Asian Journal of Information Technology 15 (12): 1916-1923, 2016
ISSN: 1682-3915

Enhanced Security Framework with DDOS Attack Defense in UMTS

[1]V. Vijaya Kumar and [2]R. Samson Ravindran
[1]AVS Engineering College, Salem, 636003 Tamil Nadu, India
[2]Mahendra Engineering College, Mallasamudram, Tamil Nadu, India

Abstract: The UMTS system and architecture are designed to accommodate Internet-like mobile services and specific services like mobile commerce to mobile users. They bring attacks from Internet and mobile users as well. Denial-of-Service (DoS) attacks aim to frustrate a legitimate user's access to mobile services or bring down servers by depleting system resources. Many approaches are proposed to thwart these attacks. This study focuses on man in the middle attack, authentication based condition and integrity protocol with a quassi puzzle to ensure the security. To resolve the re-direction attack SGSN is used. Here it uses Payload Encryption Key (PLK) to handle the man-in-the-middle attack. Next for bandwidth reduction a ticket-based authentication scheme is used. In addition to these, for ensuring the integrity EMSUCU protocol is used. A quasi puzzle is given at the last for the defensive mechanism client puzzles based on quasi partial collisions is used. Here the DDoS attack is detected in a three way detection phase. Signaling and travesing through a number of network nodes enhances the detection in earlier manner and clear idea of attack detection. Quasi puzzle is quite easy and secure algorithm for avoiding the DDoS attack as soon as it is detect.

Key words: GTP in GTP based detection, CUSUM methodology, puzzles, SSGN, DDoS

INTRODUCTION

UMTS: The Universal Mobile Telecommunications System (UMTS) is one of the new 'third generation' (3G) mobile cellular communication systems being developed within the framework defined by the ITU and known as IMT-2000. UMTS builds on the capability of today's mobile technologies by providing increased capacity, data capability and a greater range of services using a new radio interface standard called UMTS Terrestrial Radio Access (UTRA). The basic radio, network and service parameters of the UMTS system were defined by the European Telecommunications Standards Institute (ETSI) in early 1998.

ETSI developed the extremely successful second generation GSM (Global System for Mobile communications) standard, which is used by over 650 million customers world-wide and accounts for approximately 70% of the wireless communications market. An important characteristic of UMTS is that the new radio access network will be connected to an evolution of the GSM core network (Boman *et al*., 2002; Putz *et al*., 2001).

Security in UMTS: The goal of UMTS security is to provide entity authentication, data confidentiality, user confidentiality and data integrity.

Authentication is a process of verifying the identity of an entity and makes sure that the communication is authentic between parties. Authentication is needed for insuring all parties of the communication are the ones they are claiming to be. One important tool to achieve this goal is the digital signature.

Confidentiality can be defined as the prevention of unauthorized disclosure of information and it is about not letting unauthorized users read or learn, sensitive information. In using encryption, a process of taking readable and meaningful data and scrambling or transforming it so that someone who happens to intercept the data can no longer understands it.

Integrity means keeping the data in unaltered form, Integrity ensures that information is not changed or altered in transit and includes the detection modification, insertion, deletion or replay of transmitted data User confidentiality is that the permanent user identity (IMSI) cannot be eavesdropped. This service is implemented by using a temporary user identity (TMSI) which is known by the visited serving network.

Confidentiality is used to keep information secured from eavesdropper and hacker. This is achieved by ciphering of the user and signaling data between the subscriber and the network and by referring to the subscriber by temporary identities TMSI instead of using IMSI. Mobile networks must provide subscriber identity confidentiality, subscriber location

Corresponding Author: V. Vijaya Kumar, AVS Engineering College, Salem, 636003 Tamil Nadu, India

confidentiality, user data (i.e., voice and data) and signaling data confidentiality (Gardezi , 2006; Anita, 2014).

Security attacks in UMTS: There are several security issues that have to be taken into consideration when deploying a cellular infrastructure. The importance of which has increased with the advent of advanced networks like 3G. Due to the massive architecture of a cellular network, there are a variety of attacks that the infrastructure is open to:

- Denial of Service (DoS): this is probably the most potent attack that can bring down the entire network infrastructure.
- Distributed Denial of Service (DDoS): a number of hosts can be used to launch an attack
- Eavesdropping: if the traffic on the wireless link is not encrypted then an attacker can eavesdrop and intercept sensitive communication such as confidential calls, sensitive documents etc
- Message forgery: if the communication channel is not secure, then an attacker can intercept messages in both directions and change the content without the users ever knowing
- Man in the middle attack: an attacker can sit in between a cell phone and an access station, intercept messages in between them and change them
- Session hijacking: a malicious user can highjack an already established session and can act as a legitimate base station (Gardezi, 2006; Kambourakis *et al*., 2011)

This study focuses on man in the middle attack, authentication based condition and integrity protocol with a quassi puzzle to ensure the security. To resolve the re-direction attack SGSN is used. Here, it uses Payload Encryption Key (PLK) to handle the man-in-the-middle attack. Next for bandwidth reduction a ticket-based authentication scheme is used. In addition to these, for ensuring the integrity EMSUCU protocol is used. A quasi puzzle is given at the last for the defensive mechanism client puzzles based on quasi partial collisions is used.

For a flow contained development, this study first gives an introduction related to security in UMA network in the section one. The second section is a literature study of some previous related works. A well-structured and modularized proposal is given in section three followed by a simulation result in section four. At last an overall conclusion is given.

Literature review: Shidhani and Leung (2008) have proposed a couple of re-authentication protocols that reduce re-authentication delays during UMTS-WLAN VHs compared to existing protocols by substantially reducing message signaling. Additionally, they achieve secured key management and mutual authentication between the UE and authentication servers in the 3G home networks. However, further verification is required for authentication.

Oh *et al*. (2012) have proposed detection methods of 3G mobile network DoS attack. This study explains the 3G mobile network resource exhaustion type of DoS attack and the signaling DoS attack which exploits the GTP-in-GTP packet processing vulnerability in the domestic 3G mobile network.

Lei *et al*. (2006) have proposed a method based on partial collisions in hash functions. Their approach provides fine-grained control over difficulties by introducing a quasi partial collision concept. The proposed method provides the fine granularity and efficiency. This is particularly useful for access control. However there occurs energy consumption.

Lee *et al*. (2007) have proposed a statistical CUSUM-based detection mechanism to defend against the signaling attack. Using real world traces, they have shown that our detection mechanism can identify the source of a signaling attack in a timely manner before the damage becomes aggravated while producing very few false positives. In addition, their detection mechanism is robust as it depends solely on the additional signaling load and any assumed attack strategy. However the detection time is slow.

Southern *et al*. (2011) have proposed two different changes to the protocols in mobile networks to protect against the legacy integration of GSM. The former changes to the GSM protocol to protect the encryption session key from attackers and therefore to protect the UMTS communication that depends on this session key. The later solution proposes a modification in the UMTS protocol to be modified to make the UMTS encryption and integrity keys don't depend directly on the GSM key, and therefore become far from the GSM security flaws. The proposed solution will help to resolve the insecurity brought about by the legacy integration of the GSM equipment and protocols into the new UMTS system.

Problem identification and solution

Problem description: In our previous study, to eliminate the vulnerabilities and to improve the security and efficiency of CDMA-networks Secure Authentication Key Agreement Protocol (S-AKA) is used.

Considering un-focused area of our previous study this study focuses on man in the middle attack, authentication based condition and integrity protocol

with a quassi puzzle to ensure the security. To resolve the re-direction attack SGSN is used. Here, it uses Payload Encryption Key (PLK) to handle the man-in-the-middle attack. Next for bandwidth reduction a ticket-based authentication scheme is used. In addition to these, for ensuring the integrity EMSUCU protocol is used. A quasi puzzle is given at the last for the defensive mechanism client puzzles based on quasi partial collisions is used.

To give a proper flow of the solution this section starts with a proposed architecture diagram. There are four phases of the solution. Each phase of solutions carries its modular diagram with its algorithm. At last an overall algorithm is given to give the overall procedure. Mainly the proposed solution is detected in to two parts. First part is detections of the attacks and second part is security on these attacks.

MATERIALS AND METHODS

From the architectural diagram given in Fig. 1 it is clear that the procedure starts with attack detections. First signaling attack is detected through CUSUM Model. Then GTP in GTP based detection is done for DDoS attacks. SGSN detection is carried out for signaling error detection. To prohibit the attack this study is giving puzzle based detection.

In the extension work after the encryption process a secure defense mechanism for attacks in CDMA-networks is provided.

CUSUM Method for detection of signaling attack: The detection of signaling attack is detected from a test based scenario. First data's are collected and decision is taken on the parameters got from the test. The modular diagram is shown in Fig. 2.

Here for the detection of signaling attack this study can use online detection algorithm based on CUSUM method. In this a remote host is taken to be a node. The detection algorithm is applied to the remote hosts that are not marked as malicious attackers. If the remote host triggers a significant number of virtual setups over a short period of time, then there is strong evidence that the remote host attempts to raise a signaling attack and the detection algorithm is applied.

CUSUM test: This study first overview the CUSUM test and the aim of well-suited procedure for intrusion detection. In this study, we consider its version having no parameters which does not assume any a priori distribution of the data samples being considered. As long as the data samples are not extremely dependent, this

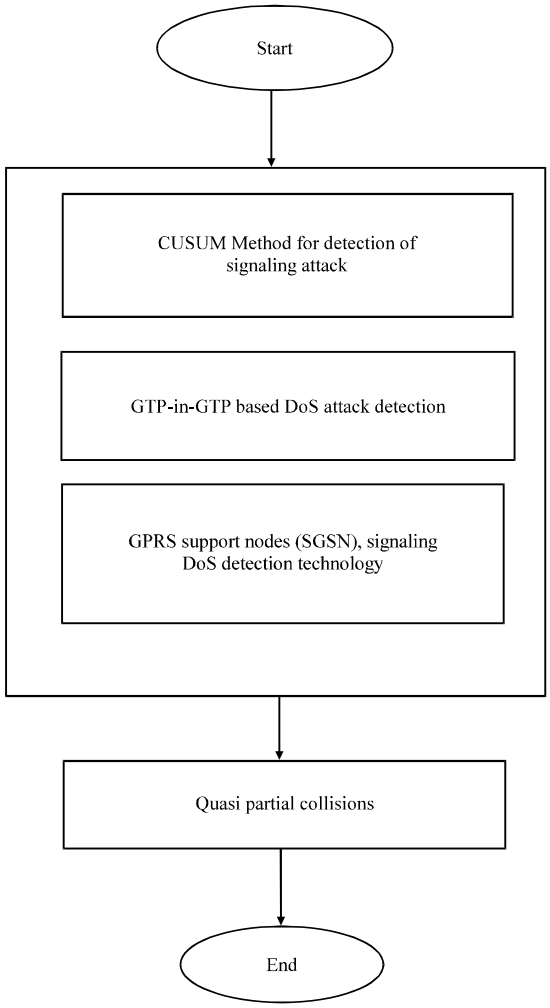

Fig. 1: Architecture diagram

study is guaranteed the solution in a better manner. This is the technique through which detection time is minimized among all possible detection schemes subject to a fixed worst-case expected false alarm rate. In the context of the signaling attack detection is done. For every remote host, the CUSUM test monitors a set of n inter-setup time samples {t1, t2, ..., tn}. Each inter-setup time sample is assigned a score z(tn). When a sample is available, this study updates the CUSUM statistic as follows:

$$qn = \max(qn-1+z(tn), 0) \quad (1)$$

Take action if $qn \geq h$ where $h>0$ is the pre-specified CUSUM threshold.

Decision on CUSUM test: Note that if an inter-setup time sample t follows a malicious behavior, then the expected score E(z(t)) should be positive so that qn will eventually

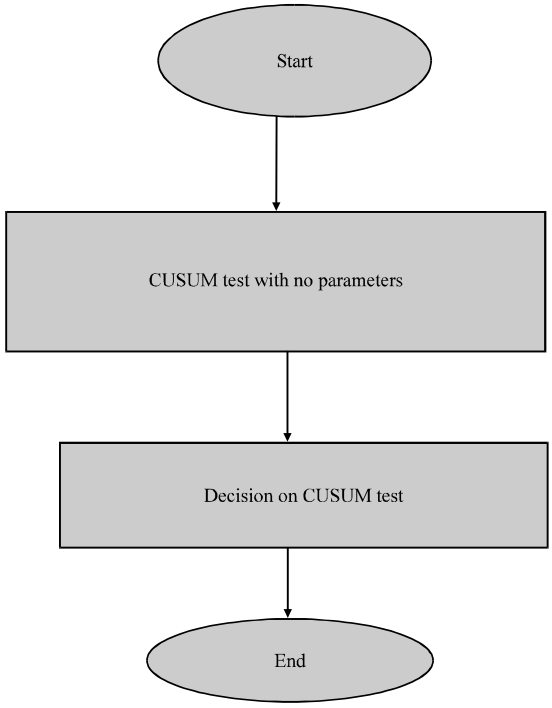

Fig. 2: Modular of CUSUM Method phase

rise above threshold h. On the other hand, EE(z(t)) should be negative when the data samples follow a benign behavior. The CUSUM test is adequate for identifying any abrupt change of a benign behavior to a malicious behavior. To understand this, note that if a host is benign, z(tn) is negative (in the expected sense) and the corresponding qn will stay around the zero value, regardless of how long the benign behavior has been observed. However, when the benign behavior turns to a malicious one, qn increases and eventually surpasses the threshold. Therefore, the CUSUM test prevents an attacker from suppressing qn with a long history of benign behavior. This ensures that the CUSUM test detects a malicious behavior in a timely manner.

Algorithm for CUSUM Method phase:

- Step 1: start the procedure
- Step 2: go for CUSUM test with no parameters
- Step 3: then error are detected through decision on CUSUM test
- Step 4: end the procedure

GTP-in-GTP based doS attack detection: GTP-in-GTP based DoS attack detection can be used when the IP address resource is allocated abnormally as it results in GTP-in-GTP packet processing vulnerability. This blocks user traffic that uses similar traffic. The suspected GTP-C packet is detected and blocked, by measuring length according to the type of GTP-C message.

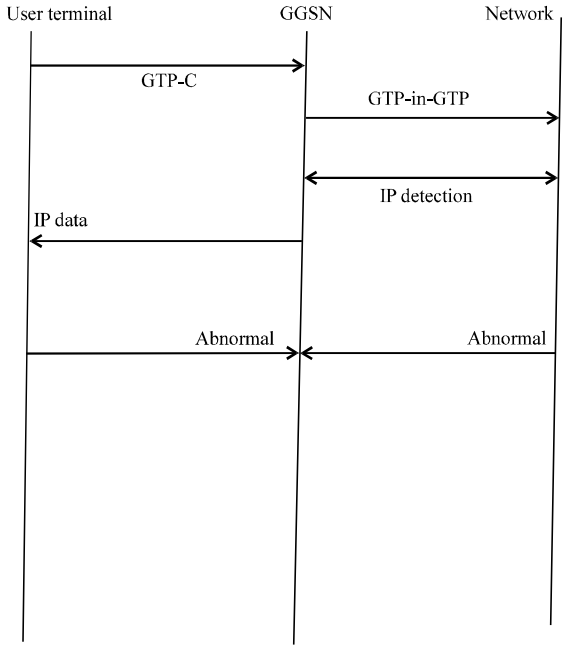

Fig. 3: Modular of GGS based detection

GGSN is provided at mobile network has GTP-in-GTP vulnerability (Fig. 3). If the user terminal sends a malicious GTP-C message, a GTP-in-GTP type packet is sent to the inside of the mobile network via the GGSN. The GGSN in the network sends the user data received from the SGSN to the Internet network, based on the destination IP address. If the user sets the GTP-C message as the GGSN's IP address, it will be sent to the GGSN. If the GTP-C message for mobile network control such as IP address allocation for the mobile network, sends the GGSN's IP address to the destination via the terminal, the IP address resource can be allocated abnormally. This type of GTP-in-GTP packet processing vulnerability can be exploited in most GGSNs installed in the domestic commercial service environment and the P-GATEWAT equipment in the network that performs a similar function to the network's GGSN as well. If the terminal creates many "GTP-C create PDP context" messages and sends them to the GGSN's IP address, the TEID and IP address of the GGSN are allocated abnormally. Likewise, a DoS attack can be launched against normal users that use the mobile internet service, if the TEID and IP address of the GGSN are exhausted by exploiting the GGSN's GTP-in-GTP packet processing vulnerability.

Algorithm for GTP in GTP based technology:

- Step 1: start the procedure with user, network and GGSN
- Step 2: end user sends GTP-C message
- Step 3: detect the IP address

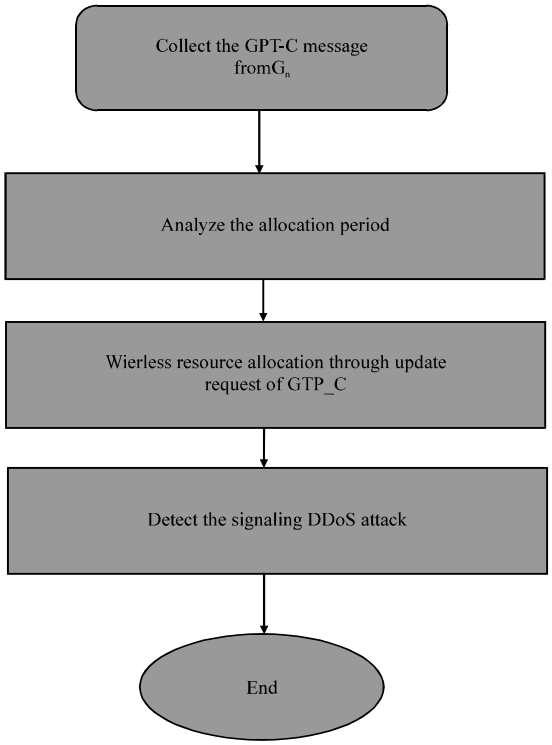

Fig. 4: The modular of SSGN module

- Step 4: check the IP address
- Step 5: detect the DDoS attack

GPRS Support Node (SGSN), signaling DoS detection technology: Besides when a DoS attack occurs by causing overload on the Radio Network Controller (RNC) and Serving GPRS Support Node (SGSN), Signaling DoS detection technology can be used (Fig. 4). Here using the tunnel ID information of the terminal the signaling DoS attack is detected and it can be prevented by deleting the terminal data call.

The signaling DoS attack is detected by analyzing the GTP-C/U collected from the Gn sector. For malicious/abnormal wireless resource allocation, either no transmission traffic at all or only small-volume traffic is generated during the active to dormant switching period. The time difference between wireless resource allocation/release and allocation/release is small to generate a large amount of signal messages in a short period of time.

Wireless resource allocation: Wireless resource release is detected by analyzing the GTP-C Update Request message that is created while the terminal is switching from the active mode to the dormant mode and back to the active mode. Malicious wireless resource allocation is detected by analyzing transmission traffic during the wireless resource allocation release period. By analyzing the time difference between abnormal wireless resource release detected in this way and release, the signaling DoS caused by malicious/abnormal wireless resource allocation is detected. The mobile terminal that causes the signaling DoS maliciously and abnormally can be handled by deleting the pre-determined data call. Unlike GTP-in-GTP, the signaling DoS is created abnormally by firmware during the terminal manufacturing process. When the signaling DoS have been detected, it is blocked on the mobile network. Therefore, the signaling DoS can be prevented by deleting the terminal data call, if the "GTP-C delete PDP context" message is created and sent to the GGSN, using the tunnel ID information of the terminal that detects the signaling DoS attack.

Algorithm for GPRS Support Node (SGSN), signaling DoS detection based technology:

- Step 1: start the procedure with collecting the GPT-C messages from G_n
- Step 2: Analyze the allocation period of the resources
- Step 3: analyze Wireless resource allocation through update request of GTP-C
- Step 4: Detect the signaling DDoS attack
- Step 5: end the procedure

Quasi partial collisions: As a defensive mechanism client puzzles based on quasi partial collisions is used. Here if the server is under attack a client based puzzle in the form of quasi value can be used before establishing a connection. This puzzle defends attacks.

This study reconsiders the idea of partial collision puzzles (Fig. 5). Given a n-bit puzzle, the client has to find a solution whose hash value cares only the first n-bit values and does not care the (n+1)-bit (x1) value and other bits values. In the (n+1)-bit puzzle, the x1 should be considered and its value must also be zero while it can be 0 or 1 as in the n-bit puzzle. Thus, more work should be done to find a new solution whose hash value has the most significant (n+1) zero bits:

$$\begin{array}{c} \text{Other bits} \quad (n\text{-}1)\text{o's} \\ \leftrightarrow \qquad\quad \leftrightarrow \\ h(C, Ns, Nc, X) = 00\ldots000\,x_1\ldots x_n \\ \leftrightarrow \\ \text{4 quasi bits} \end{array} \tag{2}$$

Thus, the need of one extra bit zero is a strong condition. This study ought to make a weak condition in order to compensate the whole requirement. Since this is

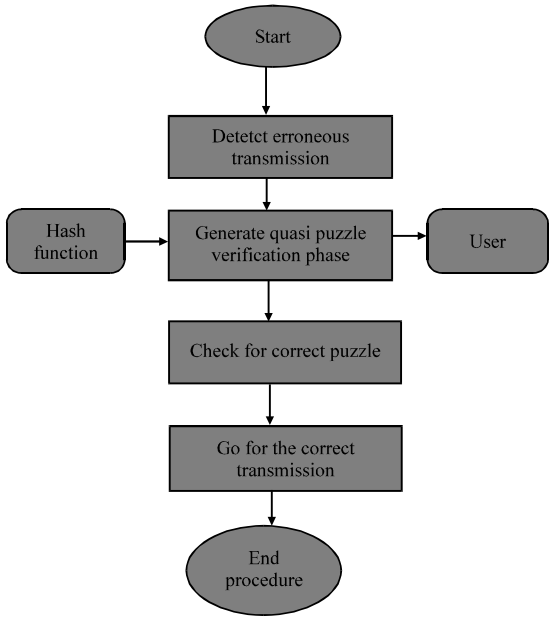

Fig. 5: Modular of quasi puzzle phase

Fig. 6: Puzzles based on quasi partial collisions

only one bit, this study cannot make use of it too much. This study might ask its neighbor bits for help. While applying this protocol to UMTS environment, the server can be service providers or operators who are the potential DoS targets.

This is similar to Aura's approach except that the server also decides a quasi value Q. The quasi value is used to control the quasi partial collisions (Fig. 6). This study will explain value later. These three values together form the puzzle that is sent to the client. To solve the puzzle, the client also generates a random nonce Nc. Now, this study modify a little the equation, for example, by considering the last 4 bits Q1-4 in the first k-bits as the following:

$$\begin{matrix} \text{Other bits} & \text{(n-1)o's} \\ \leftrightarrow & \leftrightarrow \\ h(C, Ns, Nc, X) = 00...000 Q_1 Q_2 Q_3 Q_4 x_1 ... x_n \\ \leftrightarrow \\ \text{4 quasi bits} \end{matrix} \quad (3)$$

Fig. 7: n Bits quasi collision

This equation is similar to Aura's equation. In this case, however, this study has an extra requirement. If this study isolates the 4 bits Q1Q2Q3Q4 its decimal value must be less than Q:

$$Q1Q2Q3Q4 < Q \quad (4)$$

Here, this study also uses n to control the difficulty level. Since there is a big gap between (n-1)-bit partial collision puzzle and n-bit partial collision puzzle, this study allow the last four bits, Q1Q2Q3Q4, of the first n bits to take several acceptable values instead of only 0000 in a normal k-bit partial collision puzzle. And this study still treats the whole k bits as collision. Thus, this study calls this quasi partial collision. This study requires a weak k-bit partial collision. Collision quasi collision (Fig. 7).

Hash function: Before continuing our discussion, this study needs an assumption on hash function.

Assumption 1: For a good hash function, this study assumes that the hash values of a set of random input messages distribute randomly. There are 16 combinations for these four bits from 0000-1111. This study defines a set A with Q elements chosen from these 16 combinations. Based on this assumption, the probability of a hash value whose Q1Q2Q3Q4 is in the set A is dependent only on Q and independent on the elements in A. Hence, for efficiency and simplicity, this study choose the smallest Q strings and require that Q1Q2Q3Q4<Q. The value of Q is called quasi value. The quasi value Q from the server controls the number of choices. This study can change the decimal value of the four quasi bits between 0 and 15. If Q = 1, then this equation becomes a normal k-bit partial collision puzzles. If Q = 16, then it is a (n-4)-bit partial collision puzzle. Any other values will generate a puzzle between k-bit and (n-4)-bit puzzles. In this way, this study adds several difficulty levels into the big gap. The selection of Q is practical, so this study need experiences to determine proper values. In short, quasi partial collision puzzles ask the client to give solutions whose hash values are not strictly collided but in an allowable value range. Thus, this study decreases the difficulty.

Algorithm for quasi partial collisions technology:

- Step 1: start the procedure
- Step 2: check for DDoS detection
- Step 3: if not detected go for the normal transmission
- Step 4: if detected go for the puzzle verification
- Step 5: end the procedure

Overall algorithm:

- Step 1: start the procedure
- Step 2: CUSUM Method for detection of signaling attack is done as given in section 3.2.1
- Step 3: GTP in GTP is used to detect DDoS attack
- Step 4: GPRS Support Node (SGSN), signaling DoS detection technology is carried out
- Step 5: As a defensive mechanism client puzzles based on quasi partial collisions can be used
- Step 5: end the procedure

RESULTS AND DISCUSION

Simulation model and parameters: The Network Simulator (NS2) is used to simulate the proposed architecture. In the simulation 50 mobile nodes move in a 500×500 region for 50 sec of simulation time. All nodes have the same transmission range of 40 m. The simulated traffic is Constant Bit Rate (CBR). The simulation settings and parameters are summarized in Table 1.

Performance metrics: The proposed Enhanced Security Framework with DDoS Attack Defense (ESFDAD) is compared with the S-AKA technique [ ]. The performance is evaluated mainly, according to the following metrics.

- Packet delivery ratio: it is the ratio between the number of packets received and the number of packets sent.
- Packet drop: it refers the average number of packets dropped during the transmission
- Delay: it is the amount of time taken by the nodes to transmit the data packets

Table 1: Simulation settings

Parameters	Values
No. of nodes	25
Area size	500×500
Mac	IEEE 802.11
Transmission range	40 m
Simulation time	50 sec
Traffic source	CBR
Packet size	512
Requests	25, 30, 35, 40, 45 and 50
Attackers	2
Rate	50 kb

Based on requests: In our experiment we vary the number of requests as 25, 30, 35, 40, 45 and 50. Figure 8 shows the delay of ESFDAD and SAKA techniques for different number of requests scenario. We can conclude that the delay of our proposed ESFDAD approach has 79% of less than SAKA approach.

Figure 9 shows the delivery ratio of ESFDAD and SAKA techniques for different number of requests scenario. We can conclude that the delay of our proposed ESFDAD approach has 41% of higher than SAKA approach.

Figure 10 shows the drop of ESFDAD and SAKA techniques for different number of requests scenario. We can conclude that the drop of our proposed ESFDAD approach has 97% of less than SAKA approach.

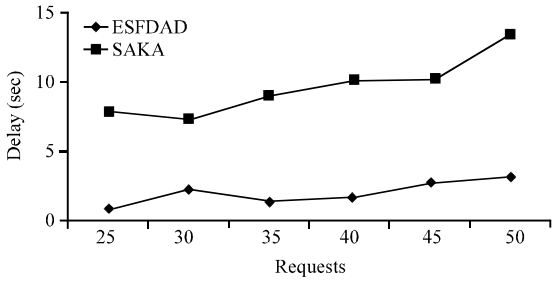

Fig. 8: Requests vs. delay

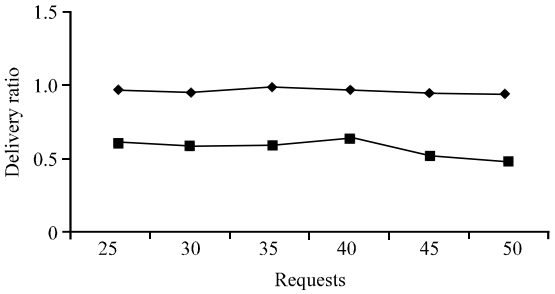

Fig. 9: Requests vs. delivery ratio

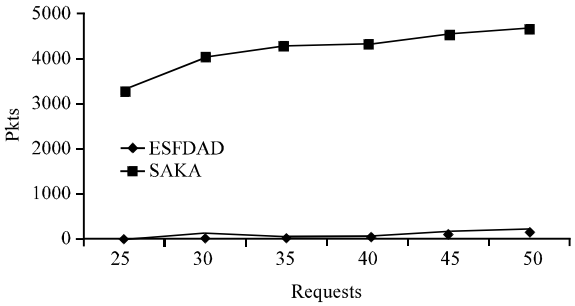

Fig. 10: Requests vs. drop

CONCLUSION

Considering un-focused area of our previous study this study focuses on man in the middle attack, authentication based condition and integrity protocol with a quassi puzzle to ensure the security. To resolve the re-direction attack SGSN is used. Here it uses Payload Encryption Key (PLK) to handle the man-in-the-middle attack. Next for bandwidth reduction a ticket-based authentication scheme is used. In addition to these, for ensuring the integrity EMSUCU protocol is used. A quasi puzzle is given at the last for the defensive mechanism client puzzles based on quasi partial collisions is used. For a flow contained development, this study first gives an introduction related to security in UMA network in the section one. The second section is a literature study of some previous related works. A well-structured and modularized proposal is given in section three followed by a simulation result in section four. At last an overall conclusion is given.

Here the DDoS attack is detected in a three way detection phase. Signaling and travesing through a number of network nodes enhances the detection in earlier manner and clear idea of attack detection. Quasi puzzle is quite easy and secure algorithm for avoiding the DDoS attack as soon as it is detect.

REFERENCES

Anita, E.A.M., 2014. A secure authentication framework for mobile ad hoc networks. Asian J Inform. Technol., 13: 58-67.

Boman, K., G. Horn, P. Howard and V. Niemi, 2002. UMTS security. Elect. Commun. Eng. J., 14: 191-204.

Gardezi, A.I., 2006. Security in Wireless Cellular Networks. Washington University in St. Louis, St. Louis, Missouri,.

Kambourakis, G., C. Kolias, S. Gritzalis and J.H. Park, 2011. DoS attacks exploiting signaling in UMTS and IMS. Comput. Commun., 34: 226-235.

Lei, Y., S. Pierre and A. Quintero, 2006. Client puzzles based on quasi partial collisions against DoS attacks in UMTS. Proceedings of the IEEE. Conference on Vehicular Technology, September 25-28, 2006, IEEE, Montreal, Quebec, ISBN: 1-4244-0062-7, pp: 1-5.

Oh, J., D. Kang, S. Kim and C. Im, 2012. 3G WCDMA Mobile network dos attack and detection technology. Networks, 1: 1-4.

Putz, S., R. Schmitz and T. Martin, 2001. Security mechanisms in UMTS. Data Prot. data Secur., 25: 1-10.

Shidhani, A.A. and V.C. Leung, 2008. Reducing re-authentication delays during UMTS-WLAN vertical handovers. Proceedings of the 19th International Symposium on Personal, Indoor and Mobile Radio Communications, September 15-18, 2008, IEEE, Cannes, France, ISBN: 978-1-4244-2643-0, pp: 1-5.

Southern, E., A. Ouda and A. Shami, 2011. Solutions to security issues with legacy integration of GSM into UMTS. Proceedings of the International IEEE. Conference on Internet Technology and Secured Transactions, December 11-14, 2011, IEEE, Abu Dhabi, UAE., ISBN: 978-1-4577-0884-8, pp: 614-619.