**Matej ROHLIK, Tomas VANEK**

Czech Technical University in Prague

# New Trends in Femtocell Backhaul Security

***Abstract***. *One of the relatively new services presented by mobile operators is a femtocell. A femtocell is a network located at the residential premises helping to extend the mobile signal to places which are difficult to cover. Furthermore, it enables the mobile operator to provide attractive service to the customer since the femtocell is connected to the mobile operator network using an IP based backhaul link over the public Internet. To ensure appropriate security over the untrustworthy environment, an IPsec tunnel is established between the femtocell access point and the provider's security gateway located at the core network perimeter. IPsec itself wasn't originally proposed to carry small voice packets resulting in a redundant overhead. This paper examines other security procedures, such as transport layer security (TLS) and Datagram TLS (DTLS) protocols.*

***Streszczenie.*** *W artykule zaprezentowano porównanie systemów ochrony pakietów danych w sieci komunikacji femtokomórek. W celu nawiązania i zabezpieczenia połączenia zastosowano tu tunelowanie IPsec między bramką operatora, a odbiornikiem, femtokomórką. Testom poddano procedury ochrony w protokołach TLS oraz DTLS. (**Nowe trendy w ochronie danych w komunikacji femtokomórek**).*

**Keywords:** Security, network, femtocell, protocol, IPsec, TLS, DTLS, SRTP, ZRTP.
**Słowa kluczowe:** ochrona, sieć, femtokomórka, protokół, IPsec, TLS, DTLS, SRTP, ZRTP.

## Introduction

A femtocell is a network located at the residential premises helping to extend the mobile signal to places which are difficult to cover. Furthermore, it enables the mobile operator to provide attractive service to the customer since the femtocell is connected to the mobile operator network using an IP based backhaul link over the public Internet. As the IP backbone Wide Area Network (WAN) topology, every available broadband technology (fiber, cable, digital subscriber line, etc.) technology can be used. The scenario is depicted in Fig. 1 [1].

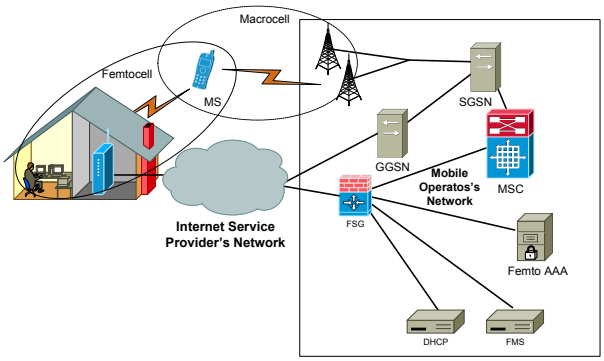


Fig.1. The Scenario of a Femtocell

The essential requirements imposed on the broadband technology are adequate transmission parameters such as jitter, delay, and bandwidth [2, 3].

## IP Backhaul Link Femtocell Security

### Architecture of the Femtocell

The central appliance of the femtocell is a device named Femtocell Access Point (FAP). Such device acts as a common access point known from the WiFi networks. The difference is that the mobile station (MS) is connected to the FAP using the 2G, 3G, or pre-4G network (GSM/GPRS/EDGE, UMTS, LTE, WiMAX, HSDPA, HSUPA, etc.). The FAP is then connected to the Femto-Security Gateway (FSG), located and the mobile operator core network perimeter, through the public Internet.

Since the public Internet is an untrustworthy environment, the user data (voice or data packets) and the signaling (control packets) are encapsulated and encrypted in a previously established IPsec tunnel. The femtocells connected to the FSG are managed by the respective Femto Management System (FMS) and are authenticate and authorized against the appropriate Femto AAA server. This approach is depicted in Fig. 2 [4,5].

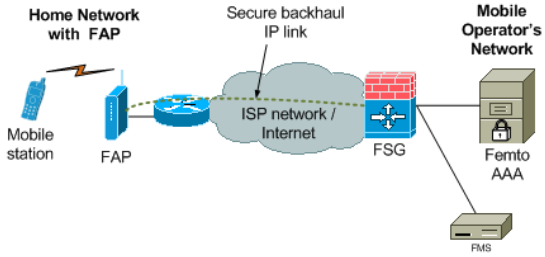


Fig.2. The Security Architecture of a Femtocell

The mutual authentication, between the network (FSG) and the FAP, is performed by the Internet Key Exchange version 2 (IKEv2) protocol with certificates [6, 7, 8]. The confidentiality between the FAP and the FSG is provided by setting up the IPsec/ESP tunnel [9].

The traffic in the operator's network (between the FSG and the FMS) is secured as well since such link is considered insecure. However, the IPsec protocol was not designed to carry small voice packets and behind Network Address Translation (NAT) causes a relatively big packet overhead. We have examined other security approached to eliminate the IPsec disadvantages.

### Considered Security Methods

This IPsec drawback can be eliminated using a Transport Layer Security (TLS) protocol defined in [10]. The TLS and SSL respectively, provide the end-points respective authentication and privacy. The practical approach, e.g., in WWW or email services, is to authenticate only the server and not the client. However, both, the server and the client can authenticate mutually. Similar to the IPsec protocol, the Public Key Infrastructure (PKI) keys can be applied to authenticate the communicating parties using certificates. TLS establishes an end-to-end secured session and is encapsulated into the reliable Transmission Control Protocol (TCP).

The TCP usage does not appear to be the optimal solution to carry the voice packets. Therefore, the Datagram TLS (DTLS) protocol was proposed to transport the data streams unreliably and is defined in [11]. The DTLS provides the same privacy to user data while using the User Datagram Protocol (UDP) as transport layer protocol.

For end-to-end data streams transport, Real-Time Transport Protocol (RTP) was designed. In conjunction with RTP Control Protocol (RCTP), RTP provides transport of the multimedia data and RTCP ensures Quality of Service (QoS) parameters [12]. Since none of the previously noticed protocols offer privacy and security to the carried data, another session oriented protocol was designed.

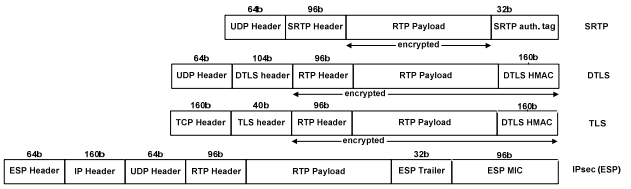


Fig.3. The Security Architecture of a Femtocell

Secure RTP (SRTP) and Secure RTCP (SRTCP) were proposed to remove the disadvantage of the unsecured protocols [13]. Both utilize the Advanced Encryption Standard (AES) in f8-mode (AES-f8) and in Segmented Integer Counter Mode (AES-CM), which is used as the default encryption algorithm. The message integrity is ensured by the HMAC-SHA-1 hash algorithm. As the extension of the original SRTP, ZRTP was developed [14]. ZRTP doesn't secure RTP streams itself, but uses a Diffie-Hellman protocol as a key-agreement method to negotiate the encryption keys for SRTP.

All of the previously noticed protocols, which provide respective security and privacy to the transported data, were taken into consideration as the adequate IPsec replacement with the main focus applied to the overhead, delay and jitter optimization.

**Alternative Security Protocols for the Femtocell Equipped Networks**

Using SRTP brings further complication in the way the ciphering keys are exchanged. There exist several standardized procedures to exchange the encryption keys (SDES [16], MIKEY [17]), and a couple of mechanisms which are currently marked as drafts (ZRTP [18]). However, none of the existing or proposed SRTP key exchange mechanisms do not count on IPsec usage. One of the newly standardized key exchange mechanisms for SRTP is using a DTLS protocol [19]. DTLS usage combined with SRTP, however, represents a complex and complicated solution, since first, it requires the original IPsec tunnel to exist for monitoring and security of the signaling and secondly, an addition of two new protocols – SRTP for protection and RTP stream and DTLS for security key exchange purposes.

As a better solution we propose to replace the IPsec technology using TLS and DTLS protocols, respectively. TLS will be used to build up an encrypted tunnel for signaling protection, remote monitoring and administration. Voice calls has to be carried by a DTLS tunnel. Fig. 3 depicts the bandwidth requirements for a single call accomplished using G.711 and G7.29 codecs secured by various encryption mechanisms. As can be seen usage of DTLS has approximately about 8 % higher demand on bandwidth compared to the traditional SRTP. However, assuming the whole communication infrastructure design, the usage of TLS and DTLS tunnel seems to be an easier and cleaner approach in comparison to the SRTP with different needed key-exchange protocol.

**TLS and DTLS Handshake Mechanisms**

In principle, TLS and DTLS protocols work in a relatively similar way. Based on the primary target of our research, we propose the corresponding changes of the selected protocol parts which require to be accomplished to the original TLS and DTLS protocols to provide and increase the overall communication efficiency instead of using the IPsec tunnel.

For further changes, we chose TLS protocol version 1.2 [20] and DTLS protocol draft version 1.2 as well [21]. The most significant change, compared to the previous versions (TLS 1.1 and DTLS 1.0), is the modification of the PRF (Pseudo-Random Function) which is used by the key derivation process. The current version of PRF does not use any combination of the old hashing functions MD5 a SHA-1 but only a single SHA-256.

By the reason of higher security for the usage of femtocells, we require the client (HeNB) to authenticate itself to the server (SeGW). Server to client authentication is always mandatory for TLS protocol. The authentication process utilizes the certification method based on X.509 certificates [22] and PKI (Public Key Infrastructure) standards [23].

Assuming TLS and DTLS, the key exchange mechanism is very similar and can be accomplished in the following two ways – complete and shortened. Complete handshake occurs in the beginning of the communication, while shortened can be used when new a connection in an existing session has to be created or refreshed.

**TLS – Transport Layer Security**

The TLS protocol is based on message exchange and each of the messages can be compressed, encrypted, padded, and attached with a MAC (Message Authentication Code). The full (complete) TLS handshake algorithm is depicted in Fig. 4. The optional messages are marked in the brackets. Messages of the Change Cipher Specification Protocol (CCSP), which are not part of the handshake protocol, are marked as italic. CCSP cause a switchover to the new negotiated algorithms and keys.

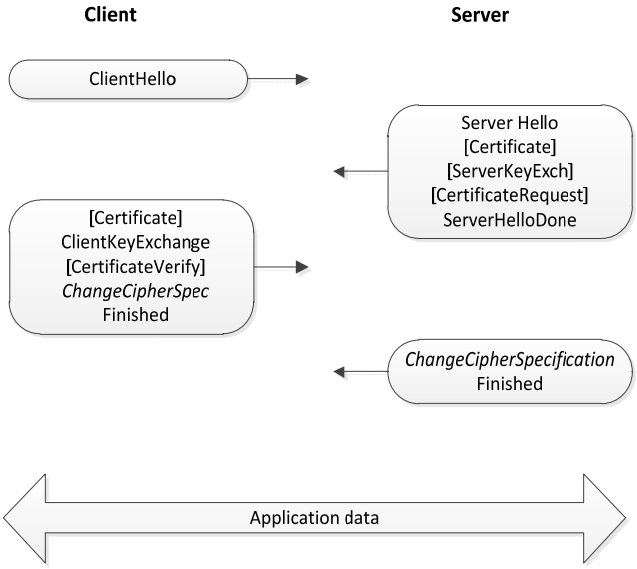


Fig.4. Complete general TLS/DTLS handshake process

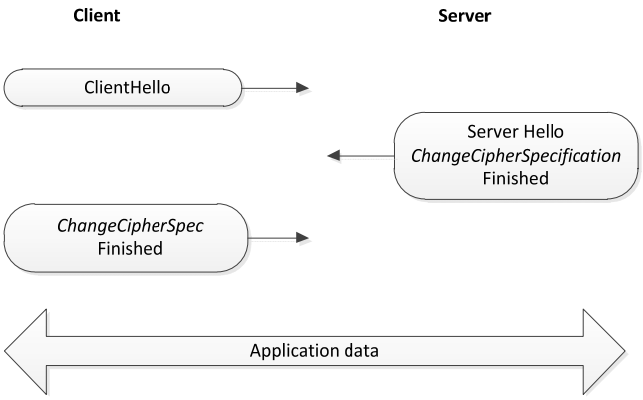


Fig.5. Simplified (resumed) TLS/DTLS handshake process

The simplified (resumed) TLS handshake for establishing new connections in existing TLS session is depicted in Fig. 5. The message labeling type is accomplished in the same way as in Fig. 4.

The security approach is based on fact that the HeNB and the SeGW, once manufactured, are provided with their own trustworthy private and public key information which is stored in the secure environment of the device [3].

**DTLS – Datagram Transport Layer Security**

DTLS handshake is done in the same way as TLS handshake only with a single difference. Because of UDP nature (no acknowledgment on delivery), DTLS itself has to handle it. This process is accomplished by retransmitting messages, if a loss or timeout occurs, and adding a stateless cookie exchange. The whole DTLS handshake process is depicted in Fig. 6.

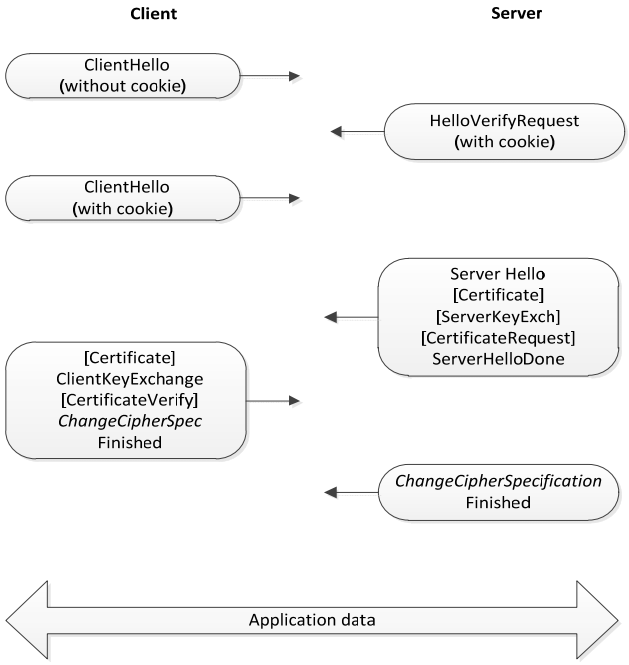


Fig.6. General full DTLS handshake process

Simplified DTLS handshake is accomplished in the same way as TLS handshake described in Fig. 5.

## Results

The measurement simulated a voice over IP call with several different codecs, encapsulations and cryptography algorithms providing security. The application layer protocol considered as an encapsulation protocol to the voice stream was RTP. Assumed security mechanisms were no security protocol, SRTP, TLS, and DTLS. ZRTP was utilized to negotiate encryption keys for SRTP. As a transport layer protocol, UDP and TCP were used. The Simena Network Emulator NE2000 [15] was applied to simulate one of the basic parameters of the network environments such as uplink/downlink bandwidth.

As the aim of this paper was to examine the currently available security methods to encrypt traffic between the FAP and mobile core network, the FAP was simulated by a laptop, the intermediate network by a Simena network emulator, and the core network by a firewall and another laptop (see Fig. 7).

The average length of the call was estimated to one minute. The measurements were accomplished in the range from 50 to 70 seconds since the measurement length does not affect the measurement itself.

Since FAP are assumed to be applied mainly in the household environment, an internet connection with parameters corresponding to a widespread technology ADSL (4 Mbps downlink and 0.25 Mbps uplink) was simulated. The home FAP is considered to operate in the "closed mode" where only allowed users (usually members of the family) are allowed to use the provided service. Therefore, only limited traffic can be considered (1 or 2 concurrent voice calls). As a consequence of the measured values, when QoS properly configured, low-utilization FAPs can be run at such low-speed connections.

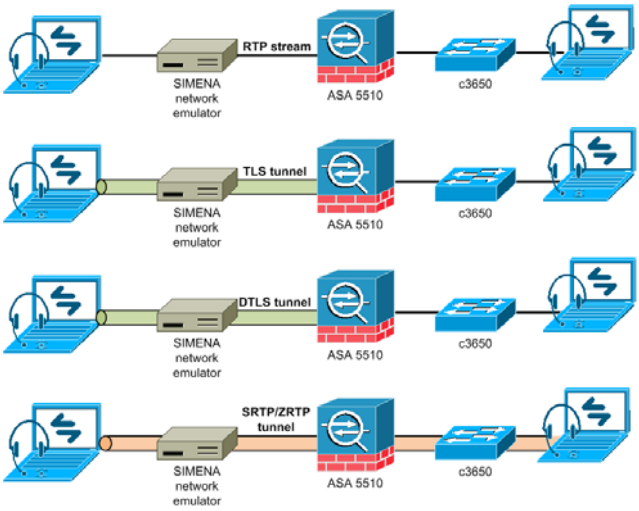


Fig.7. The Scenarios of the Simulations

For different security methods simulation, we utilized a Cisco ASA 5510 appliance (a firewall) which enabled us to capture both secured and unsecured traffic and its ensuing analysis. In case where the voice streams were encrypted by the SRTP protocol, the call conversation was established directly between the communicating parties (end stations) and the stream was not affected by the ASA firewall. The encryption keys were negotiated using the ZRTP protocol.

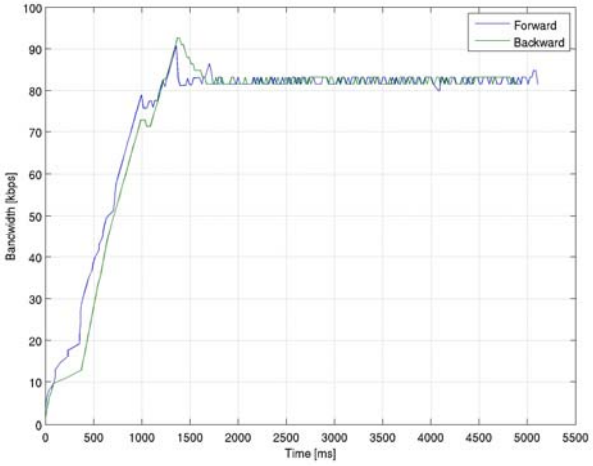


Fig.8. Bandwidth requirements for voice call with G.711 and SRTP

The Fig. 8 depicts the results of the one of a number of measurements which were accomplished. The bandwidth requirement is shown for G.711 codec while RTP stream is secured via SRTP. The total bandwidth is higher than the values in the Table 1 because the graph illustrated in the Fig. 1 includes the overhead of IPv4 protocol.

In the Fig. 9, an example of measured voice call jitter is shown. The graph represents the asymmetrical character of the simulated line. The jitter is relatively higher in the uplink than in the downlink direction which is less loaded.

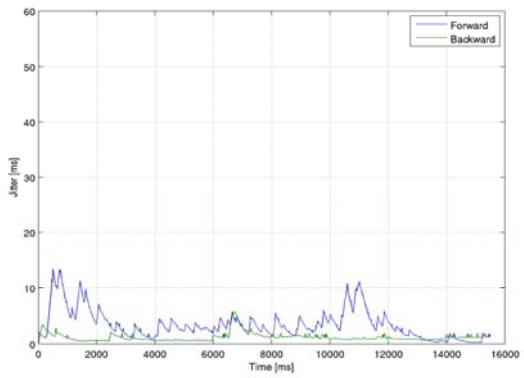


Fig.9. The Jitter of SRTP Secured Voice Call Using G.711 Codec

In the Table 1, the measured bandwidth requirements for a selected security protocol is shown. An RTP voice payload size was 20 ms for each codec. The mentioned bandwidths are related to the transport layer. The overall bandwidth requirements, when IPv4 based network layer and Ethernet link layer used, are increased by 60 B per packet, i.e., by 30 kbps.

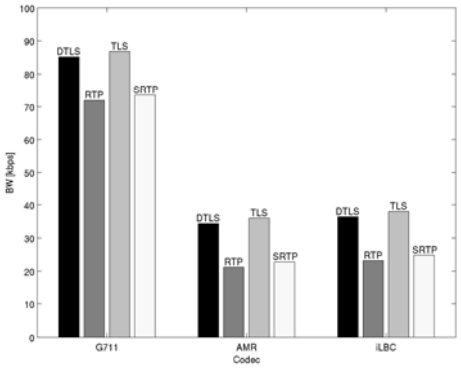


Fig.10. The BW Consumption Measured for Selected Transport Protocols and Codec

The Fig. 10 shows the average values of the transmission rate for each protocol which were determined from the analysis of the measured values.

Table 1. Measured Throughput On Transport Layer for Selected Security Protocols. RTP Voice Payload Size Was 20 ms

| Codec | Codec bitrate [kbps] | RTP [kbps] | SRTP [kbps] | TLS [kbps] | DTLS [kbps] | IPsec (ESP in tunnel mode) [kbps] |
|---|---|---|---|---|---|---|
| G.711 | 64.0 | 72.0 | 73.6 | 86.8 | 85.2 | 89.6 |
| iLBC | 15.0 | 23.2 | 24.8 | 38.0 | 36.4 | 40.8 |
| AMR | 13.2 | 21.2 | 22.8 | 36.0 | 34.4 | 38.8 |

Table 2. Measured Throughput On Transport Layer for Selected Security Protocols. RTP Voice Payload Size Was 10 ms

| Codec | Codec bitrate [kbps] | RTP [kbps] | SRTP [kbps] | TLS [kbps] | DTLS [kbps] | IPsec (ESP in tunnel mode) [kbps] |
|---|---|---|---|---|---|---|
| G.711 | 64.0 | 80.0 | 83.6 | 109.6 | 106.4 | 115.2 |
| iLBC | 15.0 | 31.2 | 34.8 | 60.8 | 57.6 | 66.4 |
| AMR | 13.2 | 29.6 | 33.2 | 59.2 | 56.0 | 64.8 |

Comparing the measured bandwidth values depicted in Tables 1 and 2, the usage of voice payload size of 10 ms enables the voice stream to have smoother pass over the network redeemed by a significant overhead growth. ZRTP increases the packet size by 4 B, i.e., for voice payload size of 20 ms by 1.6 kbps which is negligible and acceptable.

**Joint TLS and DTLS Key Exchange**

Fig. 11 illustrates a common process of keys/algorithms negotiation for TLS and DTLS. To make it simple, the `ServerKeyExchange` and `ClientKeyExchange` messages were omitted. Since these messages are used only in a situation where the certificate X.509 does not contain ciphering keys but keys designated for DSA signing (Digital Signature Algorithm) or parameters for the DH (Diffie-Hellman) protocol. In practical applications, the most common choice is RSA (algorithm proposed by Rivest, Shamir and Adleman) where the certificate contains the public key used for ciphering. In such situation, it is not necessary to exchange the above mentioned messages. Messages beginning with a TLS abbreviation are exchanged using TCP. Those messages having a DTLS abbreviation pre-pended are interchanged by UDP.

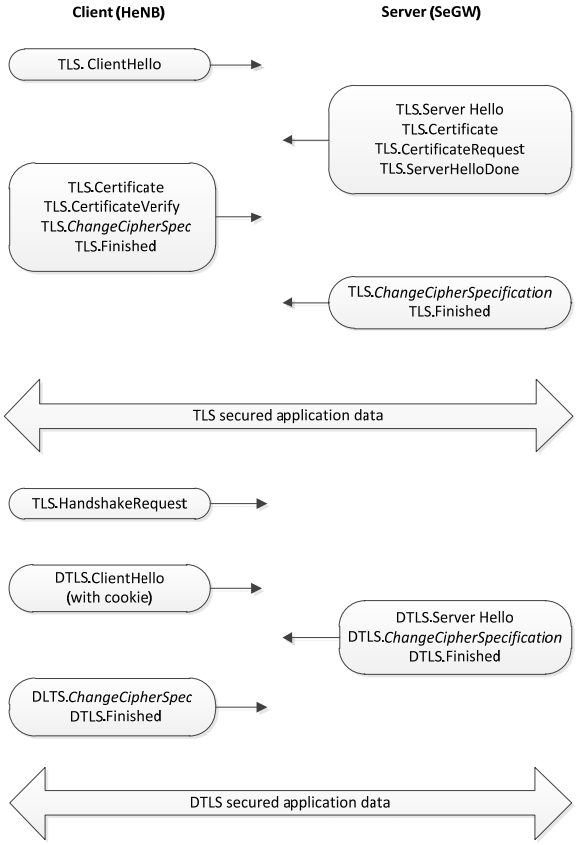


Fig.11. Joint TLS/DTLS Handshake Process

A new `TLS.HandshakeRequest` message was added into the exchange between TLS and DTLS protocols and it is fully illustrated in Fig. 12. This message, which is not a part of the TLS standard, is used to initiate a shortened DTLS handshake and concurrent stateless cookie handover to the server side (SeGW).

Since this message is sent using TCP, the delivery is reliable. The stateless cookie is calculated from the `SessionID` of the TLS session as follows:

`DTLS.Cookie=SHA-256(SessionID)`

This provides the binding between the respective TLS and DTLS sessions.

The above described exchange enables to establish a TLS and DTLS tunnel where the ciphering keys and algorithm can be established independently for each of them.

The `MessageType` field value was chosen 17 since this value one is not currently occupied. The Length field is used to provide the total message length, and the `DTLS.Cookie` filed carries a 32-bytes long identification.

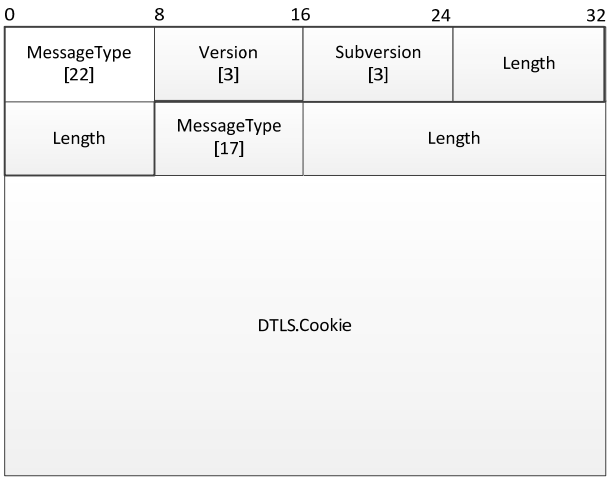


Fig.12. Joint TLS/DTLS Handshake Process

**Conclusion**

Within the optimization of the femtocell backhaul link security methods, the existing cryptographic protocols (SRTP, DTLS, and TLS) were practically experimented and analyzed.

Even though the differences between the analyzed protocols are not large, the common location of a femtocell will be behind a NAT enabled device (ADSL modem, firewall, etc.) In this case, the bandwidth requirements for IPsec increase for approximately 5 % because of the NAT-T mechanism. TLS and DTLS have similar bandwidth requirements, however, DTLS is based on UDP and such application is less susceptible to packet loss and out-of-order delivery.

Based on the analyzed results, as the most advanced and prospective solution to replace the complex IPsec mechanism is the combination of the TLS and DTLS protocols where DTLS will be applied as a voice stream security algorithm and TLS as signaling and FAP management security method.

Our further research was focused on the replacement of the currently used IPsec protocol using TLS and DTLS protocols. The integration of both protocols resulted into a joint TLS and DTLS handshake mechanism. The handshake process was modified using a new message referred as `HandshakeRequest`. This mechanism enables to build up a new DTLS connection by using the existing TLS tunnel.

The optimization and changes were considered with respect to the total influence of the currently standardized protocols. Therefore, the TLS and DTLS changes were minimized. However, the optimization process still provides areas which can be further investigated and will be the next phase of our research (e.g., PRF function modification to derive the ciphering keys).

*This research work was supported by MSMT under the project no. MSM 6840770038.*

REFERENCES

[1] Chandrasekhar, V., Andrews, J. G., Gatherer, A., Femtocell Networks: A Survey. In *IEEE Communications Magazine*. 2008.

[2] Kim, R. Y., Kwak, J. S., Etemad, K., Wimax Femtocell: Requirements, Challenges, and Solutions. In *IEEE Communications Magazine*. 2009.

[3] Hasan, S. F., Siddique, N. H., Chakraborty, S., Femtocell Versus WiFi – A Survey And Comparison of Architecture and Performance. In *Wireless Vitae'09*. 2009.

[4] *Security Issues in Femtocell Deployment* [online]. 2008 [cit. 2011-03-28]. Available: http://www.gsmworld.com/documents/fcg0510.pdf.

[5] *3GPP2 S.S0132-0 "Femtocell Security Framework 1.0"*, http://www.3gpp2.org/public_html/specs/S.S0132-0_v1.0_Femtocell_Security_Framework.pdf

[6] Korver, B., *The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2, and PKIX (RFC4945)* [online]. 2007 [cit. 2011-03-28]. Available: http://tools.ietf.org/html/rfc4945.

[7] Kaufman, C., *Internet Key Exchange (IKEv2) Protocol (RFC4306)* [online]. 2005 [cit. 2011-03-28]. Available: http://tools.ietf.org/html/rfc4306.

[8] Black, D., McGrew, D., *Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol (RFC5282)* [online]. 2008 [cit. 2011-03-28]. Available: http://tools.ietf.org/html/rfc5285.

[9] Manral, V., *Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH) (RFC4835)* [online]. 2007 [cit. 2011-03-28]. Available: http://tools.ietf.org/html/rfc4835

[10] Dierks, T., Rescorla, E., *The Transport Layer Security (TLS) Protocol Version 1.2 (RFC5246)* [online]. 2008 [cit. 2011-03-28]. Available: http://tools.ietf.org/html/rfc5246

[11] Rescorla, E., Modadugu, N., *Datagram Transport Layer Security (RFC4347)* [online]. 2006 [cit. 2011-03-28]. Available: http://tools.ietf.org/html/rfc4347.

[12] Schulzrinne, H., Casner, S., Frederick, R., Jacobson, V., *RTP: A Transport Protocol for Real-Time Applications (RFC3550)* [online]. 2003 [cit. 2011-03-28]. Available: http://tools.ietf.org/html/rfc3550.

[13] Baugher, M., McGrew, D., Naslund, M., Carrara, E., Norrman, K., *The Secure Real-time Transport Protocol (SRTP) (RFC3711)* [online]. 2004 [cit. 2011-03-28]. Available: http://tools.ietf.org/html/rfc3711.

[14] Zimmermann, P., Callas, J., Johnston, A. *ZRTP: Extensions to RTP for Diffie-Hellman Key Agreement for SRTPdraft-zimmermann-avt-zrtp-01. (RFC Draft)* [online]. 2006 [cit. 2011-03-28]. Available: http://tools.ietf.org/html/draft-zimmermann-avt-zrtp-01.

[15] *Simena Network Emulator NE2000*, [online]. 2010 [cit. 2011-03-28]. Available: http://simena.net/products/network-emulator-2/

[16] Andreasen, F., Baugher, M., Wing, D., *Session Description Protocol (SDP) Security Descriptions for Media Streams (RFC 4568)*, IETF, 2006, [online], http://tools.ietf.org/html/rfc4568

[17] Arkko, J., Carrara, E., Lindholm, F., Naslund, M., Norrman, K., *MIKEY: Multimedia Internet KEYing (RFC 3830)*, IETF, 2004, [online], http://tools.ietf.org/html/rfc3830

[18] Zimmermann, P., Callas, J., Johnston, A., Ed., *ZRTP: Media Path Key Agreement for Unicast Secure RTP (RFC 6189)*, IETF, 2011, [online] http://tools.ietf.org/html/rfc6189, ISSN: 2070-1721

[19] McGrew, D., *Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP) (RFC 5764)*, IETF, 2010, [online], http://www.ietf.org/rfc/rfc5764.txt

[20] Dierks, T., Rescorla, E., *The Transport Layer Security (TLS) Protocol Version 1.2 (RFC 5246)*, IETF, 2008, [online], http://www.ietf.org/rfc/rfc5246.txt

[21] Rescorla, E., Modadugu, N., *Datagram Transport Layer Security version 1.2, draft-ietf-tls-rfc4347-bis-06.txt*, IETF, 2011, [online], http://tools.ietf.org/html/draft-ietf-tls-rfc4347-bis-06

[22] Cooper, D. et al., *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (RFC 5280)*, IETF, 2008, [online], http://tools.ietf.org/html/rfc5280

[23] Housley, R., *Cryptographic Message Syntax (CMS) (RFC 5652)*, IETF, 2009, [online], http://tools.ietf.org/html/rfc5652

***Authors**: Matej Rohlik, Tomas Vanek, Czech Technical University in Prague, Department of Telecommunications, Technicka 2, 166 27 Prague, Czech Republic, E-mail: matej.rohlik@fel.cvut.cz, tomas.vanek@fel.cvut.cz.*