update procedure in IS-41C

Cloning Detection Using SSD Update Procedure

Assume that an attacker has succeeded in making an exact duplicate of a legitimate user's mobile station (MS). The cloned phone will have the same secret authentication key (A-key) as the original phone. It is impossible for authentication center (AC) to distinguish between the authentic mobile station and its illegal copy. In fact, the detection of cloning in this paper means that the AC has detected that cloning had happened for a particular MS. If we denote MS and MS' as two mobile stations having exactly the same authentication data, the authentication data status of MS, MS' and AC will be as following.

MS	AC	MS'
$A-Key_{MS} = A-Key_{AC} = A-Key_{MS'}$		
$SSD_{MS} = SSD_{AC} = SSD_{MS'}$		
$COUNT_{MS} = COUNT_{AC} = COUNT_{MS'}$		

Table 1 : Initial state of authentication data in MS, MS' and AC

If one of the twin mobiles, e.g., MS, accesses to network and AC and MS execute the COUNT update procedure, the security data status will change as follows.

MS	AC	MS'
$A-Key_{MS} = A-Key_{AC} = A-Key_{MS'}$		
$SSD_{MS} = SSD_{AC} = SSD_{MS'}$		
$COUNT_{MS} = COUNT_{AC} \neq COUNT_{MS'}$		

Table 2 : The agreement/disagreement state of authentication data in three parties, after COUNT update between MS and AC

After that, if MS' tries to access the network, it will necessarily cause the COUNT mismatch event to happen within the AC system and MS' may be denied access. This access failure does not seem to dissuade the user of MS' (authentic or fraudulent) from second, third or more tries to make a call. Hence, if system operator has set the AC to issue SSD Update procedure for a preset threshold number of COUNT mismatches, MS' with the true A-Key will derive the same value of new SSD with that of AC, and succeed in the procedure. In addition to the SSD Update procedure, AC of IS-41C network should initiate some correction procedure for re-agreement of COUNT values between AC and MS'. Unfortunately, however large discrepancy of COUNT values between two entities is, there is no one-step method to get the agreement. AC should send COUNT update order (each for one increment) to MS repeatedly until they are in the agreement of COUNT values. Instead, the operators may prefer to change the COUNT to the same value of that stored in MS'. After that, MS' will be in the exact agreement state with AC and MS in a disagreement state (see the following table) in turn.

MS	AC	MS'
$A-Key_{MS} = A-Key_{AC} = A-Key_{MS'}$		
$SSD_{MS} \neq SSD_{AC} = SSD_{MS'}$		
$COUNT_{MS} \neq COUNT_{AC} = COUNT_{MS'}$		

Table 3 : The agreement/disagreement state of authentication data in three parties, after SSD update between MS' and AC

Now, whenever the MS tries to access the network, it will suffer the AUTHR mismatch as well as COUNT mismatch because the MS' and AC has updated their values of SSD which is different from the old value of SSD which is still being used by the MS. This disagreement of SSD between the MS and the AC will cause subsequent AUTHR and COUNT mismatch events in the AC system quite often. This phenomenon will trigger SSD update procedure again, and the MS will succeed in the update procedure and authentication check. The agreement/disagreement state of the three entities will be like the Table 3.

MS	AC	MS'
$A-Key_{MS} = A-Key_{AC} = A-Key_{MS'}$		
$SSD_{MS} = SSD_{AC} \neq SSD_{MS'}$		
$COUNT_{MS} = COUNT_{AC} \neq COUNT_{MS'}$		

Table 4 : The agreement/disagreement state of authentication data in three parties, after SSD update between MS and AC

This scenario will necessarily repeat until the operator takes any kind of recovery action. Now we can find a

pattern of the sequential events.

- ◆ Repeated COUNT mismatches for a particular mobile station
- ◆ SSD update success for the mobile station
- ◆ Repeated AUTHR mismatches for the mobile station
- ◆ SSD update success for the mobile station
- ◆ Repeated AUTHR mismatches for the mobile station

Here we can see that cloning will inevitably cause repeated events of AUTHR mismatch and the SSD update success to happen. Of course, this sequence of events might be interleaved by another irregular event such as repeated authentication successes. However, the repetition of the above pattern within a time period will be a clear indicator of the existence of a cloned phone. It should be noted that this pattern may happen even if the IS-41C network did not employ the COUNT parameter in the authentication protocol. This is because the SSD update procedure is recommended to be executed periodically for security, which will bring a disagreement of SSD values between the AC and MS/MS'.

The observation of the stereotyped pattern may be implemented into the AC local administration procedure in many different ways. Using this, IS-41C network operators will be able to detect cloning with high confidence using the AC and its built-in local administration procedures without deploying any special add-on system at extra cost. Such an AC system is depicted in the following figure.

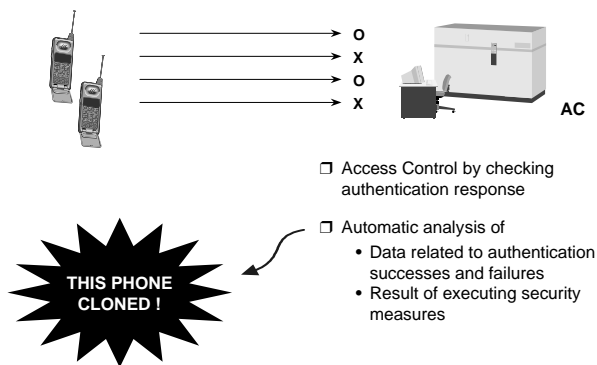


Figure 6 : Cloning detection within AC system without any add-on special purpose system

APPLICATION TO THIRD GENERATION WIRELESS SYSTEMS

Future wireless systems are considering public key cryptographic systems for their authentication purposes[5],[6]. The temporary secret key concept discussed in this paper can also be applied to the future wireless systems for detection of cloning. The application scenario for the future systems based on asymmetric tech-

niques is described below.

The network assigns a permanent secret key, K_p (analogous to A-Key in IS-41C) to a new user, from which a temporary secret key K_t (analogous to SSD in IS-41C) is to be calculated. K_t then, can be used as an input together with COUNT to a hash function to calculate the authentication response AUTHR. Figure 7 shows the computation procedure in both the mobile station and the network for the temporary key and the corresponding response value.

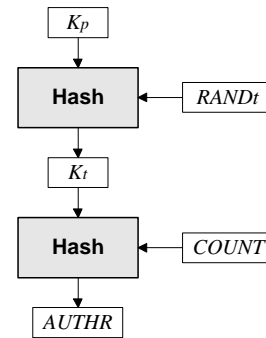


Figure 7: The procedure for the calculation of the temporary key and authentication response

$RAND_t$, a random challenge for K_t update, is to be chosen only by the network like $RAND_{SSD}$ in IS-41C protocol. The K_t update procedure, which is just similar to the SSD update procedure in IS-41C, will cause a discrepancy of AUTHR values between the network and the legitimate terminal or the illegal terminal once both terminals have been used subsequent to the cloning.

The COUNT parameter is also used in this scheme, not as a call history key, K_t . The network does not need to explicitly check if COUNT values of both the mobile station and the network match because the mismatch will lead to the AUTHR mismatch (see Figure 7). In addition, the COUNT should be updated automatically without any additional message exchange between the mobile station and the network, and always reset to zero value after successful K_t update. This relieves the network of signalling load which was required for the COUNT Update procedure in IS-41C network. In the case of IS-41C, the COUNT parameter is a call history of the mobile station and can be updated only by the relevant update order from the AC. IS-41C's COUNT has no way to be reset and can just be incremented by one. In the event of COUNT mismatch, the overhead to restore COUNT value may be formidable.

Figure 8 shows the application scenario. In the diagram, it is assumed that there is more than one mobile station with the same identity and authentication data, except that the temporary secret key K_t may be different. The clone detection parameter, AUTHR is sent from the mobile station to the network during the execution of the public-key based authentication procedure. It may be

transmitted in clear or encrypted. The network updates the event counter for the mobile station whenever it passes the public-key based authentication but fails in the secret-key authentication, and then updates the temporary key successfully. If the event count is greater than or equal to the threshold value (the value of 2 will be enough), it indicates that cloning of the phone has occurred. It should be noted that this cloning detection procedure does not need to be executed entirely on-line in real-time. Public key based authentication procedure will be executed between the mobile station and the visited network, and the secret key based cloning detection check and calculations may be executed off-line within the mobile station's home network.

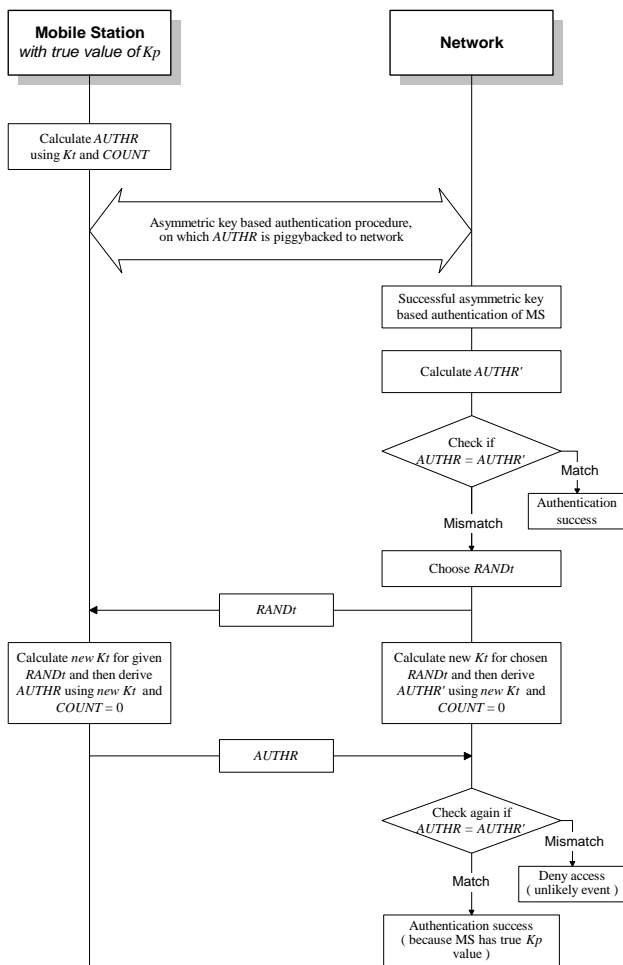


Figure 8 : Application scenario of the secret temporary key

CONCLUSION

Fraudulent usage, especially by cloning fraud, in wireless mobile communication service has forced the operators to seek for effective clone detection methods. Most of the proposed schemes require the operators to invest

considerable amount of money and modify their network infrastructure to deploy the schemes.

What if there is already built-in a more effective clone detection method in the authentication protocol itself? This paper shows that the IS-41C system has a hidden mechanism for clone detection which enables the operators to be confident in their decision about cloning fraud. This method just makes use of the SSD, a temporary secret key in IS-41C which was originally introduced for load sharing between the home network and the visited network.

Furthermore, the concept of clone detection usage of a temporary secret key can be applied to future wireless systems. If the future systems' security infrastructure is compatible with that of IS-41C systems, the application is just straightforward. On the other hand, for the systems with more sophisticated security infrastructure based on asymmetric techniques, the clone detection method can also be applied with some modifications.

REFERENCES

- [1] Eric Hill, "Fraud Trends in North America - US and Canada," Proceedings of the Conference on Fighting Mobile Fraud, IBC UK Conferences, London, 1996.
- [2] ACTS AC095, project ASPeCT, Definition of Fraud Detection Concepts, AC095/KUL/W22/DS/P/06/A, 1997.
- [3] US Patent 5,448,760, M. B. Frederick et al., Cellular Telephone Fraud Anti-Fraud System, Sep. 5, 1995.
- [4] TIA/EIA/IS-41-C (PN-2991.3), Cellular Radiotelecommunications Intersystem Operations: Automatic Roaming Information Flows, May 4, 1995.
- [5] ITU-R Recommendation M.1223, Evaluation of Security Mechanisms for IMT-2000, 1997.
- [6] ACTS AC095, project ASPeCT, Initial Report on Security Requirements, AC095/ATEA/W21/DS/P/02/B.2, Feb., 1996.