International Journal of Innovative Research in Computer Science and Engineering (IJIRCSE)
www.ioirp.com ISSN: 2394-6364, Volume – 1, Issue – 6. May 2015

AN USING A SIM-LESS DEVICES AGAINST A DENIAL OF SERVICE ATTACK TO UMTS NETWORK

[1]VINOTH RAJA.G, [2]JAISON VIMAL RAJ.T
[1]PG Student (M.E-Mobile and pervasive Computing) Department of Computer Science and Engineering
[2]Assistant Professor, Department of Computer Science and Engineering
[12]University college of Engineering, Anna University BIT Campus Trichy, India
[1]vinothrajamalik@gmail.com

Abstract— One of the fundamental security elements in cellular networks is the authentication procedure performed by means of the Subscriber Identity Module that is required to grant access to network services and hence protect the network from unauthorized usage. Nonetheless, in this work we present a new kind of denial of service attack based on properly crafted SIM-less devices that, without any kind of authentication and by exploiting some specific features and performance bottlenecks of the UMTS network attachment process, are potentially capable of introducing significant service degradation up to disrupting large sections of the cellular network coverage. The knowledge of this attack can be exploited by several applications both in security and in network equipment manufacturing sectors.

Keywords— Mobile securities, UMTS cellular network security, HLR, DOS attack.

I. INTRODUCTION

UMTS supports maximum theoretical data transfer rates of 42 Mbit/s when HSPA+ is implemented in the network. Users in deployed networks can expect a transfer rate of up to 384 kbit/s for Release '99 (R99) handsets (the original UMTS release), and 7.2 Mbit/s for HSDPA handsets in the downlink connection. These speeds are significantly faster than the 9.6 kbit/s of a single GSM error-corrected circuit switched data channel, multiple 9.6 kbit/s channels in **HSCSD** and 14.4 kbit/s for CDMA One channels.Work is also progressing on improving the uplink transfer speed with the High-Speed Uplink Packet Access (HSUPA). Longer term, the 3GPP Long Term Evolution (LTE) project plans to move UMTS to 4G speeds of 100 Mbit/s down and 50 Mbit/s up, using a next generation air interface technology based upon orthogonal frequency-division multiplexing.

UMTS phones can use a Universal Subscriber Identity ModuleUSIM (based on GSM's SIM) and also work (including UMTS services) with GSM SIM cards. This is a global standard of identification, and enables a network to identify and authenticate the (U)SIM in the phone. Roaming agreements between networks allow for calls to a customer to be redirected to them while roaming and determine the services (and prices) available to the user. In addition to user subscriber information and authentication information, the (U)SIM provides storage space for phone book contact. Handsets can store their data on their own memory or on the (U)SIM card (which is usually more limited in its phone book contact information). A (U)SIM can be moved to another UMTS or GSM phone, and the phone will take on the user details of the (U)SIM, meaning it is the (U)SIM (not the phone) which determines the phone number of the phone and the billing for calls made from the phone.Even with current technologies and low-band UMTS, telephony and data over UMTS is still more power intensive than on comparable GSM networks. Apple Inc. cited UMTS power consumption as the reason that the first generation iPhone only supported EDGE. Their release of the iPhone 3G quotes talk time on UMTS as half that available when the handset is set to use GSM. Other manufacturers indicate different battery lifetime for UMTS mode compared to GSM mode as well. As battery and network technology improves, this issue is diminishing.

II. RELATED WORK

Almost all UMTS phones are UMTS/GSM dual-mode devices, so if a UMTS phone travels outside of UMTS coverage during a call the call may be transparently handed off to available GSM coverage. Roaming charges are usually significantly higher than regular usage charges.UMTS phones (and data cards) are highly portable—they have been designed to roam easily onto other UMTS networks. In addition, almost all UMTS phones are UMTS/GSM dual-mode devices.This is facilitated by the fact that GSM/EDGE and UMTS specification are jointly developed and rely on the same core network allowing dual-mode operation including vertical handovers.The UMTS network introduces new network elements that function as specified by

3GPP:Node B (base transceiver station),Radio Network Controller (RNC),Media Gateway (MGW).so that the standard bands most commonly used for UMTS (UMTS-2100) have not been available.alternative bands are used, preventing the interoperability of existing UMTS-2100 equipment, and requiring the design and manufacture of different equipment for the use in these markets. As is the case with GSM900 today, standard UMTS 2100 MHz equipment will not work in those markets.

III. Design Method

A. Conventional Design

The conventional design of the UMTS also specifies the Universal Terrestrial Radio Access Network (UTRAN), which is composed of multiple base stations, possibly using different terrestrial air interface standards and frequency bands.

UMTS and GSM/EDGE can share a Core Network (CN), making UTRAN an alternative radio access network to GERAN(GSM/EDGE RAN), and allowing (mostly) transparent switching between the RANs according to available coverage and service needs.

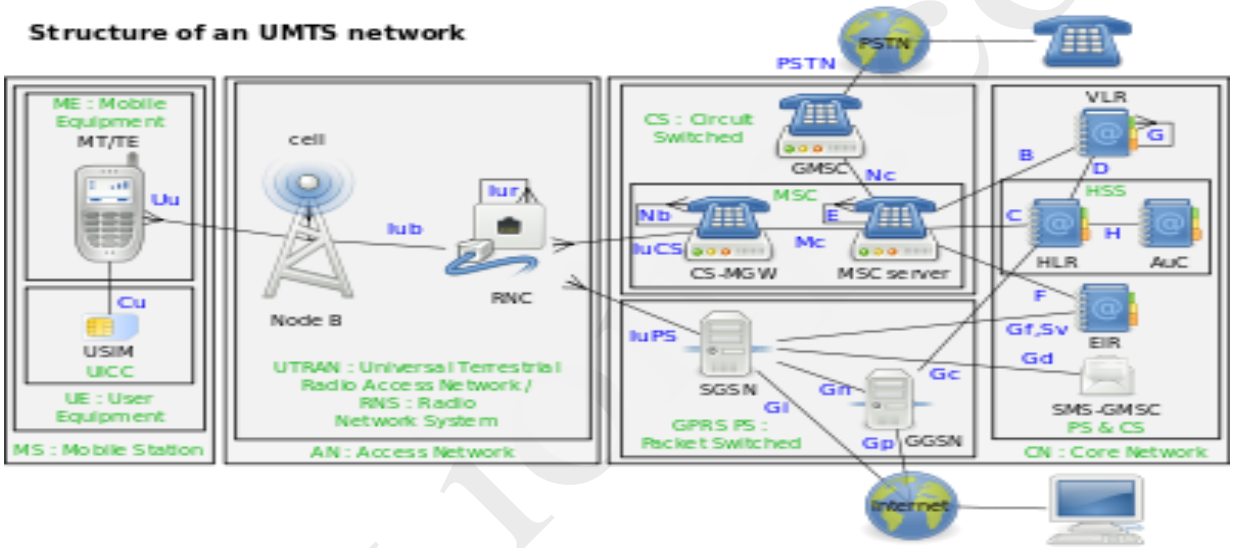

Fig1. Flow chat for UMTS

B. System Design

In this system design using set of modules will be followed in the architecture. These modules are

System architecture is shown in figure 2

/

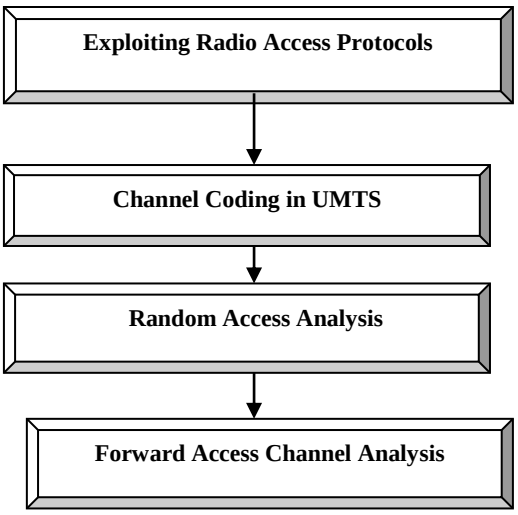

Fig 2: System Architecture

- *Exploiting Radio access protocols*

When a mobile cellular device is powered on, the UMTS protocol defines the actions that should be carried on in order to attach to the network. A high level description of the network access procedure can be sketched in the following common steps: i) cell discovery, ii) best server synchronization, iii) attachment request, iv) authentication and key agreement (AKA) and v) temporary identity creation.

- *Channel coding in UMTS*

The work however, does not provide an assessment for the HLR/AuC performance impact, thus they do not estimate the number of terminals needed by an attacker in order to considerably degrade HLR services, that is the most strategic component affected, by using the attack described above. A partial analysis of this problem is provided. They choose the insert call forwarding procedure as the attack vector because it offers the best tradeoff between computational load and execution speed. A standard mobile phone controlled via the AT inter- face has been used to simulate the effect of injecting attack traffic on a HLR already serving a typical mix of transactions.

- *Random Access Analysis*

The first UMTS bottleneck we take into account is RACH. Before accessing the RACH, the MS has to send out some short preambles, with increasing power, until Node B acknowledges the reception over the Acquisition Indicator Channel (AICH): the procedure is defined in this way in order to select the minimum power needed to reach the Node B itself. Preambles consist of 256 repetitions of a 16 chips long Walsh-Hadamard sequence: in this way, the MS may randomly choose among 16 sequences. Once the output power has been calibrated, the mobile phone may transmit its single transport block message over the RACH, which usually takes a 20 ms transmission time interval. Sticking to the single-device hypothesis, and considering that, being the attacking device stationary.

- *Forward Access Channel Analysis:*

Once the network has received the rrc Connection Request, it assigns dedicated resources via rrc Connection Setup message sent over the FACH, a shared downlink channel. This message is relatively large as it typically requires seven trans- port blocks of 168 bits each, transmitted by multiplexing them in couples, using 10 ms TTI.

C. Proposed Design

To analyze the peculiarities of UMTS radio interface at the protocol layer in order to evaluate its potential attack surface and limits in terms of number of attach requests sent to a Node B station per second. In this process we suppose to be the only device communicating with the target cell. This hypothesis seems unrealistic, but is a direct consequence of the unfairness of the attacking device: while legitimate mobile phones would back-off when facing a traffic problem, the attacking device actively works toward the consumption of all the cell's resources. Thus, most of the time a mobile phone tries to get access; it will not be served because of the high number of requests injected by the attacking device.

Moreover, as soon as a legitimate request completes, the high number of requests injected by the attacking device are likely to allow the attacker to grab the resources just freed, making it unavailable to legitimate devices.This code sequence is also called the chip sequence and a chip is the sub-period in which the pseudo noise code sequence cannot change. Thus while the original signal does not change for the bit period, the coded signal does not change only for the shorter chip period. The resulting coded signal is transmitted over the radio channel. Due to the differences in data rates between services, and because the output speed is fixed, the system should be able to apply variant scaling factors. results in an output rate directly proportional to the code length: this fact leads to the concept of spreading factor (SF) which is defined as the number of chips sent for each bit of information. However, the most important property belonging to Walsh-Hadamard codes is orthogonality, meaning that two different sequences of the same length may be multiplied together chip-by-chip and then add up the results leading to a total value equal to zero.

International Journal of Innovative Research in Computer Science and Engineering (IJIRCSE)
ISSN: 2394-6364, Volume – 1, Issue – 6. May 2015

IV. SIMULATION RESULTS

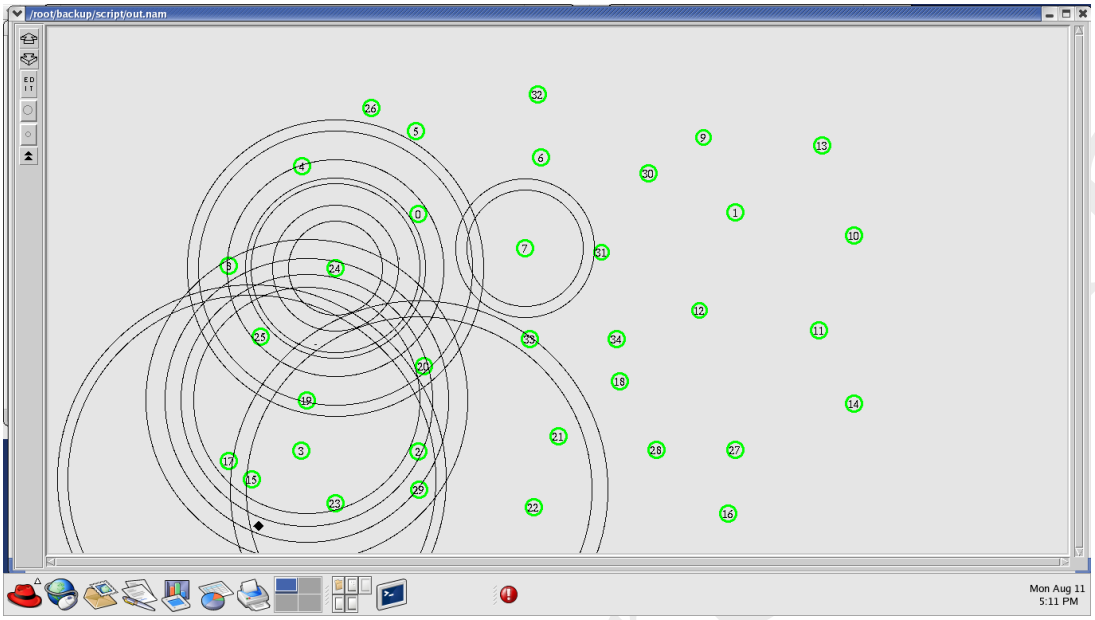

Fig 3:NAM output for Node localization and Data transmission.

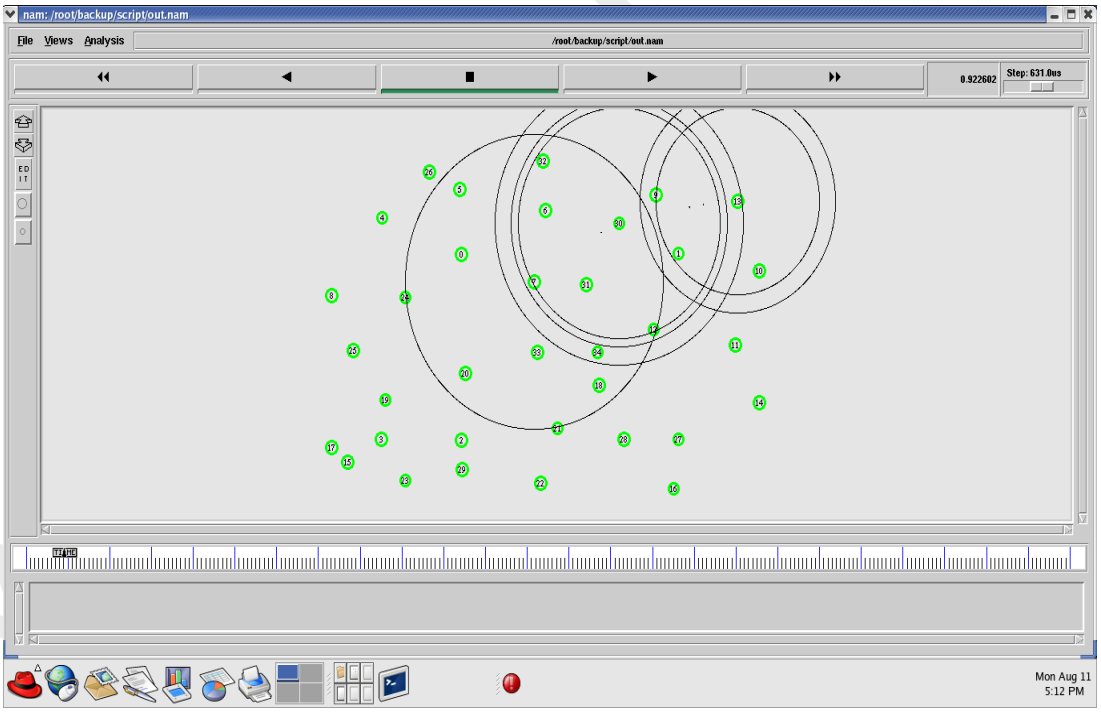

Fig 4: NAM output for Node localization and Data transmission

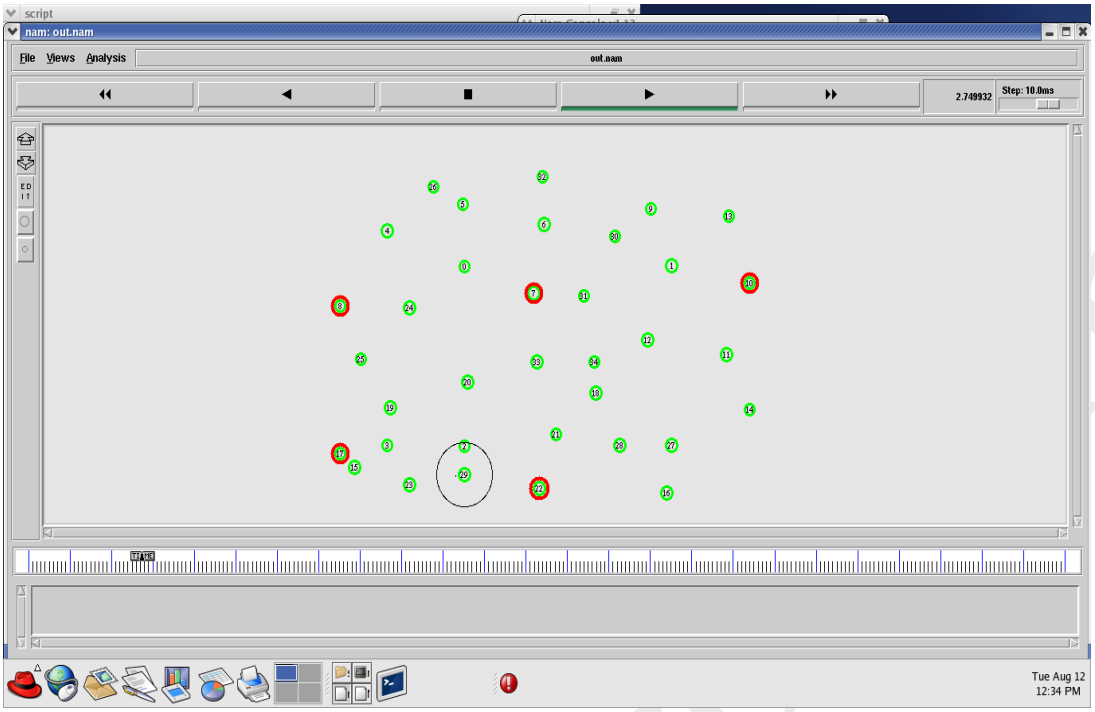

Fig 5:NAM window represents the nodes which are in reduced energy

V. CONCLUSION

The state-of-the-art attack methodologies are based on GSM network alone and require the availability of botnets with more than 10.000 smart-phones with valid SIM modules. In this work, we have explored a different approach, leveraging the 3G UMTS network and evaluating the possibility to bypass the strict timings enforced by the cellular network protocols by means of radio devices different from the ones available on the attacking devices.

References

[1] S. Capkun, M. Cagalj, R. Rengaswamy, I. Tsigkogiannis, J.-P. Hubaux, and M. Srivastava, "Integrity codes: Message integrity protection and authentication over insecure channels," IEEE Trans. Dependable Secure Comput., vol. 5, no. 4, pp. 208–223, Oct.- Dec. 2008.

[2] Y.-L. Huang, F.-Y. Leu, and K.-C. Wei, "A secure communication over wireless environments by using a data connection core," Math. Comput. Modelling, vol. 58, no. 5, pp. 1459–1474, 2013.

[3] A. Castiglione, G. Cattaneo, A. De Santis, F. Petagna, and U. Ferraro Petrillo. 2006. "SPEECH: Secure personal end-to-end communication with handheld," in Proc. ISSE Securing Electronic Busines Processes. Vieweg, pp. 287–297, [Online]. Available: http://dx.doi.org/10.1007/978-3-8348-9195-2_31

[4] Y.-L. Huang, F.-Y. Leu, I. You, Y.-K. Sun, and C.-C. Chu. (2014). A secure wireless communication system integrating RSA, Diffie-Hellman PKDS, intelligent protection-key chains and a Data Con- nection Core in a 4G environment. J. Supercomput. [Online]. 67(3), pp. 635–652. Available: http://dx.doi.org/10.1007/s11227-013- 0958-z

[5] B. Blanchet, "A computationally sound mechanized prover for security protocols," IEEE Trans. Dependable Secure Comput., vol. 5, no. 4, pp. 193–207, Oct.-Dec. 2008.

[6] P. Traynor, M. Lin, M. Ongtang, V. Rao, T. Jaeger, P. McDaniel, and T. La Porta, "On cellular botNets: Measuring the impact of malicious devices on a cellular network core," in Proc. 16th ACM Conf. Comput. Commun. Security, 2009, pp. 223–234.

[7] (2013). United States Department of Homeland Security. NIPP 2013: National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience. [Online]. Available: http://www.dhs.gov/publication/nipp-2013-partnering-critical- infrastructure-security-and-resilience