generating a counter frame using the counter CT_{c1} and the CAN identity id_{c1};

broadcasting the counter frame on the CAN such that when each module on the CAN receives the counter frame, each module is configured to:

synchronize the counter in the module using the received counter frame.

21. The system according to claim 19 wherein the gateway module is configured to periodically broadcast the nonces at the broadcast module and the receiver module by:

generating the nonce *N*;

generating a nonce frame using the nonce *N*;

broadcasting the nonce frame on the CAN such that when each module on the CAN receives the nonce frame, each module is configured to:

validate and store the nonce in the module using the received nonce frame.

22. The system according to any one of claims 6, 9, 12, 15 and 19 wherein the obtaining the CAN identity key k_{c1} comprises the receiver module being configured to:

retrieve the CAN identity key k_{c1} that is preloaded into the receiver module by the key management module.

23. The system according to any one of claims 6, 9, 12, 15 and 19 wherein the obtaining the CAN identity key k_{c1} comprises the receiver module being configured to:

compute the CAN identity key k_{c1} using the CAN identity id_{c1} and a key of an ascendant node, wherein the key of the ascendant node is preloaded into the receiver module by the key management module.

24. A method for generating a hierarchical tree structure for Controller Area Network (CAN) identities in a CAN network, the method using a key management module provided in a vehicle comprising:

organizing CAN identities of the CAN into sub-sets based on functionalities of the CAN identities, wherein each sub-set is arranged as a tree structure having a root node which could represent a function of the sub-set;

arranging the sub-sets of CAN identities into a tree structure having a root node N_R, wherein the root nodes of the sub-sets are arranged as descendant nodes of root node N_R; and

setting a key for the root node N_R and computing keys for each node in each level in the tree structure, starting from child nodes of the root node N_R, wherein a key of a

child node in the tree structure is computed using a key of a parent node and an identifier identifying the child node.

25. The method according to claim 24 wherein the computing the keys for each node in each level in the tree structure comprises:
for each child node in the tree structure,
computing a key k_c for the child node in the tree structure using a key generating function (KGF( )), a key of a parent node of the child node k_p and an identifier identifying the child node id_c, the key k_c being defined as $k_c = KGF(k_p, id_c)$.

26. The method according to claim 24 or 25 wherein before the setting the key for the root node N_R, the method comprises the step of:
selectively inserting at least one intermediate node between the root node N_R and a root node of one of the sub-sets such that the intermediate node represents an ascendant node of the root node of one of the sub-sets.