L-037

S3F: Secure Sensor Sharing in NerveNet

李　睿棟†　　　井上　真杉†
Ruidong Li　　　Masugi Inoue

1． Introduction

We are working on the wireless regional network for New Generation Network (NWGN) in the AKARI project [3]. The proposed NerveNet [1，2] is a prospective future platform to provide services to local residents. In NerveNet, managed mesh network provides functions for packet transmission, sensor networks (SNs) work as nerve cells to sense environment and databases are utilized for information dissemination. We investigate the sensor information collection in NerverNet.

We are considering a novel sensor sharing scenario, which has not been considered before. Currently, sensors sense environment, and sensor data is collected and stored in servers and then shared with users, such as Live E! [5]. In contrast, in our scenario, individuals directly collect sensor data from sensors and then transfer the collected data to their selected databases. This scenario is motivated by the needs of privacy. In the current style of sensor data collection and usage, the individuals have no controllability on their private data, such as location, photo. They do not know when and where their individual information is collected and who will use this collected information.

To solve this problem, we propose the novel style of sensor usage in NerveNet. In our scenario, we call these individuals, who directly interact with sensors, as sensor network users (SNUs). The deployed SNs connect to communication platform through SNUs or sensor gateway (SGW). The individual related information will only collected by users themselves. They decide whether collecting information from the sensors around them or not and decide where these collected information will be stored. Thus, in our scenario, SNUs need securely collect information from the sensors deployed and managed by various sensor network owners (SNOs), which is called sensor sharing problem.

To share the sensors securely with various SNUs, the ID-oriented attacks including impersonation attack, fake-ID attack, sybil attack should be inhibited. That is, in NerveNet scenario, adversaries can impersonate the legal sensors to provide false information to SNU. On the other hand, they can also act as a legal SNU to acquire information from sensors.

In the traditional researches on the security of SNs, their motivations are mostly on preventing the attacks on different layers of sensor networks including physical layer, link layer, routing layer, and application layer [4]. Meanwhile, most of them considered the same assumptions of SN, where one SN, one gateway and one remote task manager exist. Both focus point and assumptions are completely different from our scenario.

To solve this problem, we propose a secure sensor sharing framework (S3F) to enable SNUs interact with sensors deployed by different SNOs directly and securely. In the proposed S3F, there is a shared key between each sensor and its corresponding SNO, and when one SNU wants to collect information from one sensor, she will get one-time assertion authorization from SNO and then acquire information from the sensor.

2． System Descriptions and Security Requirements

The entities in the interactions in S3F include previously mentioned SNO, SNU, and another entity, which is called NerveNetP (NerveNet Provider). The NerveNetP denotes the entity that operates and manages NerveNet.

Consider sensor sharing scenario in Fig. 1. In one NerveNet, there are many BSs for forming managed mesh network for transmission of data, and many CSGs (Community Service Gateways), which serves as application server and databases. In a NerveNet, NerveNetP operates the managed mesh network and some public CSGs. At the edge of NerveNet, there are SNs, which are deployed and managed by different SNOs. They connect to NerveNet platform through SNUs or SGWs. Take SNU as an example in Fig. 1. SNU is a mobile terminal, who collects information from sensor$_1$ and transfers the information to its private CSG$_1$ securely when it is located in SN$_1$. In the whole system, secure communication among the entities of SNU, CSG, BS can be assured [2], but SNs are the security weak point, since the sensors owned by different SNOs cannot be well protected.

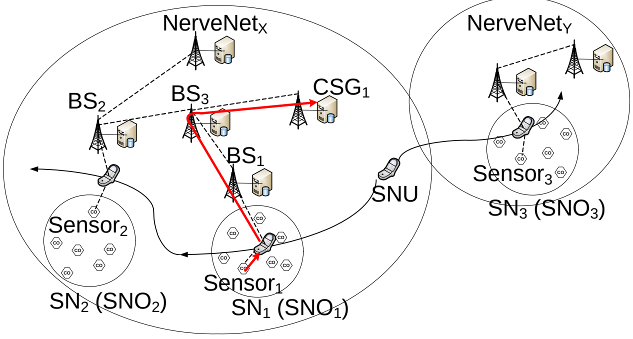

Fig. 1 Sensor Sharing Scenario

We also use Fig. 1 to illustrate secure sensor sharing scenario. In Fig. 1, there are two regional networks, NerveNet$_X$ and NerveNet$_Y$ and the arrow line is the moving route for SNU. SNU registered in NerveNet$_X$, which is the home NerveNet. NerveNet$_Y$ is the foreign NerveNet for this SNU. When SNU moves around, she travels through several SNs, for example, SN$_1$, SN$_2$, SN$_3$. These SNs belong to different SNOs, SNO$_1$, SNO$_2$, and SNO$_3$. Meanwhile, SN$_1$ and SN$_2$ locate in the area of NerveNet$_X$, and SN$_3$ locates in the area of NerveNet$_Y$. When SNU exists in these SNs, she wants to collect her individual related information from these sensors. For example, SNU wants to connect information directly from sensor$_1$ from SN$_1$, sensor$_2$ from SN$_2$ and sensor$_3$ from SN$_3$. Thus, before accessing these sensors, SNU need to obtain the permission from their owners, SNO$_1$, SNO$_2$, and SNO$_3$, respectively. This is basic scenario for sensor sharing, which will be a foundation for future network.

To inhibit ID-oriented attacks in sensor sharing scenario, we identify the security requirements for S3F as follows.

S1. Assertion Integrity: We use assertion to specify the authorization content from SNO. For example, this SNU is authorized to access the sensor during 2010.7.8 AM11:00-PM1:00 for location information. S1 is just to guarantee the assertion authorization to be unable to be modified by the intermediate entities, such as SNU and immediate forwarding sensors.

S2. Sensor Ownership Authentication: It is to assure that sensors' ownership can be proved to be the one as claimed. This property can ensure prevention of ID-oriented attacks to sensors.

S3. SNU Identity Authentication: It is to guarantee the interacting sensor that SNU's identity is the one as claimed by her. This property ensures the prevention of faked SNU ID attack.

† New Generation Network Research Center, National Institute of Information and Communications Technology (NICT)

3. Notations

We use the following notations in the proposed S3F:
N_A: Nonce generated by A.
$K_{A\text{-}B}$: The symmetric key shared by entity A and entity B
$\{M\}_K$: The encryption of message M using key K.
H(M): The hash of message M

4. Proposed Secure Sensor Sharing Framework (S3F)

The proposed S3F will be elaborated in this section. To describe S3F clearly, we utilize the general secure sensor sharing scenario as in Fig. 1 and add the servers for SNO_1, NerveNetP, and SNO_3 in this scenario. $Sensor_1$, SNO_1, and $NerveNetP_x$ represent typical entities in home NerveNet. $Sensor_3$ and SNO_3 denote typical entities in foreign NerveNet. These entities are utilized to express that SNU directly collects information from sensors in home NerveNet and foreign NerveNet, repectively.

The whole view of the proposed S3F is provided as in Fig. 2, which illustrates the interactions among SNO, NerveNetP, and sensors. When SNU wants to collect information from $sensor_1$, she will request to SNO_1 for the service. SNO_1 will authenticate the identity of SNU through $NerveNetP_X$, then it provides the assertion authorization to SNU after correct authentication. Similar procedure will be also performed when desiring to collect information from $sensor_3$. The difference between them is the authentication of SNU's identity. When travelling around the $NerveNet_Y$, the authentication of SNU needs to be performed with assistance of $NerveNetP_X$.

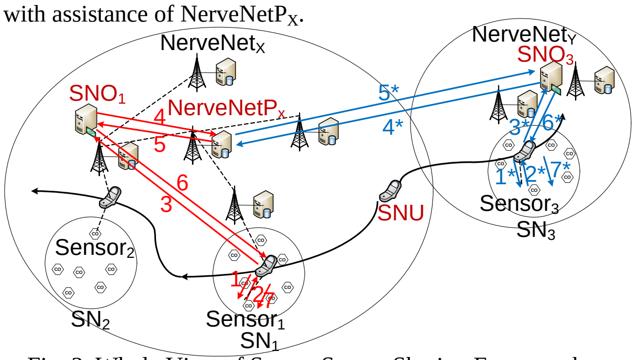

Fig. 2. Whole View of Secure Sensor Sharing Framework

We assume there is a symmetric key pair between SNO and each sensor she deployed and managed. From Fig. 2, we can see there are 7 steps need to acquire information from sensors. We use number k to represent each step necessary in home NerveNet, and k* to denote the steps necessary to access sensors in a foreign NerveNet. Actually, for both cases, step 1, 2, 3, 6, 7 is the same, only step 4 and 5 are different, which are related to the authentication of identity of SNU. The descriptions for steps have been provided as follows.

1=1* Request for Information (RfI)
2=2* Reply with SNO
3=3* Request for Service (RfS) to the SNO
4. SNO request $NerveNetP_X$ to authenticate the identity of SNU
4*. SNO request Home NerveNetP to authenticate the identity of SNU
5. $NerveNetP_X$ successfully authenticates SNU
5* Home NerveNetP authenticate successfully of SNU
6=6*. Reply with the assertion authorization to SNU
7=7*. Security interactions and collect information

The detailed message flows (MFs) are provided in Fig. 3. The step 7 is detailedly described using three MFs. Take MFs for information acquisition from $sensor_1$ in $NerveNet_X$ as example. Similar process can be obtained for access sensors in $NerveNet_Y$.

The crucial message flows are provided as follows.

MF1: $SNO_1 \rightarrow SNU: \{Assertion, SK1, H(Assertion, SK1)\}_{KSensor1-SNO1}, SK1$

MF2: $SNU \rightarrow Sensor_1: \{Assertion, SK1, H(Assertion, SK1)\}_{KSensor1-SNO1}, N_{SNU}$

MF3: $Sensor_1 \rightarrow SNU: \{N_{SNU}\}_{SK1}, N_{Sensor1}$

MF4: $SNU \rightarrow Sensor_1: \{N_{Sensor1}\}_{SK1}$

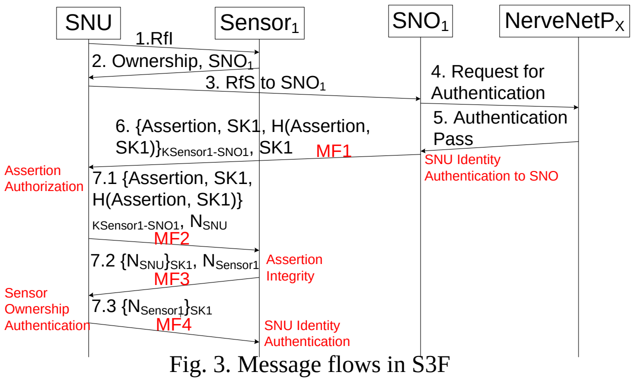
SNU
Sensor1
SNO1
NerveNetPX
1.RfI
2. Ownership, SNO1
3. RfS to SNO1
4. Request for Authentication
5. Authentication Pass
6. {Assertion, SK1, H(Assertion, SK1)}KSensor1-SNO1, SK1
MF1
SNU Identity Authentication to SNO
Assertion Authorization
7.1 {Assertion, SK1, H(Assertion, SK1)} KSensor1-SNO1, NSNU
MF2
7.2 {NSNU}SK1, NSensor1
MF3
Assertion Integrity
Sensor Ownership Authentication
7.3 {NSensor1}SK1
MF4
SNU Identity Authentication

Fig. 3. Message flows in S3F

In MF1, SK1 is used to establish session key between SNU and $Sensor_1$ and authenticate the identity of SNU and the corresponding sensor. SK1 is appended after Assertion, which describes the authorized privilege of SNU. H(Assertion, SK1) is used to assure the integrity of assertion. The whole message is encrypted by shared key between SNO_1 and $Sensor_1$. We call $\{Assertion, SK1, H(Assertion, SK1)\}_{KSensor1-SNO1}$ the assertion authorization. SK1 is securely distributed to SNU.

In MF2, SNU sends this assertion authorization appended with a random number N_{SNU} to $Sensor_1$ to see whether the corresponding sensor can decrypt the assertion authorization and encrypt this random number using session key SK1.

In MF3, the corresponding sensor decrypts the assertion authorization using its shared key and get session key SK1 and check the hash value to see whether the assertion has been modified or not. Then it sends the N_{SNU} encrypted by SK1 appended with a random number generated by itself, $N_{Sensor1}$, to SNU to see whether SNU know the SK1.

In MF4, SNU gets the correct encrypted N_{SNU} from the corresponding sensor, and thus the ownership of this sensor has been assured. Also SNU sends the $N_{Sensor1}$ encrypted with SK1 to the sensor, the sensor can know the identity of SNU is authentic.

5. Conclusions

In the paper, we identified the importance of a novel scenario, sensor sharing scenario in NerveNet, and the security requirements for it. We proposed a S3F to achieve these requirements. Under S3F, the identity of SNU is assured by NerveNetP, the ownership of sensor is guaranteed by the shared key between SNO and sensor, and the assertion integrity is ensured by the hash of assertion.

References

[1] M. Inoue, et al., "Sensor-Terminal-Network Cooperative Architecture for Context-Aware Services," IEEE WCNC 2010, Sydney, Australia, Apr. 18-21, 2010.
[2] M. Inoue, et al., "A Future Access Network Architecture for Providing Personalized Context-Aware Services with Sensors," AccessNets 2009, Hong Kong, China, Nov. 1-3, 2009.
[3] Akari Architecture Design Project, http://akari-project.nict.go.jp/
[4] J. Sen, "A Survey on Wireless Sensor Network Security," IJCNIS, vol. 1, no. 2, Aug. 2009.
[5] Live E!, http://www.live-e.org/