International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Denial of Service Attack to UMTS (Radio) Networks Using Sim-Less Devices to Increase Network Efficiency

J Pramod Kumar[1], Abdul Wasay Mudasser[2]

[1]M. Tech Student (Wireless and Mobile Communication), Department of Electronics and Communication Engineering, Lords Institute of Engineering & Technology, Hyderabad, India

[2]Associate Professor, Dept. of ECE, Lords Institute of Engineering & Technology, Hyderabad, India

Abstract: ***One of the fundamental security elements in cellular networks is the authentication procedure performed by means of the Subscriber Identity Module (SIM) that is required to grant access to network services and hence protect the network from unauthorized usage. Nonetheless, in this proposed work we present a new kind of denial of service (DoS) 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 Universal Mobile Telecommunication System (UMTS) network attachment process, are potentially capable of introducing significant service degradation up to disrupting large sections of the cellular network coverage. Beyond protocol-specific vulnerabilities, the same network complexity may also hide potential performance bottlenecks in signalling protocols or control applications or components that can be exploited by several kinds of Denial of Service (DoS) attacks in order to tear down critical service subsystems or overwhelm them with large number of requests, exhausting the resources needed to ensure network operations. The knowledge of this attack can be exploited by several applications both in security and in network equipment manufacturing sectors.***

Keywords: Universal Mobile Telecommunication System (UMTS), Denial of Service (DoS), Subscriber Identity Module (SIM)

1. Introduction

Mobile phones based on cellular networks are one of the most successfully deployed technologies of the last decades and coverage of cellular networks in the world has generally become pervasive. Both an effect and a cause of this success may be seen in the evolutional cycle of the network technologies. In fact, while the evolution from early analog networks to recent 3G/4G solutions has allowed Mobile Network Operators(MNOs) to offer new services to their customers, the same time it has pushed new needs into the customers that, closing the cycle, require more resources to be supported. As an example, we may observe how the user needs have evolved from simple voice and short text message communications to high speed Internet connections and ubiquitous access to multimedia streams and storage repositories made possible by the introduction of General Packet Radio Service (GPRS) allowing data delivery according to both the circuit and packet switched paradigms. In this scenario, mobile communication networks have gained the role of critical infrastructure for the global community like transportation or electricity so that many individuals and business activities relying on them for their day-to-day operations may be severely impacted by any service degradation or disruption. It is thus critical to tackle the problem of security in mobile networks from every possible perspective, not only focusing on the confidentiality and integrity of codes [1], end-to-end connections [2], [3] information flows [4] but also considering the availability of the network itself. The complexity of the mobile network structure may hide both unknown and known vulnerabilities that proper analysis tools and formal techniques can unveil [5].

Beyond protocol-specific vulnerabilities, the same network complexity may also hide potential performance bottlenecks in signalling protocols or control applications/components that can be exploited by several kinds of Denial of Service (DoS) attacks in order to tear down critical service subsystems or overwhelm them with large number of requests, exhausting the resources needed to ensure network operations. Nonetheless, the potential impact of these attacks on mobile phone networks has not been sufficiently assessed and needs further study.

By focusing on the node attachment procedure in Universal Mobile Telecommunications System (UMTS) infrastructures, shows that it is possible to mount a full-fledged DoS attack potentially capable of shutting down large sections of the network coverage without the need of hijacking or controlling actual users' terminals, as well as that the number of devices necessary to make such an attack effective is limited to a few hundred ones. This attack exclusively operates at the user-level by relying on unavoidable protocol level signalling features so that no hacking on intra-operator facilities is needed. It is indirectly targeted at the Home Location Register (HLR) that is the database containing information on mobile subscribers as well as call blocking and forwarding rules that can be overwhelmed by service requests [6]. Since this database is a critical component, often revealing to be a major bottleneck within the overall infrastructure, an outage of its functionality may cause an interruption of other mobile services too, finally resulting in a mobile network DoS potentially leaving thousands of devices without their lifelines to the network core. Furthermore, the presented attack does not require the use of real mobile handsets equipped with valid Subscriber Identity Module (SIM) modules and needs only a limited number (a few hundred) of

UMTS radio interfaces, eventually located on a single ad-hoc device, in order to inject the signalling traffic necessary to reach a critical level of disruption on the target cellular infrastructure.

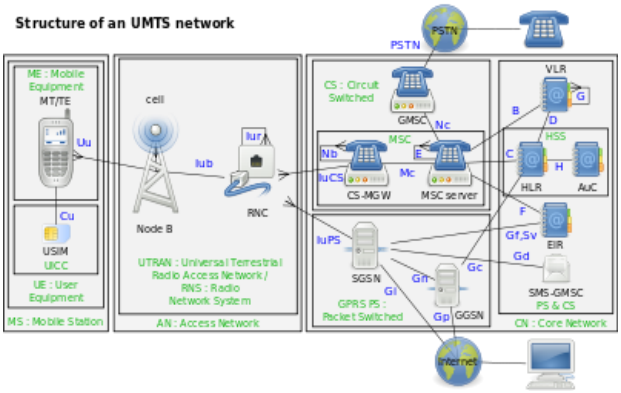

Figure 1: UMTS Network Architecture

2. UMTS Network Introduction

A typical UMTS Public Land Mobile Network(PLMN) architecture (see Fig. 1) is divided into three main building blocks: Mobile station (MS): The MS or user equipment (UE) may be a mobile phone/terminal or a mobile broadband modem providing UMTS protocol stack and radio access capabilities. It is marked with a worldwide unique identifier, called International Mobile Equipment Identity (IMEI) and equipped with a SIM in order to allow end user identification and authentication based on a unique subscriber identifier, the International Mobile Subscriber Identity (IMSI), together with its associated private cryptographic key.UMTS Terrestrial Radio Access Network(UTRAN) Core network (CN): The CN connects each RNC to the Serving GPRS Support Node(SGSN) and to the mobile switching center (MSC), in order to transport, respectively, packet and circuit switched information. MSC and SGSN also interconnect the UTRAN. The structure of UMTS network is given above.

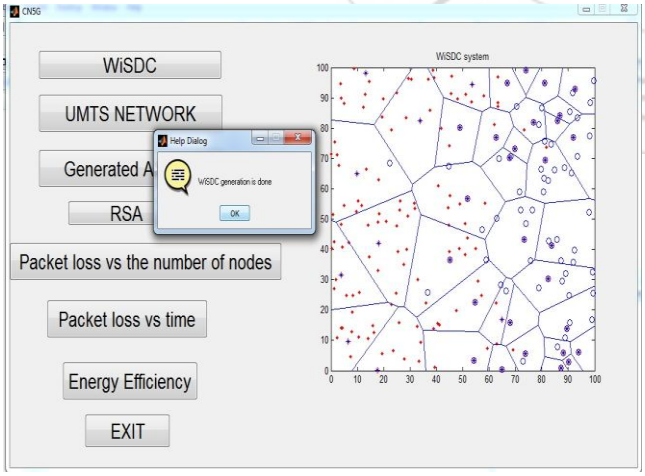

Figure 2: Generation of a normal Radio network

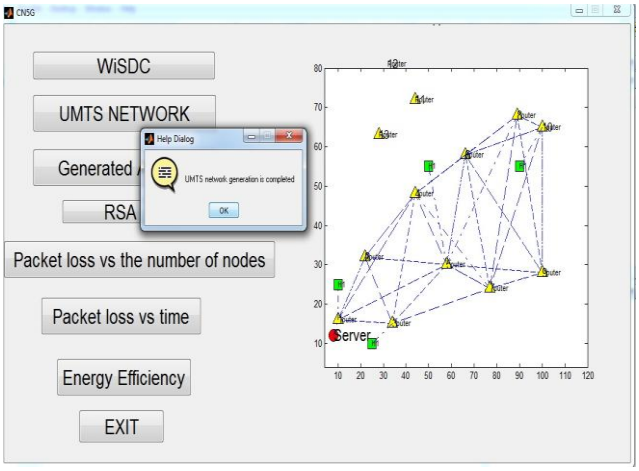

Figure 3: Generation of UMTS network

3. Existing Methods

3.1 Jamming attacks

The simplest way to prevent a mobile network from offering its services is using a radio jammer. Four jamming models differing in type and duration of the emitted signal and study the feasibility of detecting such attacks. They show that a jammer always injecting regular data, called deceptive, is the most effective one but the random version. It alternates between sleeping and transmitting, may represent a valid alternative taking energy conservation in consideration. Even with smart, protocol-specific intrinsic trade-off between finite power supply and continuous transmission make this kind of attack limited both in space and time. Signal strength or packet delivery ratio. It is not enough to spot an ongoing jamming attack. Thus they define two algorithms are defined based on classification and consistency check phases that mix together multiple indicators in order to conclude the presence of a jammer. The mobile network outlier moving from physical towards upper layers increases both the complexity of the attack and the size of the involved network segment. In order to be able to prove higher layer attacks possible, researchers have had to wait for a device with extensible capabilities. A kind of device that made its first market appearance in 2000 but actually had a significant deployment only in 2007.

3.2 Smartphone botnet attack

Past Internet security studies prove in order to mount a DoS attack a botnet is the tool that provides the most suitable characteristics. Mobile networks have constraints and peculiarities that should be taken into consideration. The model both a single mobile operator's network topology and different contact graph distributions. By leveraging the generally distributed architecture of VOIP services, a VOIP infection can reach 70% of users in around 4 hours generating major congestion effects on the RNC-to-SGSN link. On the other hand, MMS infection spreads at a much slower pace because it is constrained by a few centralized servers that act as bottlenecks. Creating a mobile phone botnet is generally more challenging than doing it with traditional Internet nodes. This derives both from the fact that mobile phone nodes are usually less apt at running daemon processes and to the fact that most of the time

mobile phones are connected to the internet with a private IP address.

3.3 Telephony Denial-of-Service

Voice over IP has made abusive origination of large numbers of telephone voice calls inexpensive and readily automated while permitting call origins to be misrepresented through caller ID spoofing. According to the US Federal Bureau of Investigation, telephony denial-of-service (TDoS) has appeared as part of various fraudulent schemes: A scammer contacts the victim's banker or broker, impersonating the victim to request a funds transfer. The banker's attempt to contact the victim for verification of the transfer fails as the victim's telephone lines are being flooded with thousands of bogus calls, rendering the victim unreachable.

3.4 Radio Resource Exhaustion Attack

GPRS network characterizes two different types of radio resource exhaustion attacks targeting data connection setup and tear-down mechanisms. In the setup attack authors continue exploring control channel depletion effects. They analyse the Random Access Channel (RACH). RACH is shared by all mobile terminals attempting to establish connections with the network. To minimize contention, its access is mediated through slotted-ALOHA protocol. During the attack, neighbouring phones are forced to continuously begin short-lived data connection, thus accessing RACH and flooding it. The authors find out that, for the city of Manhattan, 3Mbps of malicious traffic cause a data and voice connection blocking probability of 65%. Along with that, they point out how attacking data realm could have effect on voice realm too because of the single shared control channel. This fact is extremely interesting and it is important to notice that even outside the data connection. There are multiple ways to force a mobile phone to access the RACH. This achieves similar results. The data setup exploited is just an instance of this effect although it is possibly the one that is most easily kept concealed to the phone owners. Differently from the setup attack, the attack targeting the tear-down mechanism is entirely contained in the data portion of the mobile network. It cannot affect the voice network and can only cause a DoS in the data network. When a new data own with the user equipment is established, the base station assigns to it a 5-bit Temporary Flow Identifier (TFI) used to mark all packets belonging to the same flow. Once the last packet has been delivered, the base station can release the TFI. This event takes place after a 5 seconds delay in order to take into account minor variations in data interarrival times. Exploiting this delay a malicious attacker can exhaust all TFIs. A possible example implementation of this attack requires a rogue Internet server answering 32 requests coming from the same neighbourhood with 1-byte-packets sent every 5 seconds. As in the case of the SDDCH attack.

4. Proposed Method

Attacking the UMTS Network with help of Simless Devices

4.1 Performing DoS-attacks

A wide array of programs are used to launch DoS-attacks. Most of these programs are completely focused on performing DoS-attacks, while others are also true Packet injectors, able to perform other tasks as well. Such tools are intended for benign use, but they can also be utilized in launching attacks on victim networks.

Handling
Defensive responses to denial-of-service attacks typically involves the use of a combination of attack detection, traffic classification and response tools, aiming to block traffic that they identify as illegitimate and allow traffic that they identify as legitimate. A list of prevention and response tools is provided below:

Firewalls
Firewalls can be set up to have simple rules such to allow or deny protocols, ports or IP addresses. In the case of a simple attack coming from a small number of unusual IP addresses for instance, one could put up a simple rule to drop (deny) all incoming traffic from those attackers. More complex attacks will however be hard to block with simple rules: for example, if there is an ongoing attack on port 80 (web service), it is not possible to drop all incoming traffic on this port because doing so will prevent the server from serving legitimate traffic.[35] Additionally, firewalls may be too deep in the network hierarchy. Routers may be affected before the traffic gets to the firewall. Nonetheless, firewalls can effectively prevent users from launching simple flooding type attacks from machines behind the firewall.

Switches
Most switches have some rate-limiting and ACL capability. Some switches provide automatic and/or system-wide rate limiting, traffic shaping, delayed binding (TCP splicing), deep packet inspection and Bogon filtering (bogus IP filtering) to detect and remediate denial-of-service attacks through automatic rate filtering and WAN Link failover and balancing.

Routers
Similar to switches, routers have some rate-limiting and ACL capability. They, too, are manually set. Most routers can be easily overwhelmed under a DoS attack. Cisco IOS has features that prevent flooding, i.e. example settings.

4.2 Estimation of Effect

The work 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.

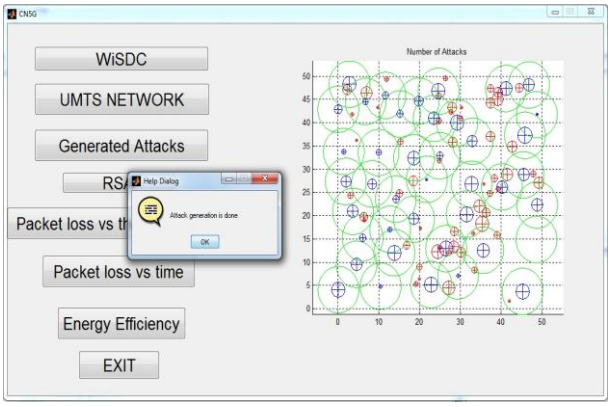

Figure 4: Attack Generation

5. Accessing the UMTS Radio Network

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.

Focusing on the message exchanges between MS and Node during the attack. The RACH is the uplink used to carry mobile device's access requests. The FACH is used to answer incoming random access requests; it carries the information needed by the mobile phone to access the dedicated channel (DCH) used for further communications. The FACH is used to answer incoming random access requests; it carries the information needed by the mobile phone to access the dedicated channel (DCH) used for further communications.

5.1 RSA Algorithm

This idea omits the need for a "courier" to deliver keys to recipient's over another secure channel before transmitting the originally-intended message. In RSA, encryption keys are public, while the decryption keys are not, so only the people with the correct decryption key can decipher an encrypted message. Everyone has their own encryption and decryption keys. The keys must be made in such a way that the decryption key may not be easily deduced from the public encryption key. The receiver may need to verify that a transmitted message actually originated from the sender (signature), and didn't just come from there (authentication). This is done using the sender's decryption key, and the signature can later be verified by anyone, using the corresponding public encryption key. Signatures therefore cannot be forged. Also, no signer can later deny having signed the message. This is not only useful for electronic mail, but for other electronic transactions and transmissions, such as fund transfers. The security of the RSA algorithm has so far been validated.

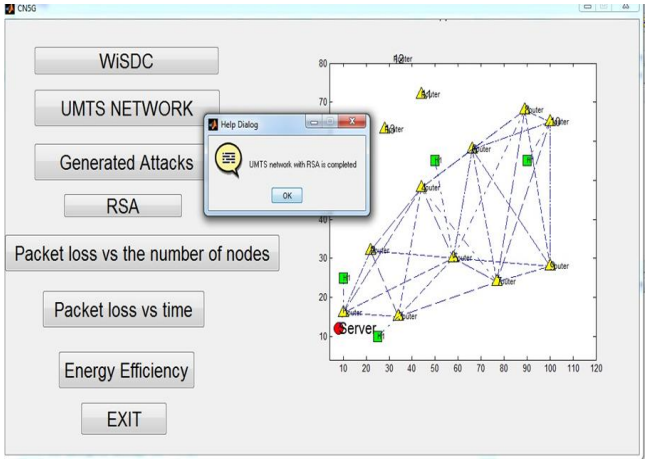

Figure 5: Showing UMTS network with RSA

5.2 Different Methods in RSA

5.2.1 BMRSA (Batch Multi-Prime RSA)

Multi-prime RSA is an isolated version of RSA cryptosystem. In Multi-prime the modulus consists of more than two prime numbers and the decryption will be speed-up by using Chinese remainder theorem.

5.2.2 EAMRSA (Encrypt Assistant Multi-Prime RSA):

Improves RSA decryption performance based on the Multi-Prime RSA and RSA-S2 system. The experimental results show that the speed of the two variants decryption has been substantially improved.

6. Results

6.1 Analysis of Packet loss vs. number of nodes

Packet loss affects the perceived quality of the application. Several causes of packet loss or corruption would be bit errors in an erroneous wireless network or insufficient buffers due to network congestion when the channel becomes overloaded. Some of the packets are lost due to network congestion or due to noise. Simulation results show Packet loss ratio is minimum in the proposed method, so as to keep the successful delivery of high QoS. According to ITU (International Telecommunication Union) standards, the value of packet loss is minimal due to implementation of RSA Algorithm to UMTS network.

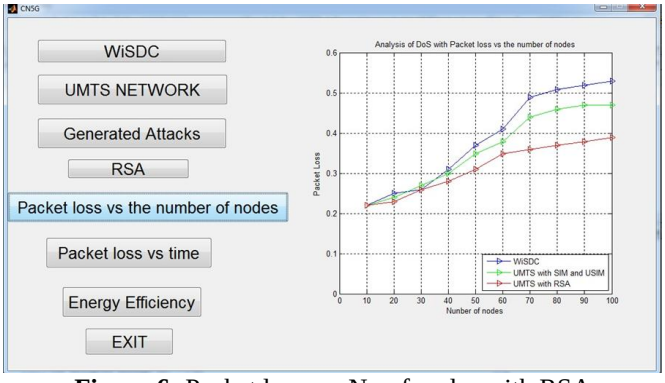

Figure 6: Packet loss vs. No of nodes with RSA

6.2 Analysis of Packet loss *vs*. time

A novel Markov model is constructed to calculate the packet loss probability and the delay distribution of real-time wireless packets. These packets are transmitted through an erroneous channel modeled by a two-state Markov chain. If a packet transmission is not successful, the packet is retransmitted until a delay limit is exceeded. At that time, the packet is discarded and the transmission of the next packet begins. This packet-dropping process has a significant impact on packet loss probability but is seldom considered in other Markov models.

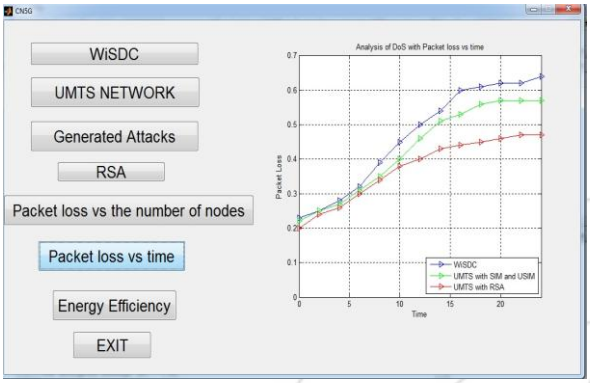

Figure 7: Packet Loss vs Time With RSA

6.3 Energy efficiency

Simulation is carried out using Mat lab tool. Set up a simulation environment consist of more than sensor nodes which scattered randomly over a100mX100m square area. The base station is at (81, 90). It is assumed that all the nodes begin with the same initial energy of 0.5 joules. We have compared the performance of the protocols on the basis of two parameters – energy efficiency and fault tolerance. The first parameter gives average energy dissipation per node and second parameter indicates the overall lifetime of the network.

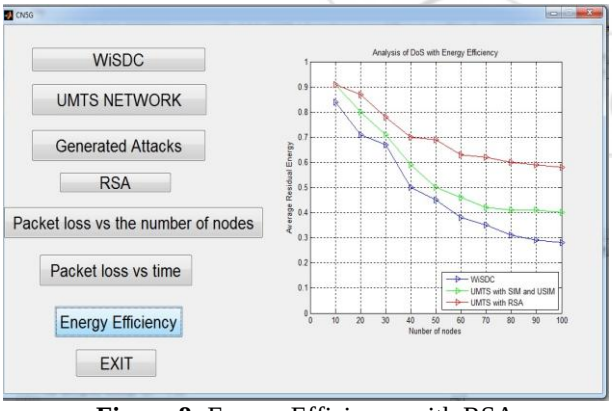

Figure 8: Energy Efficiency with RSA

7. Advantages

The proposed attack to UMTS network has the following advantages

- Reduces the number of needed resources.
- Increase in efficiency.
- Decrease in packet Loss.

8. Application

- Cyber warfare device manufacturing process.
- Artificial intelligence sector.
- Military scenarios to defeat UMTS network temporarily in specific area.
- Useful in dimensioning through 'Tortureest'.

9. Conclusion and Future Scope

Several ways to mount DoS attacks against mobile network infrastructures are known. However, in order to make the attack successful, the state-of-the-art attack methodologies [6] are based on GSM network alone and require the availability of botnets with more than 10.000 smartphones 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 consumer market. Accordingly, in order to cope with the above timing limits, we envisioned an ad-hoc attacking device, equipped with multiple UMTS radio interfaces and no SIM modules. This device allowed us to design a novel attack methodology exploiting the network access procedures and to greatly reduce the number of needed resources. Thus, we massively enhanced the threat level of the described attack.

The feasibility of the attack without a botnet is very important for a two-fold reason: first, the usage of a dedicated device allows gathering the resources needed to mount the attack without interfering with users and running the risk of being discovered before the actual attack; second, avoiding the usage of devices in possession of unaware users allows optimal displacement of attacking equipment and reduces the risk of attack failures due to an incorrect placement of the botnet nodes. In fact, it is possible that an unusual clustering of nodes in a botnet could produce a concentration of devices that saturates the cell signaling bandwidth and prevents some of the nodes to fulfill their full attacking potential.

On the contrary, the device we envision is not owned by a user, and hence conditioned by his movements, so that it can be precisely placed by the attacker and even remotely triggered to start the attack. All of these factors represent a significant increase in the dangerousness of the attack when compared to the existing ones and can make the described device an interesting target also for the cyber-warfare or cellular network production industry.

The future work of this study will be implementation of the system and checking its efficiency in practical use and make it use practically in the real time systems for avoiding DoS attacks. In future, further optimization of this technique can also be done.

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 Connection 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-partneringcriticalinfrastructure-security-and-resilience

[8] (2008). European Commission, European Programme for Critical Infrastructure Protection (EPCIP). [Online]. Available: http://ec.europa.eu/dgs/home-affairs/what-we do/policies/crisis-andterrorism/critical-infrastructure/index_en.htm

[9] V. Viduto, C. Maple, and W. Huang, "Managing threats by the use of visualisation techniques," Int. J. Space-Based Situated Comput., vol. 1, no. 2/3, pp. 204–212, 2011.

[10] A. Armando, A. Merlo, M. Migliardi, and L. Verderame, "Breaking and fixing the android launching flow," Comput. Security, vol. 39, pp. 104–115, 2013.

[11] A. Mylonas, S. Dritsas, B. Tsoumas, and D. Gritzalis, "Smartphone security evaluation—the malware attack case," in Proc. Int. Conf. Security Cryptography, 2011, pp. 25–36.

[12] K. Derr, "Nightmares with mobile devices are just around the corner!" in Proc. IEEE Int. Conf. Portable Inform. Dev., 2007, pp. 1–5.

[13] C. Guo, H. J. Wang, and W. Zhu, "Smart-phone attacks and defenses," in Proc. 3rd Workshop Hot Topics Netw., 2004, pp. 1–6.

[14] P. Traynor, P. McDaniel, and T. La Porta, "On Attack Casuality in Internet-Connected Cellular Networks," in Proc. 16th USENIX Security Symp., 2007, pp. 1–16**.**

[15] A. Castiglione, R. De Prisco, and A. De Santis. (2009). Do you trust your phone? Proc. 10th Int. Conf. E-Commerce Web Technol., vol. 5692, pp. 50–61 [Online]. Available: http://dx.doi.org/10.1007/978-3-642-03964-5_6

[16] C. Fleizach, M. Liljenstam, P. Johansson, G. M. Voelker, and A. Mehes. (2007). Can you infect me now?: Malware propagation in mobile phone networks. Proc. ACM Workshop Recurring Malcode, pp. 61–68. [Online]. Available: http://doi.acm.org/10.1145/1314389.1314402

[17] C. Mulliner and J.-P. Seifert, "Rise of the iBots: Owning a telco network," in Proc. 5th Int. conf. Malicious Unwanted Softw., 2010, pp. 71–80.

[18] A. P. Felt, M. Finifter, E. Chin, S. Hanna, and D. Wagner. (2011). A survey of mobile malware in the wild. Proc. 1st ACM Workshop Security Privacy in Smartphones Mobile Dev., pp. 3–14. [Online]. Available: http://doi.acm.org/10.1145/2046614.2046618

[19] P. Traynor, W. Enck, P. McDaniel, and T. La Porta, "Mitigating attacks on open functionality in SMS-capable cellular networks," in Proc. 12th Annu. Int. Conf. Mobile Comput. Netw., 2006, pp. 182–193.

[20] M. Khan, A. Ahmed, and A. R. Cheema, "Vulnerabilities of UMTS access domain security architecture," in Proc. IEEE 9th Int. Conf. Softw. Eng., Artif. Intell., Netw. Parallel/Distrib. Comput., 2008, pp. 350–355.

[21] G. Kambourakis, C. Kolias, S. Gritzalis, and J. Hyuk-Park, "Signaling-oriented DoS attacks in UMTS networks," in Proc. 3rd Int. Conf. Workshops Adv. Inform. Security Assurance, 2009, pp. 280–289.

[22] N. Gobbo, A. Merlo, and M. Migliardi. (2013). A denial of service attack to GSM networks via attach procedure, Proc. ARES Workshop, vol. 8128, pp. 361–376,[Online]. Available: http://dx.doi. org/10.1007/978-3-642-40588-4_25

[23] 3GPP, (2012). TS 25.214—Physical layer procedures (FDD). [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/25214.htm

[24] 3GPP, (2012). TS 24.008—Mobile radio interface Layer 3 specification; Core network protocols; Stage 3. [Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/24008.htm

[25] 3GPP, (2012). TS 25.322—Radio Link Control (RLC) protocol specification. [Online]. Available: http://www.3gpp.org/ftp/Specs/htmlinfo/25322.htm

[26] C. Johnson, H. Holma, and I. Sharp, "Connection setup delay for packet switched services," in Proc. 6th IEEE Int. Conf. 3G Beyond,2005, pp. 1–5.

[27] H. Holma and A. Toskala, WCDMA for UMTS. Hoboken, NJ, USA: Wiley, 2002.

Author Profile

Pramod Kumar Jonnalgadda Completed B.tech Degree in 2012 in Electronics and Communication Engineering. Having 1 year of experience in Computer Networking and Wireless Communications. Presently Pursuing M.Tech from **Lords Institute of Engineering & Technology.Hyderabad** in Wireless and Mobile Communications.

Abdul Wasay Mudasser Completed B.tech in 2007 & M.tech in 2010 from JNTUH. Having 5years of Teaching and 2years of Industrial Experience. Field of interest is wireless communication, Telecommunication, Computer Networking and Image Processing. Presently working as Associate Professor in Department of Electronics & Communication Engineering at **Lords Institute of Engineering & Technology. Hyderabad.**