TICTOC
Internet-Draft
Intended status: Standards Track
Expires: March 19, 2012

Y. Xu
Huawei Technologies

September 16, 2011

IPsec security for packet based synchronization
draft-xu-tictoc-ipsec-security-for-synchronization-02.txt

Abstract

Cellular networks often use Internet standard technologies to handle synchronization. This document defines an extension based on WESP. Usually, several traffic flows are carried in one IPsec tunnel, for some applications, such as, 1588 or NTP, the packets need to be identified after IPsec encryption to handle specially. In order to achieve high scalability in implement, a separate IPsec tunnel will not be established for some special traffic. This document analyses the need for security methods for synchronization messages distributed over the Internet. This document also gives a solution on how to mark the synchronization message when IPSec is implemented in end to end frequency synchronization."

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 6, 2012.

Table of Contents

1. Introduction

When transferring timing in internet, a shared infrastructure is used, and hence the path is no longer physically deterministic. It leaves open the possibility to disrupt, corrupt or even spoof the timing flow, where a timing signal purports to come from a higher quality clock than it actually does. In the extreme, this may be used to attack the integrity of the network, to disrupt the synchronization flow, or cause authentication failures. On the other hand, it may be possible for unauthorized users to request service from a clock server. This may overload a clock server and compromise its ability to deliver timing to authorized users.

For the cellular backhaul applications, two kinds of synchronization are needed, one is the recovery of an accurate and stable frequency synchronization signal as a reference for the radio signal (e.g. GSM, UMTS FDD, LTE FDD). In addition to frequency synchronization, phase/time synchronization are also needed in Mobile technologies, This is the case for the TDD technologies such as UMTS TDD,LTE TDD.

Frequency synchronization is normally implemented in an end-to-end scenario where none of the intermediate nodes in the network have to recognize and process the synchronization packets. However In phase/ time synchronization, a hop-by-hop scenario will request intermediate nodes to process the synchronization packets If very accurate phase/ time is needed (e.g. sub-microsecond accuracy).

Femtocell is the typical cellular backhaul application that requires time synchronization. A Femtocell is defined as a wireless base station for deployment in residential environments and is typically connected to the mobile core network via a public broadband connection (eg., DSL modem, cable modem). Femtocell improves cellular network coverage and saves cost for operators. Just like a typical macrocell (larger base station), a Femtocell (residential base station) requires a certain level of synchronization (frequency or phase/time) on the air interface, predominantly frequency requirements.

The [3GPP.33.320] specification defines some of the high-level network architecture aspects of a Home NodeB (3G UMTS) and a Home eNodeB (4G LTE). In addition, the Femto Forum organization also provides a network reference model very similar to 3GPP. Both architectures have commonalities as illustrated in Figure 1.

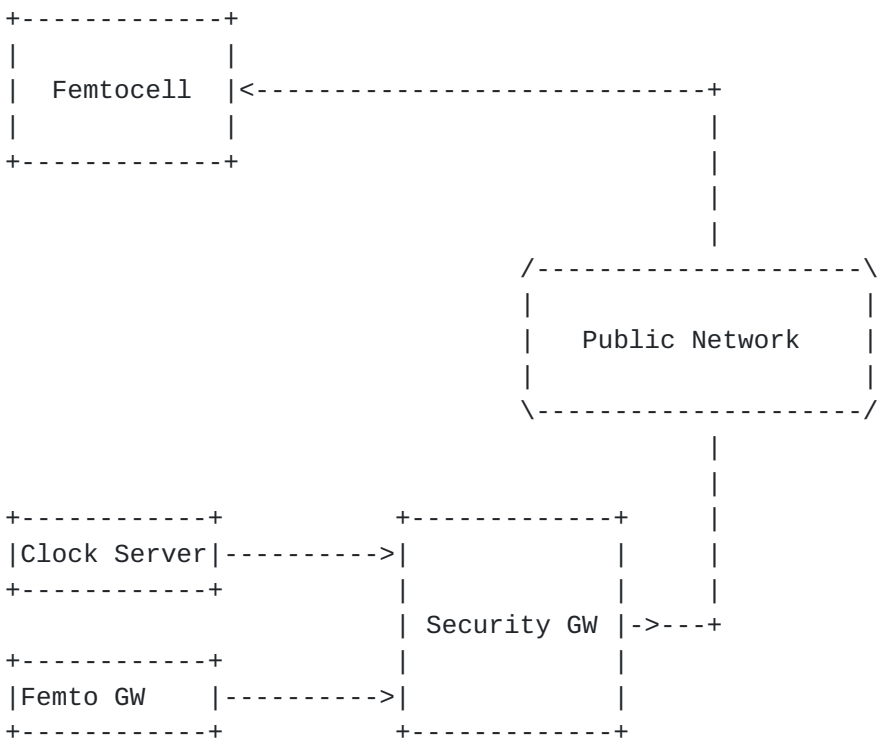

Figure 1. Typical Architecture of a Femtocell Network

The network architecture shows that a public network is used to establish connectivity between Femtocell and core network elements (e.g., Security Gateway, Femto Gateway, Clock server, etc.). With respect to synchronization process, Femtocell will therefore see synchronization messages exchanged over the public network (e.g, Internet). This presents a set of unique challenges for mobile operators.

One challenge involves the security aspects of such the Femto architecture. In both reference models, the communication between Femtocell and Femto Gateway is secured by a mandatory Security Gateway function. The Security Gateway is mandatory since the Femto Gateway and Clock server communicate to Femtocell via a public backhaul broadband connection (also known as the 3GPP iuh interface or Femto Forum Fa interface). The [3GPP.33.320] specification requires that the Femtocell SHALL support receiving time synchronization messages over the secure backhaul link between Femtocell and the Security Gateway, and Femtocell SHALL use IKEv2 protocol to set up at least one IPsec tunnel to protect the traffic with Security Gateway.

This document provides analysis on security requirements for packet-based synchronization and proposes IPsec security solution for end to end frequency synchronization.

2. Terminology used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

3. Security requirements for synchronization

The ITUT [G.8265] specification provides general consideration on synchronization security. Because packet-based timing streams may be observed at different points in the network, there may be cases where timing packets flow across multiple network domains which may introduce specific security requirements. There may also be aspects of security that may be related to both the network (e.g. authentication and/or authorization) and to the synchronization protocol itself. ITUT [G.8265] specification recommends to use existing, standards-based security techniques to help ensure the integrity of the synchronization. Examples may include encryption and/or authentication techniques, or network techniques for separating traffic, such as VLANs or LSPs. Specifically for the performance issue, it may not be possible to implement some security requirements without actually degrading the overall level of timing or system performance. From above analysis, following synchronizations requirements are listed:

1. synchronization client SHOULD be prevented from connecting to rogue clock servers
2. clock servers SHOULD be prevented from providing service to unauthorized synchronization client
3. Security mechanisms to achieve synchronization SHOULD minimize any degradation in performance and this side effect SHOULD be controlled to meet specific synchronization requirements(e.g., Femtocell synchronization)

4. Security mechanism for synchronization

There are mainly two kinds of security mechanism used in current synchronization: authentication-based and encryption-based.

For the authentication-based security mechanism, a shared secret key between the synchronization client and the clock servers is used to compute an authentication code (known as an "Integrity Check Value",

ICV) over the entire message datagram. [IEEE1588] contains an experimental security annex defining an authentication-based approach. This approach also implements a challenge-response mechanism to confirm the creation of any security association (SA) between a clock servers and a synchronization client. A limitation of the process is that no method of sharing the key is proposed in [IEEE1588]. This MUST be handled by other means.

For the encryption-based security mechanism, a shared-key approach is also used. Instead of creating an ICV, the shared key is used to encrypt the contents of the packet completely. The encryption might be performed in the synchronization device itself, or it might be performed in a separate device, e.g. a secure gateway. An example might be where the timing packets have to pass through an encrypted tunnel (e.g. an IPSec tunnel). Full encryption might be required for various reasons. The contents of the packet may be considered secret, such as might be the case where accuracy of the time distribution is being sold as a service. Alternatively, it may be because other traffic from a device is considered secret, and hence it is easier to encrypt all traffic.

IPsec, as a popular security mechanism, is being considered in some mobile applications, especially in case of unsecure backhaul links (e.g. Femtocells, [3GPP.33.320]) being involved. IPsec can provide data source authentication, confidentiality, integrity that is suitable to end to end synchronization without intermediate nodes. It provides security services by Authentication header (AH) and Encapsulating security payload (ESP). Authentication Header provides integrity protection and data origin authentication. Moreover, ESP can be used to provide confidentiality besides data origin authentication, connectionless integrity. For the time packet protection, the critical issue is the precision of the timestamps. That is the receiver must mark the time as soon as possible when taking over the time packet, and the time will be used for frequency synchronization. And in the implementation, an IPsec tunnel is created to carry all the traffic between the IPsec end points considering the cost of IPsec SA establishment, i.e., this IPsec tunnel will be used to protect both the service traffic packets and time packets. Therefore, for protect against active and passive attack, confidentiality and integrity will be configured when deploying IPsec processing policy. But nodes cannot recognize 1588 packets as defined in [IEEE1588]as the port is encrypted by IPsec. It becomes complicated when processing IPsec packets as the nodes will not be able to identify the 1588 packets that need to be time stamped any more. This document describes a method to resolve this problem. For time packets, some identifiers that can be used to recognize all such packet at the physical layer are defined in WESP, and all of these are provided with data integrity protection. For

example, if only frequency synchronization is needed, an end-to-end scenario where none of the intermediate nodes in the network have to recognise and process the synchronization packets might be suitable to use IPsec security mechanism. In this case, the synchronization packets will be encrypted if the packed is transported in the IPSec tunnel.

IPsec can meet synchronization requirement 1 and 2 in section 3. However IPsec still need some enhancement to meet requirement 3. Normally, device will decrypt IPSec message in IP layer, but in order to improve the synchronization accuracy, some synchronization protocol (e.g. [IEEE1588]) requests to process the synchronization message in hardware, therefore the synchronization device may need to identify synchronization messages in physical layer before the message is decrypted. How to identify the synchronization messages in IPsec becomes the most important issue to keep the synchronization accuracy in IPsec synchronization scenario.

5. The extension of WESP

As discussed above section, it has advantage to identify whether the tunnel packets received by synchronization client are the special timing packets or not. This section proposes a solution to identify the timing packets When using IPsec to protect the whole time synchronization message. The main thought is to use time packet identifier which is included in the WESP format to identify whether the received data packet is a timing packet or not.

5.1. Existing WESP format

[RFC5840] describes an encapsulating ESP, i.e., WESP, and affords an extension for ESP. This document applies WESP to provide a mechanism to identify time packet within an IPsec tunnel, the IPSec endpoints could distinguish the time packet and do the corresponding synchronization processing.

The WESP format is as follows:

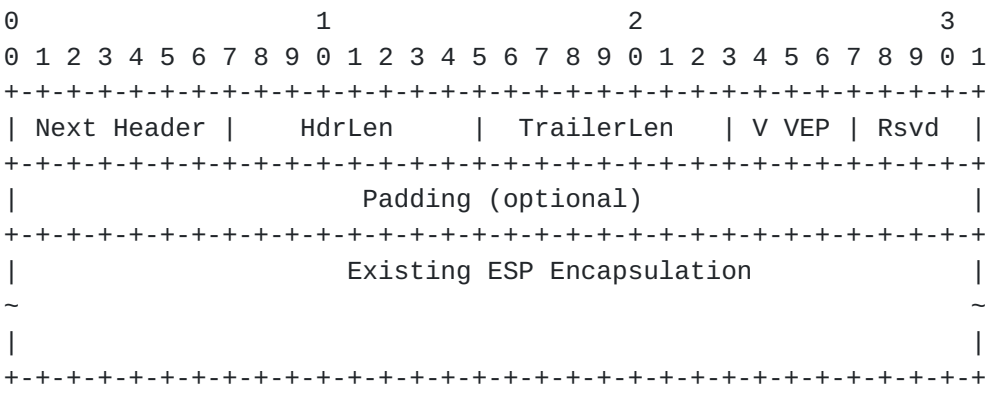

Figure 2. Format of an WESP Packet

These fields are introduced with the extended WESP format in next section.

5.2. Extended WESP format

This document describes the extension for the WESP for the additional application. It allows the ESP receiver or intermediate node not only distinguish encrypted and unencrypted traffic, but also identify whether the encrypted packets are the common packets or the time packets.

The extension format is depicted as follows:

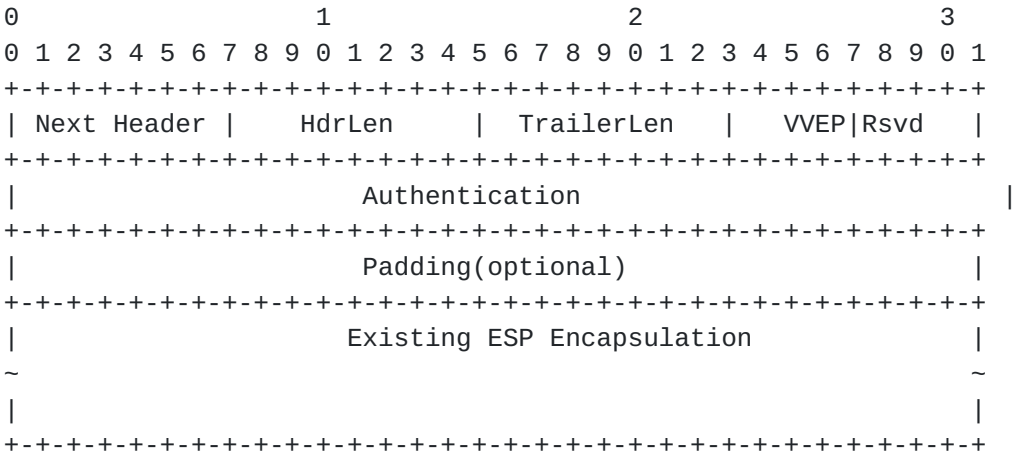

Figure 3. The extended WESP format

The definitions of these fields are as follows:

- Next Header is identical with the definition in [RFC5840]. It MUST be the same as the Next Header field in the ESP trailer when using ESP in the Integrity-only mode. When using ESP with encryption, the "Next Header" field looses this name and semantics and becomes an empty field that MUST be initialized to all zeros. The receiver MUST ensure that the Next Header field in the WESP header is an empty field initialized to zero if using ESP with encryption.
- HdrLen is identical with the definition in [RFC5840]. It is the offset from the beginning of the WESP header to the beginning of the Rest of Payload Data (i.e., past the IV, if present and any other WESP options defined in the future) within the encapsulated ESP header, in octets. HdrLen MUST be set to zero when using ESP with encryption.
- TrailerLen contains the size of the Integrity Check Value (ICV) being used by the negotiated algorithms within the IPsec SA. TrailerLen MUST be set to zero when using ESP with encryption. One issue must be taken into account that if using ESP with encryption, TrailerLen has lost the significance of ICV, as any attacker could juggle the field definition above, Next Header, HdrLen, TrailerLen to zero, and forward the modified packet to the receiver. The receiver will deal with the dummy encrypted packet falsely.
- Authentication contains extended data type, extended data length, the optional Algorithm ID field and extended data and ICV when using ESP with encryption. This part will be depicted in next section.
- Flags: The bits are defined most-significant-bit (MSB) first, so bit 0 is the most significant bit of the flags octet. The four bits "Rsvd" are used for the future, the least significant bit of the four bit to indicate the some extended information is included when using ESP not only integrity but also with encryption, i.e., if the least significant bit is set to one, the corresponding extended information will be contained in Authentication payload.

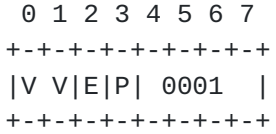

Figure 4: Flags Format

The definitions of each specific field in flags is as follows:

- Version (V): It requires the new version number, and MUST be sent as 0 and checked by the receiver.

- Encrypted Payload (E): Setting the Encrypted Payload bit to 1 indicates that the WESP (and therefore ESP) payload is protected with encryption. If this bit is set to 0, then the payload is using integrity-only ESP.
- Padding header (P), 1 bit: If set (value 1), the 4-octet padding is present. If not set (value 0), the 4-octet padding is absent. The alignment requirement must be guarantee as defined in [RFC5840].
- Rsvd, 4 bits: Reserved for future use. The reserved bits MUST checked whether the least significant bit is set as 0 or 1. If setting with 0, it will be ignored by the receiver. If setting with 1, the receiver will check the correction by ICV, either TrailerLen using ESP without encryption or Authentication when using ESP with encryption.

5.3. Authentication field

The Authentication field is comprised of extended data type, extended data length, the optional Algorithm ID field and extended data and ICV when using ESP with encryption. The extended data type indicates the packet type. When the type is time packets, it could identify whether the time packet is the event message or not. In addition, ICV parts offer the authentication of data integrity for the whole extended Data is provided.

The figure of the proposed flexible ESP format is as following:

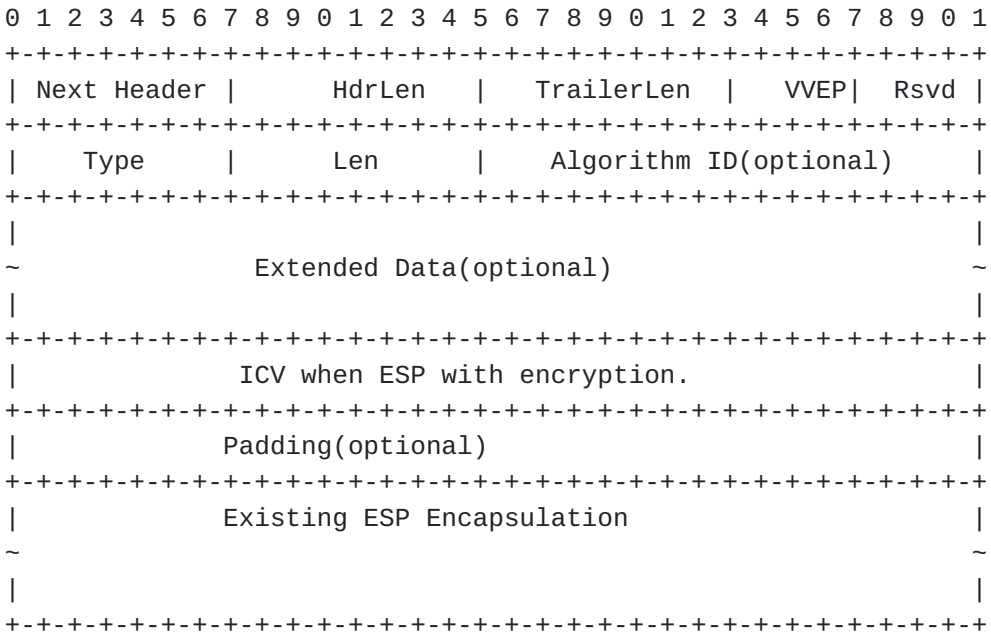

Figure 5. The detailed WESP format

In Femtocell scenario, as the link between Security Gateway and clock server is normally security path, the message transmitted between them are in plain text. When Security Gateway receives the message, it identifies the time packet at first, then put appropriate value to Data type field to identify the message type in Payload Data. After that, it could put more packet information into Extended Data Payload, such as UDP port number or timestamps, then Extended Data Length, Algorithm ID, Extended Data integrity Check value (Figure 4), could also be filled consequently. The following figure illustrates on how to use this new flexible ESP format to identify time packet.

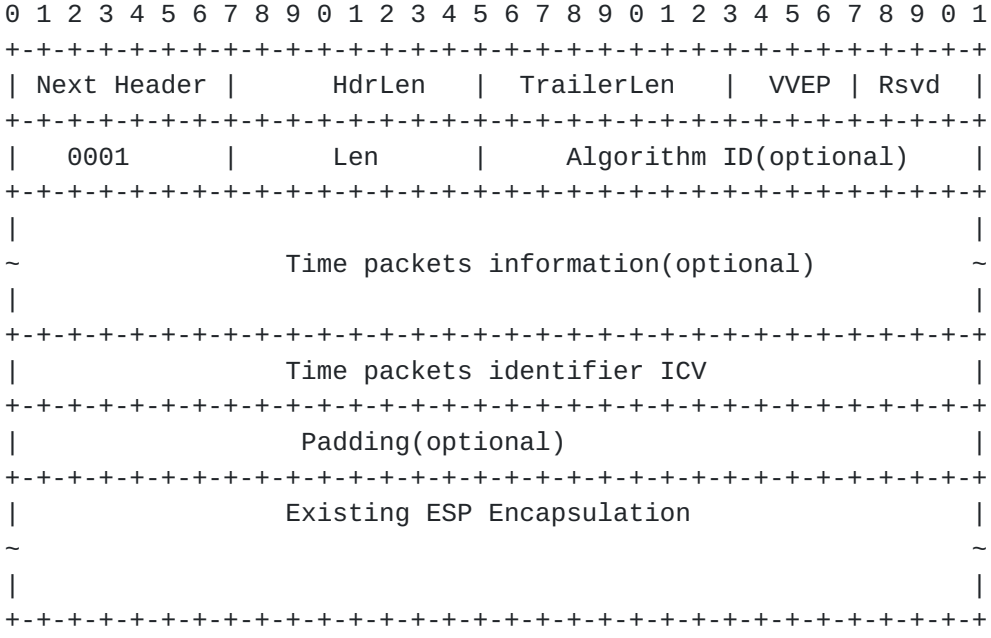

Figure 6. WESP format for time-packet

- o type (8-bit) - The value 0x1 here indicates that the extended context is time packet.
- o Length (16-bit)- The length of whole extended additional authentication data
- o Time packets information(variable)- the addintional message information, such as UDP port number or timestamps. It is a part of Authentication payload.
- o Algorithm ID- It indicates which algorithm could be used to generate the extended data ICV. It is a part of Authentication payload.The integrity algorithm negotiated during IKEv2 could be used, also Algorithm ID field in the extended additional

authentication data could be marked to indicate the integrity algorithm, such as HMAC-SHA1, HMAC-256, or others. It is a part of Authentication payload.

- o Time packets identifier integrity Check value (variable) - Time packets identifier integrity Check value, and used to guarantee the integrity of transmission.

Time packets information, Algorithm ID are the optional fields. As the integrity protection is only for the Extended Data when ESP with encryption but not for the whole ESP packet, the time delay of calculation can be decreased. In addition, if the integrity protection is not necessary, this part of security validation could be ignored.

6. Example

In this section, the procedure to identify time packet in Security Gateway scenario is depicted.

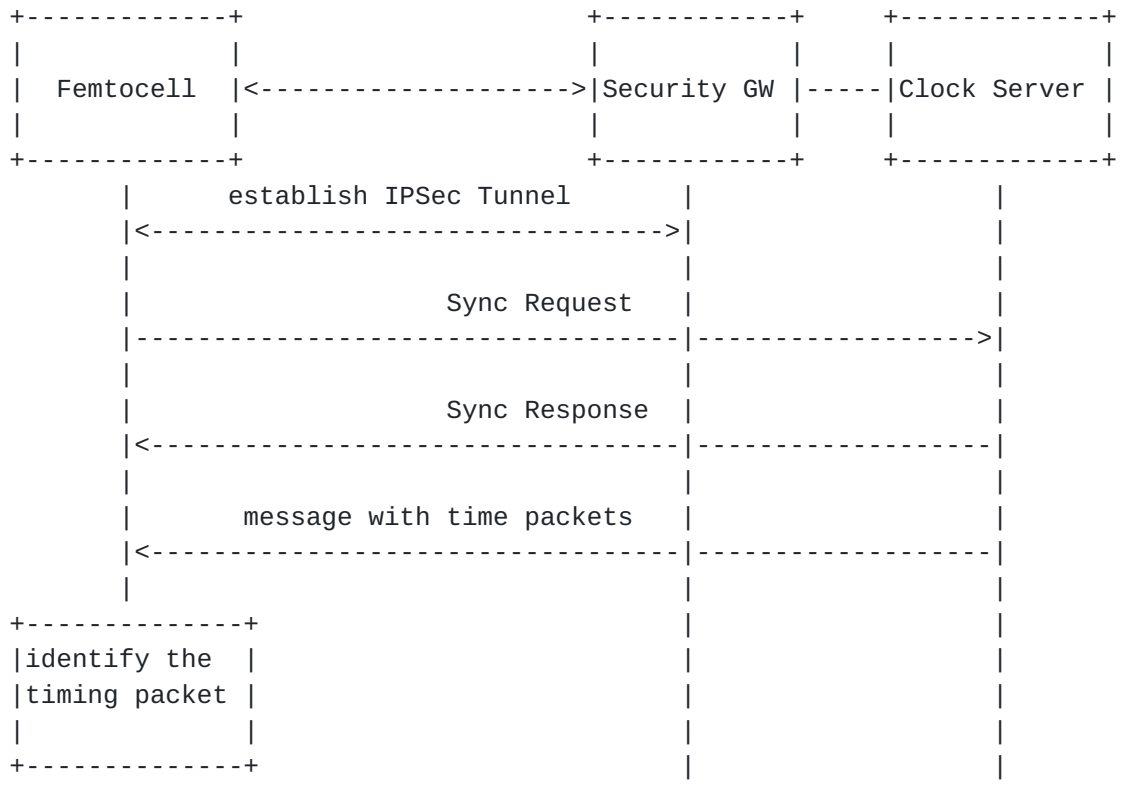

Figure 7. Example Procedure

In the Security Gateway scenario, The IPsec with tunnel mode is

established between Femtocell and Security Gateway. After Femtocell and Clock server exchange the Sync Request and Sync Response, the clock server will send the time packets to Femtocell to implement frequency synchronization with the protection of IPsec tunnel. When Femtocell receives the message, it can identify whether it is time packet, and can also identify whether the time packet is the event message by the time packet information in the unencrypted field as defined in the new ESP format. If the message is time packet and identifies that it is the event message, Femtocell will do special process for the event message, such as recording the message receiving time. On the server side, When Security Gateway receives the message, it identifies the time packet at first, then put appropriate value to Data type field to identify the message type in Payload Data, after that, it could put more packet information into Authentication Payload, such as UDP port number or timestamps, then Extended Data Length, Algorithm ID, Extended Data integrity Check value, could also be filled consequently.

7. IPv4/v6 consideration for IPsec based sychronization

IPsec is a security mechanism used both for IPv4 and IPv6, and WESP-based solution has no impact on the IPv4 header and makes the transition/migration from IPv4 to IPv6 seamless.

8. Security Considerations

This protocol variation inherits all the security properties of regular ESP as described in [RFC4303].

This document describes the modification or extension for the WESP for the additional application. The approach described in this document requires the ESP endpoints to be modified to support the new protocol. It allows the ESP receiver or intermediate node not only to distinguish encrypted and unencrypted traffic deterministically, but also identify whether the encrypted packets are the common packets or the time packets by a simpler implementation for the transport node.

Note that whether the time packets identified by the defined mark or tag are transparent or not, there is always a possibility for attackers to employ interception attacks to block transmission. How to prevent interception attack is out of scope of this draft.

9. IANA Considerations

There have been no IANA considerations so far in this document.

10. Acknowledgments

The authors appreciate the valuable work and contribution done to this document by Marcus Wong.

11. References

11.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.

[RFC5840] Grewal, K., Montenegro, G., and M. Bhatia, "Wrapped Encapsulating Security Payload (ESP) for Traffic Visibility", RFC 5840, April 2010.

11.2. Informative References

[3GPP.33.320] 3GPP, "Security of Home Node B (HNB) / Home evolved Node B (HeNB)", 3GPP TS 33.320 10.3.0, June 2011.

[G.8265] IEEE, "Architecture and requirements for packet based frequency delivery", V0.2 June 2010.

[IEEE1588] IEEE, "Standard for A Precision Clock Synchronization Protocol for Networked Measurement and Control Systems", IEEE Std 1588-2008.

Author's Address

Yixian Xu
Huawei Technologies
Huawei Building, Xinxi Road No.3
Haidian District, Beijing 100085
P. R. China

Phone: +86-10-82836300
Email: xuyixian@huawei.com