Análisis de Caso de Uso Rih Project

***Casos de Uso (Formato Alto nivel)***

|  |  |
| --- | --- |
| ***Caso de Uso*** | Enviar Datos |
| ***Actores*** | Smart Meter (SM) / Sink (Gateway) |
| ***Tipo*** | Primario |
| ***Descripción*** | Este caso de uso comienza cuando el SM / Sink contiene datos de interés (medición de voltaje, consumo, precio, etc) y desea enviarlo a un destino (SM o Sink). |

|  |  |
| --- | --- |
| ***Caso de Uso*** | Retransmitir Datos |
| ***Actores*** | Smart Meter (SM) / Sink (Gateway) / Repeater |
| ***Tipo*** | Primario |
| ***Descripción*** | Este caso de uso comienza cuando el SM / Sink / Repeater recibe un paquete y éste forma parte de la ruta hacia el destino y debe retransmitir el paquete hasta otro SM vecino. |

|  |  |
| --- | --- |
| ***Caso de Uso*** | Procesar Datos |
| ***Actores*** | Smart Meter (SM) / Sink (Gateway) |
| ***Tipo*** | Esencial |
| ***Descripción*** | Este caso de uso comienza cuando el SM / Sink recibe un paquete (de control o de datos), independiente si es destinado a él o no. Decide qué hacer con el paquete recibido (retransmitir, eliminar, encolarlo o guardarlo) y generar estadísticas y métricas relevantes a la red. |

|  |  |
| --- | --- |
| ***Caso de Uso*** | Asegurar Datos |
| ***Actores*** | Smart Meter (SM) / Sink (Gateway) |
| ***Tipo*** | Real (Sujeto a tecnología de entrada) |
| ***Descripción*** | Este caso de uso comienza cuando el SM/ / Sink crea/recibe un paquete de datos y desea enviarlo/recibirlo con mecanismos de seguridad asociados al protocolo. |

***Casos de Uso (Formato Extendido)***

|  |  |
| --- | --- |
| ***Caso de Uso*** | Enviar Datos |
| ***Actores*** | Smart Meter (SM) / Sink (Gateway) |
| ***Propósito*** | Transmitir los datos de interés al destino |
| ***Precondición*** | Calcular/Medir y almacenar las variables de interés. |
| ***Resumen (Descripción)*** | Este caso de uso comienza cuando el SM / Gateway contiene datos de interés (medición de voltaje, consumo, precio, etc) y desea enviarlo a un destino (Gateway/SM). |
| ***Tipo*** | Primario |
| ***Referencias Cruzadas*** | RF1, RF2, RF3, RF4, RF6 |
| ***Código de Referencia*** | CUED01 |

***Curso Normal de Eventos ENVIAR DATOS:***

|  |  |
| --- | --- |
| **Actor: SM / Gateway** |  |
| 1.- Este caso de uso comienza cuando el SM / Gateway tiene información por enviar. |  |
| 2.- Crea un mensaje que contiene campo tipo y la información. |  |
| 4.- Envía el mensaje al módulo inferior. |  |
| 5.- Desplegar status del mensaje. |  |
| 6.- Se continúa pasando el mensaje a los módulos inferiores y se transmite por el medio inalámbrico hasta un dispositivo cercano. |  |
| 7.- Preparar temporizador para posteriormente enviar la nueva data recopilada. |  |

***Curso Alternativo de Eventos ENVIAR DATOS:***

|  |  |
| --- | --- |
| **Actor: SM / Gateway** |  |
| 2.1.- Dispositivo falla. |  |
| 2.2.- Reparar dispositivo. |  |
| 2.3.- Incluir a la red. |  |
| 2.1.- Dispositivo detecta algún error. |  |
| 2.2.- Despliega mensaje de error. |  |
| 2.3.- Reparar dispositivo. (¿?) |  |

|  |  |
| --- | --- |
| ***Caso de Uso*** | Retransmitir Datos (Forwarding/Routing) |
| ***Actores*** | Smart Meter (SM) / Sink (Gateway) / Repeater |
| ***Propósito*** | Encaminar los datos de SM vecinos hacia el destino. |
| ***Precondición*** | Calcular y almacenar la ruta hacia todos los nodos de la red. Recibir los paquetes de datos en un formato establecido. |
| ***Resumen (Descripción)*** | Este caso de uso comienza cuando el SM / Sink / Repeater recibe un paquete y éste forma parte de la ruta hacia el destino y debe retransmitir el paquete hasta otro SM vecino. |
| ***Tipo*** | Primario |
| ***Referencias Cruzadas*** | RF4, RF5, RNF1, RNF2, RNF3, RNF4 |
| ***Código de referencia*** | CURD01 |

***Curso Normal de Eventos RETRANSMITIR DATOS:***

LOOP (Implementación CSMA – MAC Layer)

|  |  |
| --- | --- |
| **Actor A: tipo: SM / Gateway / Repeater** | **Actor B: tipo SM / Gateway / Repeater** |
| 1.- Este caso de uso comienza cuando  recibe un paquete de un dispositivo vecino. |  |
| 3.- Detecta que él forma parte de la ruta, y debe prepararse para retransmitir. |  |
| 2.- Envía un mensaje ACK. |  |
|  | 3.- Deja de reenviar el mismo paquete. |
| 4.- Envía el paquete a la capa superior (Network Layer). |  |
| 5.- Revisa en la tabla de ruta, quién de sus nodos vecinos forma parte de la ruta. |  |
| 6.- Actualiza el paquete indicando como destino a algún nodo vecino. |  |
| 7.- Envía el mensaje a la capa inferior (MAC Layer). |  |
| 8.- Prepara el paquete enviando mensajes de control. |  |
|  | 9.- Dispositivo vecino responde mensajes de control. |
| 10.- Envía el mensaje al medio. (Physical Layer) |  |
|  | 11. Envía mensaje ACK. |
| 12.- Recibe mensaje ACK. |  |
| 13.- Permanece en estado IDLE. |  |

***Curso Alternativo de Eventos RETRANSMITIR DATOS:***

|  |  |
| --- | --- |
| **Actor: SM / Gateway / Repeater** | **Actor: SM / Gateway / Repeater** |
|  | 2.1.- Reenvía el paquete {FrameRetries < N} |
| 2.2.- Paquete no es destinado a él para retransmitir y lo elimina. |  |
|  | 2.1.- Reenvía el paquete {FrameRetries < N} |
| 2.2- Encolar paquete si ya se está procesando otro. |  |
| 2.3.- Procesar el otro paquete. |  |
| 2.4.- Procesar el paquete encolado. |  |
|  | 2.1.- Reenvía el paquete {FrameRetries < N} |
| 2.2.- No hay respuesta. |  |
|  | 2.1.- Reenvía el paquete {FrameRetries < N} |
| 2.1.- Paquete es una réplica de otro anterior. |  |
| 2.2.- Eliminar el paquete. |  |
| 2.3.- Actualiza estadísticas de mensaje (duplicados, recibidos, enviados, etc) |  |
|  | 2.1.- Reenvía último paquete. |
|  | 2.2.- Envia a capa superior mensaje error. |
|  | 2.3.- Actualiza estadísticas de mensaje (duplicados, recibidos, enviados, etc) |

|  |  |
| --- | --- |
| ***Caso de Uso*** | Procesar Datos |
| ***Actores*** | Smart Meter (SM) / Sink (Gateway) |
| ***Propósito*** | Recibir la información destinada al nodo y tratarla según lo que se requiere. |
| ***Precondición*** |  |
| ***Resumen (Descripción)*** | Este caso de uso comienza cuando el SM / Sink recibe un paquete (de control o de datos), independiente si es destinado a él o no. Decide qué hacer con el paquete recibido (retransmitir, eliminar, encolarlo o guardarlo) y generar estadísticas y métricas relevantes a la red. |
| ***Tipo*** | Esencial |
| ***Referencias Cruzadas*** | RNF5. |
| ***Código de referencia*** | CUPD01 |

***Curso Normal de Eventos PROCESAR DATOS:***

|  |  |
| --- | --- |
| **SM / Gateway** |  |
| 1.- Este caso de uso comienza cuando el dispositivo recibe un paquete destinado a él |  |
| 2.- Para cada módulo actualiza estadísticas de mensajes (recibidos, transmitidos). |  |
| 3.- Envía el mensaje a módulos superiores |  |

|  |  |
| --- | --- |
| ***Caso de Uso*** | Asegurar Datos (Etapa Intercambio claves Públicas) |
| ***Actores*** | Smart Meter (SM) / Sink (Gateway) |
| ***Propósito*** | Transmitir e intercambiar la llave pública entre SM y Gateway con el fin de autenticar en el proceso de envío de datos. |
| ***Precondición*** | Finalizar el proceso de creación de tabla de enrutamiento. Calcular mediante un algorítmo las llaves pública y privada con un tamaño fijo. |
| ***Resumen (Descripción)*** | Este caso de uso comienza cuando el SM/ Gateway recibe mensaje de control para iniciar el intercambio de llave pública. |
| ***Tipo*** | Real (Sujeto a tecnología de entrada) |
| ***Referencias Cruzadas*** | RNF5, RNF6, RNF7 , RNF9 |
| ***Código de referencia*** | CUAD01 |

***Curso Normal de Eventos ASEGURAR DATOS:***

***(etapa de intercambio llaves públicas)***

|  |  |
| --- | --- |
| **SM / Gateway** | **Gateway / SM** |
| 1.- Este caso de uso comienza cuando el dispositivo recibe un paquete de control asociado al fin del proceso de creación de la tabla de enrutamiento. |  |
| 2.- Prepara un mensaje incluyendo la llave pública. |  |
| 3.- Calcula el CRC del mensaje y lo adjunta al paquete. |  |
| 4.- Envía el paquete al destino. |  |
|  | 5.- Recibe el paquete y lo analiza. |
|  | 6.- Obtiene la llave pública. |
|  | 7.- Verifica que el CRC es correcto y almacena clave pública. |
|  | 8.- Envía un *Acknowledgement* (ACK) de respuesta incluyendo la posición geográfica del dispositivo cifrándolo con la llave pública del orígen. |
| 9.- Recibe ACK. |  |
| 10.- Comprueba CRC y almacena la posición geográfica del dispositivo destino. (Primera autenticación) |  |
| 11.- Caso SM: Espera la recepción de clave simétrica.  Caso: Gateway, Continúa enviando clave pública al siguiente dispositivo o comienza con intercambio de clave simétrica. |  |

***Curso Alternativo de Eventos ASEGURAR DATOS:***

***(etapa de intercambio llaves públicas)***

|  |  |
| --- | --- |
| **SM / Gateway** | **Gateway / SM** |
| 4.1- Envía el paquete al destino. |  |
| 4.2.- Durante la transmisión el paquete se pierde por errores de la red. |  |
| 4.3.- Tiempo de espera de ACK acaba. Consulta si fue autenticado (por el ack de posicionamiento). |  |
| 4.4 Reenvía la llave con el paquete al destino. |  |
|  | 7.1.- CRC es incorrecto. |
|  | 7.2.- No almacena clave pública (posibilidad de estar alterada). No envía ACK y continúa esperando la clave. |
| 7.3.- Tiempo de espera de ACK acaba. Consulta si fue autenticado (por el ack de posicionamiento). |  |
| 7.3.- Reenvía la llave con el paquete al destino. |  |
|  |  |

|  |  |
| --- | --- |
| ***Caso de Uso*** | Asegurar Datos (Etapa Intercambio claves Simétricas) |
| ***Actores*** | Sink (Gateway) / Smart Meter (SM) |
| ***Propósito*** | Revocar las llaves simétricas si lo hubiera.  Enviar nueva llave simétrica a los SM con el fin de autenticar en el proceso de envío de datos. |
| ***Precondición*** | Finalizar el proceso de intercambio de datos o de llave pública. |
| ***Resumen (Descripción)*** | Este caso de uso comienza cuando el Gateway finaliza su etapa de intercambio de datos o clave pública y debe enviar la nueva clave simétrica al destino. |
| ***Tipo*** | Real (Sujeto a tecnología de entrada) |
| ***Referencias Cruzadas*** | RNF5, RNF6, RNF7 , RNF9 |
| ***Código de referencia*** | CUAD02 |

***Curso Normal de Eventos ASEGURAR DATOS:***

***(etapa de intercambio llaves simétricas):***

|  |  |
| --- | --- |
| **Gateway** | **SM** |
| 1.- Este caso de uso comienza cuando el dispositivo recibe un paquete de control asociado al fin del proceso de envío de datos o de clave pública. |  |
| 2.- Envía un mensaje de control a módulo aplicación para detener el envío de datos. |  |
| 3.- Invalida clave simétrica de un SM en particular y crea una nueva. |  |
| 4.- Prepara un mensaje para invalidar clave simétrica para ese SM. |  |
| 5.- Envía el mensaje de revocación al destino. |  |
|  | 6.- Recibe el paquete y lo analiza. |
|  | 7.- Elimina la clave simétrica almacenada. |
|  | 8.- Envía ACK en respuesta de la revocación de la clave. |
| 9.- Recibe ACK. |  |
| 10.- Envía clave simétrica a destino. |  |
|  | 11.- Recibe el paquete y lo analiza. |
|  | 12.- Verifica CRC es correcto y almacena la nueva clave simétrica. |
|  | 13.- Envía un *Acknowledgement* (ACK) de respuesta incluyendo la posición geográfica del dispositivo cifrándolo con la nueva llave simétrica, incluyendo el cifrado su clave privada de la posición resumida con el HMAC. |
|  | 14.- Envía mensaje de control a módulo aplicación para comenzar a enviar datos. |
| 15.- Recibe ACK y verifica CRC si está correcto. |  |
| 16.- Verifica HMAC descifrándolo con la clave pública del destino. |  |
| 17.- Compara la posición geográfica del dispositivo destino con el almacenado. |  |
| 18.- Envía mensaje de control a módulo aplicación para comenzar a enviar datos. |  |

***Curso Alternativo de Eventos ASEGURAR DATOS:***

***(etapa de intercambio llaves simétricas)***

|  |  |
| --- | --- |
| **SM / Gateway** |  |
| 5.1.- Envía el paquete de revocación al destino. |  |
| 5.2.- Tiempo de espera del ACK asociado finaliza. |  |
| 5.3.- Reenvía paquete con la misma llave. |  |
|  | 11.1.- Recibe paquete y lo analiza. |
|  | 11.2.- CRC es incorrecto. No envía ACK. |
|  | 7.2.- No almacena clave simétrica (posibilidad de estar alterada). No envía ACK y continúa esperando clave. |
| 7.3.- Tiempo de espera de ACK acaba. Consulta si fue autenticado (por el ack de posicionamiento). |  |
| 7.3.- Reenvía paquete con la misma llave. |  |
| 16.1.- Autenticación falló, reinicia el proceso con el mismo dispositivo y una llave nueva. |  |

|  |  |
| --- | --- |
| ***Caso de Uso*** | Asegurar Datos (Etapa Intercambio de datos) |
| ***Actores*** | Smart Meter (SM) / Sink (Gateway) |
| ***Propósito*** | Establecer mecanismos de seguridad a los datos recibidos para su envío. |
| ***Precondición*** | Caso SM: Debe estar autenticado luego de recibir la llave simétrica.  Caso Gateway: Recibir ACK con posicionamiento y autenticar nodo destino. |
| ***Resumen (Descripción)*** | Este caso de uso comienza cuando el SM/ Gateway es autenticado/autentica y debe enviar datos del dispositivos con mecanismos de seguridad. |
| ***Tipo*** | Real (Sujeto a tecnología de entrada) |
| ***Referencias Cruzadas*** | RNF5, RNF6, RNF7, RNF8 , RNF9 |
| ***Código de referencia*** | CUAD03 |

***Curso Normal de Eventos ASEGURAR DATOS (etapa intercambio de datos):***

|  |  |
| --- | --- |
| **SM / Gateway** | **Gateway / SM** |
| 1.- Este caso de uso comienza cuando el SM/ Gateway es autenticado/autentica un SM. |  |
| 2.- Recibe un mensaje del módulo aplicación. |  |
| 3.- Fragmenta el mensaje en tamaños y los almacena (????) |  |
| 4.- Selecciona un fragmento y calcula su CRC. |  |
| 5.- Ejecuta el algoritmo de cifrado en los datos. |  |
| 6.- Prepara el mensaje y lo envía al destino. |  |
|  | 7.- Recibe el mensaje fragmentado desde el módulo inferior y lo almacena. |
|  | 8.- Verifica que los fragmentos están completos. |
|  | 9.- Ejecuta el algoritmo de decifrado a los fragmentos y los acumula. |
|  | 10.- Calcula el CRC del mensaje completo. |
|  | 11.- Calcula la MAC del mensaje completo. |
|  | 12.- Comprueba que el CRC del mensaje recibido es igual al del adjunto en el paquete. |
|  | 13.- Comprueba que la MAC del mensaje recibido es igual al del adjunto en el paquete y lo envía al módulo aplicación. |

***Curso Alternativo de Eventos ASEGURAR DATOS (etapa intercambio de datos):***

|  |  |
| --- | --- |
| **SM / Gateway** |  |
| 6.1.- Determina que no ha sido autenticado (origen o destino). |  |
| 6.2.- Elimina o desecha el mensaje y espera su autenticación. |  |
|  | 8.1.- Determina que hay fragmentos incompletos y desecha el mensaje. |
|  | 12.1.- Los CRC no son iguales y desecha el mensaje (posibilidad de mensajes con errores). |
|  | 13.1.- Las MAC no son iguales y desecha el mensaje (posibilidad de mensajes no íntegros). |