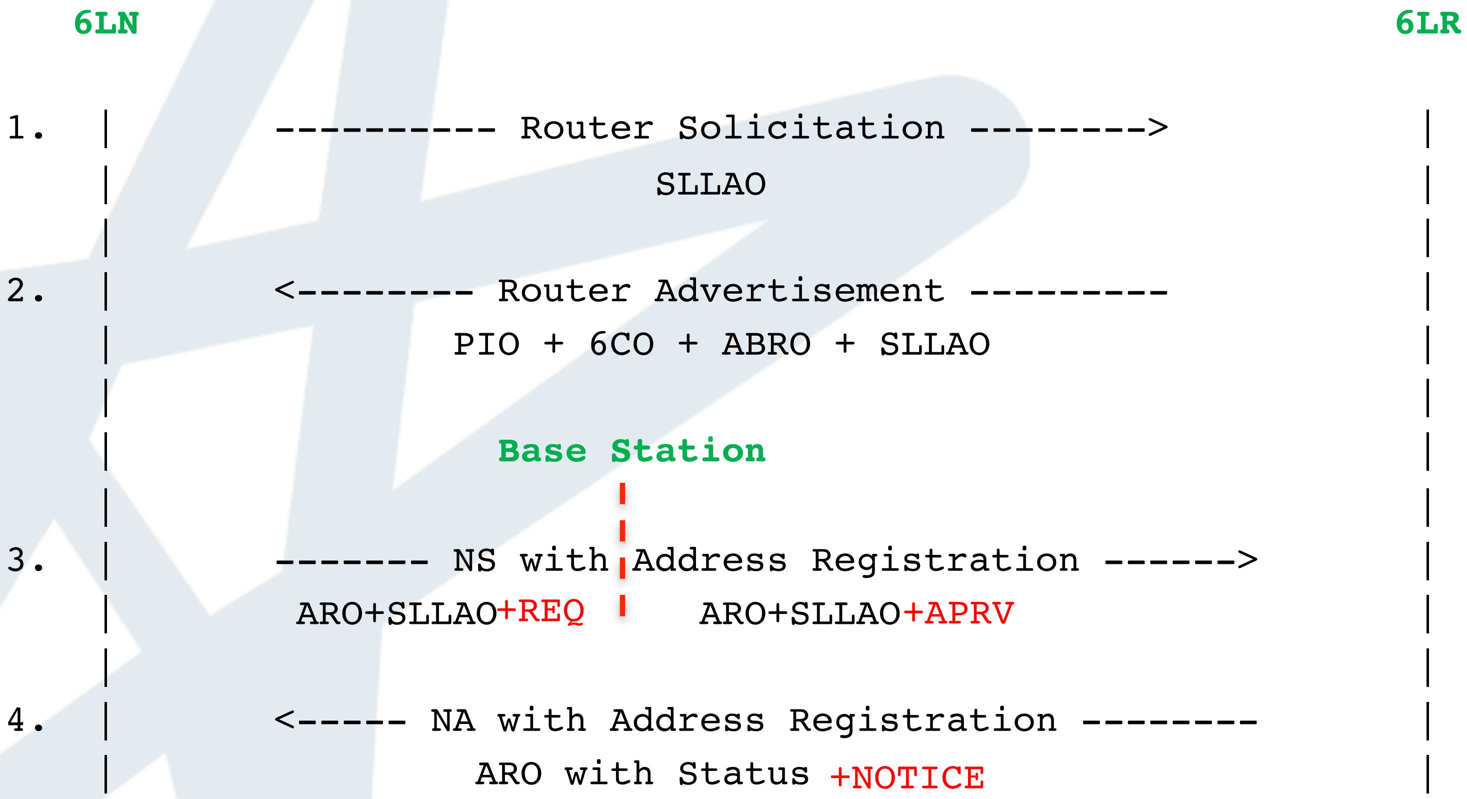
Lightweight Key Establishment & Management Protocol (KEMP) in Dynamic Sensor Networks

Update

draft-qiu-roll-kemp-01

Ying QIU, Jianying ZHOU, Feng BAO

1. ND Messages



```
   6LN                                                          6LR

1. |       ---------- Router Solicitation -------->              |
   |                        SLLAO                                |
   |                                                             |
2. |       <--------- Router Advertisement ---------             |
   |                PIO + 6CO + ABRO + SLLAO                     |
   |                                                             |
   |                  Base Station                               |
   |                                                             |
3. |       ------- NS with Address Registration ------>          |
   |        ARO+SLLAO+REQ         ARO+SLLAO+APRV                 |
   |                                                             |
4. |       <----- NA with Address Registration --------          |
   |              ARO with Status +NOTICE                        |
```

1. ND Message -- Format

Neighbor Solicitation / Advertisement Message Format

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |     Code      |          Checksum             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| | | |                     Reserved                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                       Target Address                          +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
~                                                               ~
~                                                               ~
~                                                               ~
~                    (Destination Address)                      ~
~                                                               ~
~                                                               ~
~                                                               ~
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Options ...
+-+-+-+-+-+-+-+-+-+-+-+-
```

req = {*src*=*ID*, *Dst*= *BS*, *RT* || R_0 || *MAC*(K_{BN}, *ID* || *RT* || R_0) }

aprv = {*src*=*BS*, *dst*=*RT*, *E* (K_{BT}, *ID* || R_0 || R_1 || K_{NR})}

notice = {*src*=*RT*, *Dst*=*ID*, R_0 || R_1 || *MAC*(K_{NR}, *RT* || *ID* || R_0 || R_1)}

2. Multiple Trust Domains

- Request from Rene Struik and Shoichi Sakane

1) If these multiple domains are managed by one base station (key centre), each node address should include the prefix of the domain. With the prefix, a base station / key centre could distinguish each node and avoid any confliction.
2) If these multiple domains have their own base station and the sensor node know its destination base station, extend the node's cache table to store the secret between node and these base stations.
3) If the sensor node cannot decide which base station is its destination, let the req message carry a set of all of MACs with generated by the secret between the node and the basestaion, respectively.

3. Node Bootstraps

- Request from Shoichi how to establish the secure session between N and RT_first when the node bootstraps.

- After bootstrapping, the sensor node N sends its first request to Base station via RT_first (i.e. Redirect Message Format defined in sec 4.5, RFC4861) as below:

  REQ = {Src=SN, Dst= BS, RT_first||R0||MAC(K_BN, SN||RT_first||R0)}

- Hence, the BS will return APPV message to RT_first. Upon receiving the notice from RT_first, the sensor node could establish the secure session with RT_first by normal processing.

4. Other Comments

- Comments from Matt , Greg and Shoichi

1) Section 2 should be expanded: describe what types of devices are in the network (sensors, routers, basesstations), what their capabilities are in terms of communication and computation, if they are mobile, etc.. Adding some details from RFC 4919 might be appropriate.
2) In the introduction or Section 2 it might help to describe some typical attacks that this proposal is trying to prevent, and maybe describe some of the adversary's capabilities.
3) Two nodes must be in range of router or basestation to establish a key. Using public key-techniques this limitation is not present.
   - Do we need to consider this scenario in sensor networking? IMHO, the job of a sensor is to collect the information and send to base station to analysis and process, or performs the commands from the base station. The capability of communicating directly between any two nodes (neighbour or long distance) should be the scope of mobile networks. Any comments?
4) On management of the table of shared keys: the draft suggests that the oldest key in the table should be expunged if additional space is required. This is undesirable: instead an LRU (least recently used) type of algorithm should be used (or other page replacement algorithm which gives better performance given the access patterns of this application). Such an algorithm will require a small amount of overhead, but this cost will be offset by a reduced number of key agreements.
5) In the notice message, is it really necessary for R0 to be sent back to the node? The node already knows this value, and it must be used to check the MAC.
   - the R0 cannot be ignored because the sensor node might send out many request messages with various R0 if it cannot receive the notice message in time. Hence, the sensor node must know which R0 is used in the notice message.

4. Other Comments (cont)

- Comments from Matt , Greg and Shoichi

6) Should give some possible choices for the encryption and MAC algorithms used in the protocol, and what properties they should have. For example, in the appv message encryption is used, but I think it should be authenticated encryption. The primitives in Suite E (http://tools.ietf.org/html/draft-campagna-suitee-00) would probably be suitable.

7) No guidance is given on key management issues. How do new sensors establish shared keys with all routers and base stations? What about adding new routers, how do all existing sensors get re-keyed?

8) The document gives no recommendations for parameter sizes / message encoding format.

9) What is the identifier of each node and how to provision each identifier into each node.

   – the IDs of nodes should be assigned (auto/manual) before deployment.

10) How does Node know the address of Basestation.

   – Node should carry one or more addresses of the trust base stations before deployment.

Future Works

- Define the transmission format.
- Feedback and improve.

Thanks

Q & A