ISO/IEC JTC 1 N 9208

2008-07-28

ISO/IEC JTC 1
Information Technology

Document Type:	**Proposed NP**
Document Title:	**SC 6 Proposal for a New Work Item, Security framework for ubiquitous sensor network**
Document Source:	**SC 6 Secretariat**
Reference:	
Document Status:	**This document is circulated to JTC 1 National Bodies for concurrent review. If the JTC 1 Secretariat receives no objections to this proposal by the due date indicated, we will so inform the SC 6 Secretariat.**
Action ID:	**ACT**
Due Date:	**2008-10-28**
No. of Pages:	**31**

Secretariat, ISO/IEC JTC 1, American National Standards Institute, 25 West 43rd Street, New York, NY 10036; Telephone: 1 212 642 4932; Facsimile: 1 212 840 2298; Email: lrajchel@ansi.org

Telecommunications and Information Exchange Between Systems

ISO/IEC JTC 1/SC 6

Document Number:	6N13661
Date:	2008-07-18
Replaces:	
Document Type:	Text for NP ballot
Document Title:	Text for NP ballot, Security framework for ubiquitous sensor network
Document Source:	WG 7
Project Number:	
Document Status:	SC 6 NBs are requested to ballot through the ISO e-balloting system (www.iso.org/jtc1/sc6) no later than 2008-10-18.
Action ID:	LB
Due Date:	2008-10-18
No. of Pages:	30

ISO/IEC JTC1/SC6 Secretariat Ms. Jooran Lee, KSA (on behalf of KATS)

Korea Technology Center #701-7 Yeoksam-dong, Gangnam-gu, Seoul, 135-513, Republic of Korea ;

Telephone: +82 2 6009 4808 ; Facsimile: +82 2 6009 4819 ; Email : jooran@kisi.or.kr

PROPOSAL FOR A NEW WORK ITEM

Date of presentation of proposal: 2008-07-18	Proposer: JTC 1/SC 6/WG 7
Secretariat: KATS National Body Korea	**ISO/IEC JTC 1 N** ISO/IEC JTC 1/SC 06 N13661

A proposal for a new work item shall be submitted to the secretariat of the ISO/IEC joint technical committee concerned with a copy to the ISO Central Secretariat.

Presentation of the proposal - to be completed by the proposer. .

Title (subject to be covered and type of standard, e.g. terminology, method of test, performance requirements, etc.) Specification of Data Value Domain

Security framework for ubiquitous sensor network

Scope (and field of application)

This draft Recommendation describes security threats and security requirements to the Ubiquitous Sensor Network. In addition, this draft Recommendation categorizes security technologies by security functions that satisfy above security requirements and by the place to which the security technologies are applied in the security model of the Ubiquitous Sensor Network. Finally, the security function requirements for each entity in the network and possible implementation layer for security function are presented.

Purpose and justification - attach a separate page as annex, if necessary

Recently, sensor network become one of the interesting topics for the emerging applications in the world. Also, JTC 1/SC 6 started new standardization work on sensor network issues to meet market urgent requirements on this new potential area. During the SC 6 meeting in April 2008, which is co-located with ITU-T SG 17, the possible collaboration work on sensor network issues with ITU-T SG 17 had been discussed. The meeting noted that security aspects of sensor network are very important for the future deployment of sensor network applications. Also, it was informed that ITU-T Q.9/17 have been developing draft recommendation on security framework for ubiquitous sensor network. According to the meeting agreements in April 2008, SC 6/WG 7 had decided to propose new project on Security Framework for USN as a common text project with ITU-T SG17.

Currently, draft text of ITU-T X.usnsec-1 is not mature enough at this moment and it is planned for consent in 4Q 2010 by the ITU-T SG 17. For the completion of this draft recommendation, lots of collaborative works are required in the future meeting. It is expected that collaborative work will accelerate the development of this specification and produce a good quality of common text standard for both organization.

Programme of work

If the proposed new work item is approved, which of the following document(s) is (are) expected to be developed?

__X__ a single International Standard

___ more than one International Standard (expected number: .....)

____ a multi-part International Standard consisting of ..... parts

____ an amendment or amendments to the following International Standard(s) .....
____ a technical report , type .....

And which standard development track is recommended for the approved new work item?

_X__a. Default Timeframe

____b. Accelerated Timeframe

____c. Extended Timeframe

Relevant documents to be considered

The current text of ITU-T Draft Recommendation X.usnsec-1: Security Framework of USN, which has been developing by ITU-T Q.9/17, is attached to this document for your consideration. Current text of ITU-T X.usnsec-1 is not completed enough and it needs further collaborative work between ITU-T SG 17 and JTC 1/SC 6.

Co-operation and liaison

ITU-T SG 17

Preparatory work offered with target date(s)

None

Signature: `Jooran Lee, ISO/IEC JTC 1/SC 6 Secretariat`

Will the service of a maintenance agency or registration authority be required? .....No.....
- If yes, have you identified a potential candidate? .....
- If yes, indicate name .....

Are there any known requirements for coding? .....No.....
-If yes, please specify on a separate page

Does the proposed standard concern known patented items? .....No.....
- If yes, please provide full information in an annex

Are there any known requirements for cultural and linguistic adaptability? .....No.....

-If yes, please specify on a separate page

Comments and recommendations of the JTC 1 or SC 6 Secretariat - attach a separate page as an annex, if necessary

Comments with respect to the proposal in general, and recommendations thereon:

It is proposed to assign this new item to JTC 1/SC 6/WG 7

Voting on the proposal - Each P-member of the ISO/IEC joint technical committee has an obligation to vote within the time limits laid down (normally three months after the date of circulation).

Date of circulation:	**Closing date for voting:**	**Signature of Secretary:**
2008-07-18	2008-10-18	Jooran Lee

NEW WORK ITEM PROPOSAL - PROJECT ACCEPTANCE CRITERIA		
Criterion	**Validity**	**Explanation**
A. Business Requirement		

A.1 Market Requirement	Essential ___ Desirable _X__ Supportive ___	
A.2 Regulatory Context	Essential ___ Desirable ___ Supportive ___ Not Relevant _X_	
B. Related Work		
B.1 Completion/Maintenance of current standards	Yes ___ No_X__	
B.2 Commitment to other organisation	Yes _X_ No____	It is proposed as a common text project with ITU-T SG17.
B.3 Other Source of standards	Yes ___ No__X_	
C. Technical Status		
C.1 Mature Technology	Yes ___ No_X__	Even if ITU-T SG 17 has been developed a draft recommendation on USN security framework, it is not completed enough and it needs lots of collaboration.
C.2 Prospective Technology	Yes ___ No_X__	
C.3 Models/Tools	Yes ___ No__X_	
D. Conformity Assessment and Interoperability		
D.1 Conformity Assessment	Yes ___ No__X_	
D.2 Interoperability	Yes ___ No__X_	
E. Adaptability to Culture, Language, Human Functioning and Context of Use		

E.1 Cultural and Linguistic Adaptability	Yes ___ No__X_	
E.2 Adaptability to Human Functioning and Context of Use	Yes ___ No__X_	
F. Other Justification		See attachment for further consideration

Notes to Proforma

A. Business Relevance. That which identifies market place relevance in terms of what problem is being solved and or need being addressed.

A.1 Market Requirement. When submitting a NP, the proposer shall identify the nature of the Market Requirement, assessing the extent to which it is essential, desirable or merely supportive of some other project.

A.2 Technical Regulation. If a Regulatory requirement is deemed to exist - e.g. for an area of public concern e.g. Information Security, Data protection, potentially leading to regulatory/public interest action based on the use of this voluntary international standard - the proposer shall identify this here.

B. Related Work. Aspects of the relationship of this NP to other areas of standardisation work shall be identified in this section.

B.1 Competition/Maintenance. If this NP is concerned with completing or maintaining existing standards, those concerned shall be identified here.

B.2 External Commitment. Groups, bodies, or for external to JTC 1 to which a commitment has been made by JTC for Co-operation and or collaboration on this NP shall be identified here.

B.3 External Std/Specification. If other activities creating standards or specifications in this topic area are known to exist or be planned, and which might be available to JTC 1 as PAS, they shall be identified here.

C. Technical Status. The proposer shall indicate here an assessment of the extent to which the proposed standard is supported by current technology.

C.1 Mature Technology. Indicate here the extent to which the technology is reasonably stable and ripe for standardisation.

C.2 Prospective Technology. If the NP is anticipatory in nature based on expected or forecasted need, this shall be indicated here.

C.3 Models/Tools. If the NP relates to the creation of supportive reference models or tools, this shall be indicated here.

D. Conformity Assessment and Interoperability Any other aspects of background information justifying this NP shall be indicated here.

D.1 Indicate here if Conformity Assessment is relevant to your project. If so, indicate how it is addressed in your project plan.

D.2 Indicate here if Interoperability is relevant to your project. If so, indicate how it is addressed in your project plan

E. **Adaptability to Culture, Language, Human Functioning and Context of Use**

NOTE: The following criteria do not mandate any feature for adaptability to culture, language, human functioning or context of use. The following criteria require that if any features are provided for adapting to culture, language, human functioning or context of use by the new Work Item proposal, then the proposer is required to identify these features.

E.1 Cultural and Linguistic Adaptability. Indicate here if cultural and natural language adaptability is applicable to your project. If so, indicate how it is addressed in your project plan.

ISO/IEC TR 19764 (Guidelines, methodology, and reference criteria for cultural and linguistic adaptability in information technology products) now defines it in a simplified way:

"ability for a product, while keeping its portability and interoperability properties, to:

- be internationalized, that is, be adapted to the special characteristics of natural languages and the commonly accepted rules for their se, or of cultures in a given geographical region;

- take into account the usual needs of any category of users, with the exception of specific needs related to physical constraints"

Examples of characteristics of natural languages are: national characters and associated elements (such as hyphens, dashes, and punctuation marks), writing systems, correct transformation of characters, dates and measures, sorting and searching rules, coding of national entities (such as country and currency codes), presentation of telephone numbers and keyboard layouts. Related terms are localization, jurisdiction and multilingualism.

E.2 Adaptability to Human Functioning and Context of Use. Indicate here whether the proposed standard takes into account diverse human functioning and diverse contexts of use. If so, indicate how it is addressed in your project plan.

NOTE:

1. **Human functioning is defined by the World Health Organization at http://www3.who.int/icf/beginners/bg.pdf as:**
   <<In ICF (*International Classification of Functioning, Disability and Health), the term functioning refers to all body functions, activities and participation.*>>
2. **Content of use is defined in ISO 9241-11:1998 (*Ergonomic requirements for office work with visual display terminals (VDTs) – Part 11: Guidance on usability) as:***
   <<Users, tasks, equipment (hardware, software and materials), and the physical and societal environments in which a product is used.>>
3. **Guidance for Standard Developers to address the needs of older persons and persons with disabilities).**

F. Other Justification Any other aspects of background information justifying this NP shall be indicated here.

<Attachment> ITU-T Draft Recommendation X.usnsec-1

ITU-T Draft Recommendation X.usnsec-1, Security Framework for Ubiquitous Sensor Network

This is a draft text of ITU-T X.usnsec-1, Security Framework for Ubiquitous Sensor Network, developed by ITU-T Q.9/17. This is an output document of ITU-T Q.9/17 Geneva meeting in April 2008.

This document is not stable enough and it is planned for Consent in 4Q 2010 by the ITU-T SG 17. For the completion of this draft recommendation, lots of collaborative works are required in the future meeting.

Summary

This draft Recommendation describes security threats and security requirements to the Ubiquitous Sensor Network. In addition, this draft Recommendation categorizes security technologies by security functions that satisfy above security requirements and by the place to which the security technologies are applied in the security model of the Ubiquitous Sensor Network. Finally, the security function requirements for each entity in the network and possible implementation layer for security function are presented.

Keywords

Security framework for Ubiquitous Sensor Network, Sensor Node Compromise, Secure Data Aggregation, Pair-wise key establishment, Group-wise key, Authenticated Broadcast Data

Content

1 Scope

Recent advancement of wireless based communication technology and electronics makes the low-cost, low power sensor network feasible. Basically USN consists of two parts: sensor network being composed of a large number of sensor nodes and the application server controlling the sensor node in the sensor network or collecting information from the sensor nodes in the sensor network.

USN can be an intelligent information infrastructure of advanced e-Life society which delivers user-oriented information and provides knowledge services to anyone at anywhere and anytime, where the information and knowledge is developed by using context awareness with detecting, storing, processing and integrating situational and environmental information gathered from sensor tags and/or sensor nodes affixed to anything. Since there are many threats in transferring the information in USN, appropriate security mechanisms are needed to protect against those threats in USN.

This draft Recommendation describes security threats and security requirements to the Ubiquitous Sensor Network. In addition, this draft recommendation categorizes security technologies by security functions that satisfy above security requirements and by the place to which the security technologies are applied in the model of the Ubiquitous Sensor Network. Finally, the security function requirements for each entity in the network and possible implementation layer for security function are presented.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is published regularly. A reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.800]	ITU-T Recommendation X.800 (1991), *Security architecture for Open Systems*
[ITU-T X.805]	ITU-T Recommendation X.805 (2003), *Security architecture for systems providing end-to-end communications*
[ITU-T X.1111]	ITU-T Recommendation X.1111 (2007), *Framework for security technologies for home network*

3 Terms and definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 Access Control [ITU-T X.800]: The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.

3.1.2 Authentication [ITU-T X.800]: See Data Origin Authentication and Peer-Entity Authentication.

3.1.3 Authorization [ITU-T X.800]: The granting of rights, which includes the granting of access based on access rights.

3.1.4 **Accessibility [ITU-T X.800]**: The property of being accessible and useable upon demand by an authorized entity.

3.1.5 **Confidentiality [ITU-T X.800]**: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

3.1.6 **Data Origin Authentication [ITU-T X.800]:** The corroboration that the source of data received is as claimed.

3.1.7 **Denial of Service [ITU-T X.800]**: The prevention of authorized access to resources or the delaying of time-critical operations.

3.1.8 **Digital Signature [ITU-T X.800]**: Data appended to, or a cryptographic transformation (see cryptography) of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient.

3.1.9 **Integrity [ITU-T X.800]:** The property that data has not been altered or destroyed in an unauthorized manner.

3.1.10 **Key [ITU-T X.800]**: A sequence of symbols that controls the operations of encipherment and decipherment.

3.1.11 **Key Management [ITU-T X.800]**: The generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy.

3.1.12 **Privacy [ITU-T X.800]**: The right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

3.1.13 **Repudiation [ITU-T X.800]**: Denial by one of the entities involved in a communication of having participated in all or part of the communication.

3.1.14 **Security policy [ITU-T X.800]**: The set of criteria for the provision of security services.

3.1.15 **Threat [ITU-T X.800]**: A potential violation of security

3.2 Terms defined in this Recommendation

This document defines the following terms:

3.2.1 **Bootstrapping:** It refers to a process to establish a secure communication association between the sensor nodes which may have been initialized with key information, enabling the sensor node to communicate with each other sensor node after deployment of sensor nodes. This can be regarded as one of the key management.

3.2.2 **Credentials:** It refers to a set of key related information comprising keys, keying materials and cryptographical algorithm.

3.2.3 **Group-wise key**: It refers to a key which is used to protect a multicast communications among a set of sensor nodes over a shared wireless link.

3.2.4 **Pair-wise key:** It refers to a key which is used to protect an unicast communication between a pair of sensor nodes over a single wireless link.

3.2.5 **Secure data aggregation:** It refers to an in-network process which is performed on the aggregator node to securely transfer the aggregation value to sink node by combining the sensed values sent by a number of sensor nodes. In this scheme, each sensor node sends an encrypted sensed value to the aggregator, then aggregator calculate the encrypted aggregator results by using aggregation functions, such as summing function, average function, median

function, and maximum value or minimum value, the sink node obtains the aggregation value by decrypting the encrypted aggregator results.

3.2.6 Ubiquitous Sensor Network: USN could be an intelligent information infrastructure of advanced e-Life society which delivers user-oriented information and provides knowledge services to anyone at anywhere and anytime. USN is composed of an application server, IP-based core network, a base station, a large number of sensor nodes. Part of USN includes wireless sensor network.

3.2.7 **Wireless sensor network(WSN):** It is composed of a base station and a large number of the sensor nodes with the wireless transmission capability.

4 Abbreviations and acronyms

This contribution uses the following abbreviations:

USN – Ubiquitous Sensor Network

WSN–Wireless Sensor Network

5 Conventions

In this Recommendation:

The keywords "**is required to"** indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords "**is recommended"** indicate a requirement which is recommended but which is not absolutely required. Thus this requirement need not be present to claim conformance.

The keywords "**is prohibited from"** indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords "**can optionally"** indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

6 Security model for USN

Figure 1 describes the major USN's application areas which include home network application, pollution monitoring, fire monitoring, and flood monitoring.

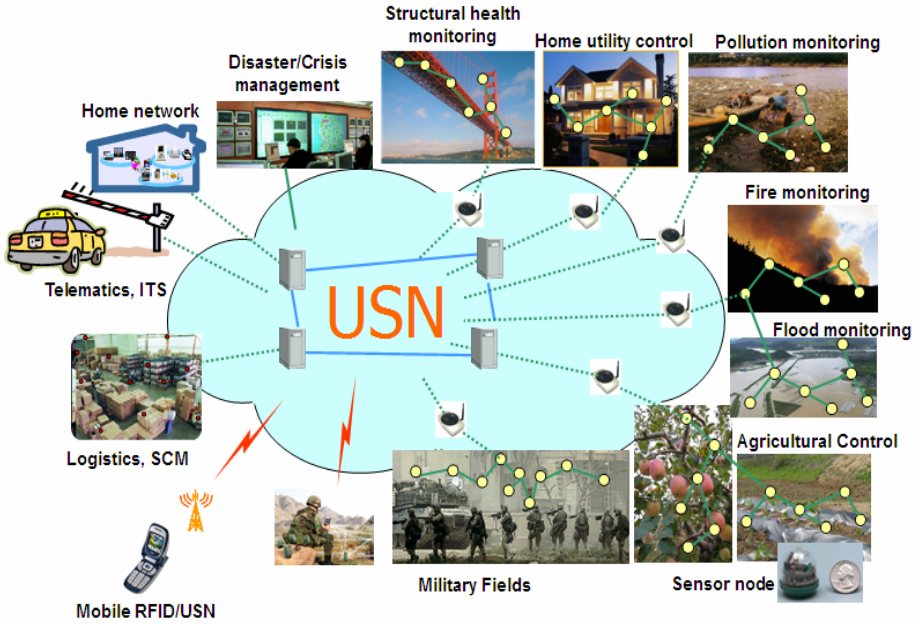

Figure 1 – Application area for USN

Source: ITU NGN-GSI Rapporteur Group Meeting " Draft Recommendation *Y.USN-reqts*, "Requirements for support of USN applications and services in NGN environment," (Geneva, 11-21 September 2007), available at: http://www.itu.int/md/T05-NGN.GSI-DOC-0266/en

The Figure 2 describes the overall structure of USN. Based on this basic structure, the security model should be defined for USN security.

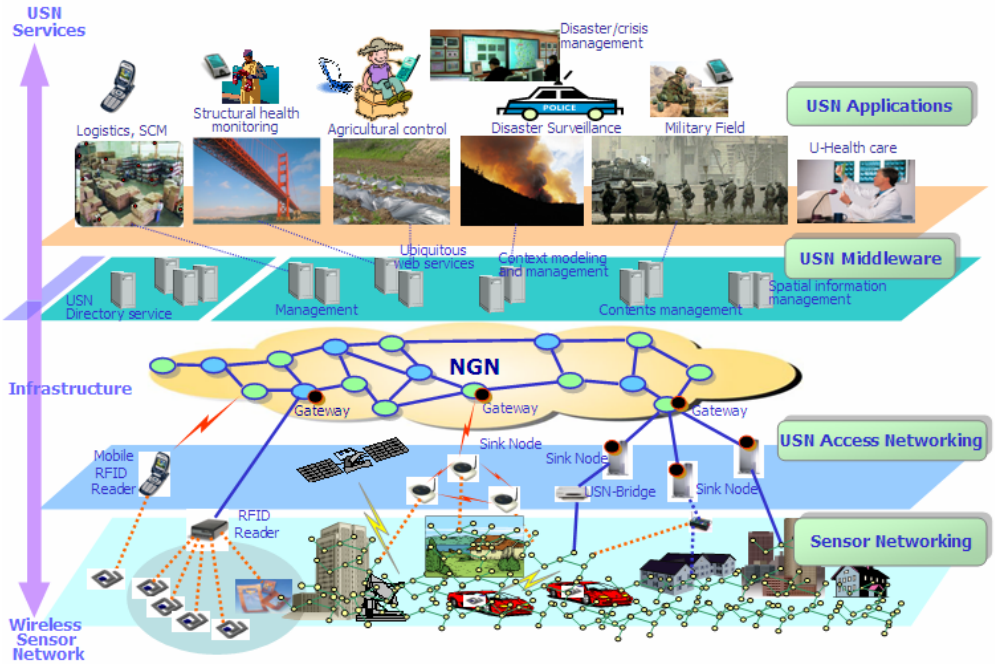

Figure 2 – Overall structure of USN

Source: ITU NGN-GSI Rapporteur Group Meeting " Draft Recommendation *Y.USN-reqts*, "Requirements for support of USN applications and services in NGN environment," (Geneva, 11-21 September 2007), available at: http://www.itu.int/md/T05-NGN.GSI-DOC-0266/en

The sensor networking domain of USN corresponds usually to WSN but includes wire-line sensor networks as well. So, many kinds of wired and wireless networking technologies may be used according to service characteristics and requirements. Here are examples: RS-422, 423, 485, PLC (Power Line Communication), CAN (Controller Area Network), Ethernet, N-RFID, Bluetooth, WLAN, IEEE 802.15.4, etc. where leaf sensor devices may be sensor tags and/or sensor nodes.

Sensor networks are not isolated but connected usually to customer networks via various access networks and core networks as shown in Figure 2. The access networking domain corresponds to many access networking technologies such as xDSL, HFC, PLC, satellite, GPRS, CDMA, GSM, HSDPA, WiBro, etc. The core networks are NGN, Internet, etc. USN might require some extensions and/or additions to core network architectures in order to cover new functional capability requirements extracted from USN applications and services. The USN middleware will be comprised of many software functionalities such as context models and processing, sensory information gathering, data filtering, contents management, Web Services functions, network and software management, sensor profile management, directory services, interworking gateways, etc. Based on all those functions, USN applications and services can be established and provided to customers as well as enterprises, organizations and government.

The security model for USN can be divided into 2 parts: one for IP network and the other for Wireless Sensor network. However, since there is no security model for wireless sensor network studied by ITU-T, this Recommendation intends to develop the security model for WSN as well as IP network.

The communication patterns within our WSN fall into three categories:

- Node to base station communication, e.g. sensor readings.
- Base station to node communication, e.g. specific requests.
- Base station to all nodes, e.g. routing beacons, queries or

We make the following assumptions:

- The base station is computationally robust, having the requisite processor speed, memory and power to support the cryptographic and routing requirements of the sensor network. The base station is part of a trusted computing environment.
- The communication paradigm is either base station to sensor or sensor to base station.

So how such network managements are integrated should be taken into account.

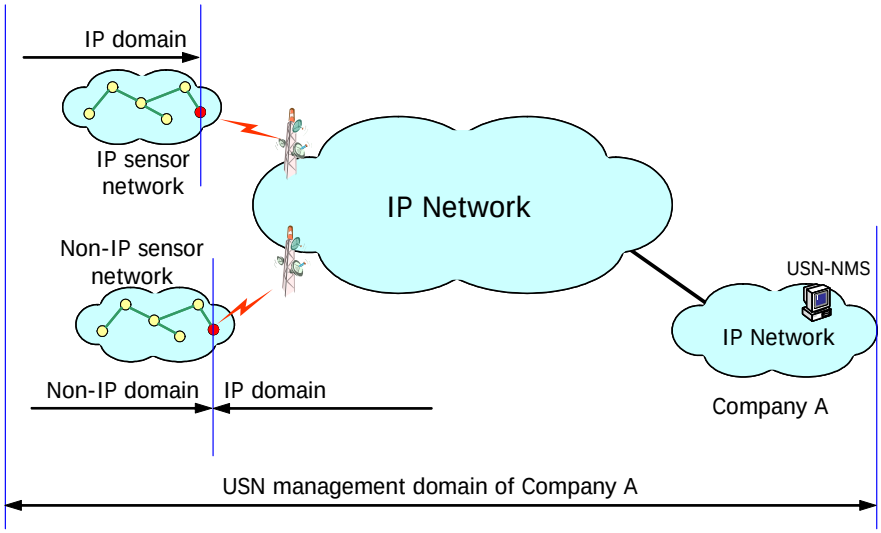

Figure 3 – A USN network configuration

Source: ITU NGN-GSI Rapporteur Group Meeting " Draft Recommendation *Y.USN-reqts*, "Requirements for support of USN applications and services in NGN environment," (Geneva, 11-21 September 2007), available at: http://www.itu.int/md/T05-NGN.GSI-DOC-0266/en

The characteristics of the sensor network are as follows;

- The sensor network consists of a lot of sensor nodes interconnected by wireless medium.
- The sensor nodes are deployed densely in a wide area.
- The sensor nodes are vulnerable to failure.
- The communication from BS to sensor node would be broadcast type or point-to-point type.
- Sensor nod has a limited power, computational capacity, and memory.
- Sensor node may not have a global identification.

There are three components in WSN; application server which communicate with sink node, sink node, called a base station, which interface sensor network and application server, and a collection of sensor nodes using the wireless communication to communicate with each other. The sink may communicate with application server via Internet or Satellite. The Security in IP-based network is very similar to the security in ITU-T X.805. Hence, the Recommendation focuses on the security of the wireless sensor network (WSN) being composed of a set of sensor nodes using wireless transmission.

To communicate information between the sensor nodes, a secure association between each sensor nod needs to be established before the secure communication between them can be carried out. However, the following characteristics of the sensor network make the design of secure communication very difficult;

- **Infeasible to use the public key cryptosystems**: The limited computational power, memory size, and power supply make it very difficult to use the public key cryptosystem, such as Diffie-Hellman key agreement or RSA encryption and signature. Even though the sensor node has the resource to perform the very complex operation of public key cryptosystem, it cause a vulnerability to denial of service attack.
- **Vulnerability to sensor node compromise**: Since the sensor nodes may be deployed in very hostile positions, it causes the vulnerability to sensor nodes. When the attacker obtains the sensor node, he/she is able to access to sensitive information, such as key information or sensed information. This attack can be prevented by using tamper-resistant sensor node which results in high-cost sensor node. However, a large number of sensor node makes it very difficult to employ the tamper-resistant sensor node since it cause very high-cost network.
- **Difficulty to obtain the after-deployment knowledge**: In most cases, the sensor nodes will be deployed in a random scattering manner. Therefore, it is difficult for the security protocol to know the location knowledge of the neighbour node.
- **Limited memory size, limited transmission power, and limited transmission bandwidth**: Since there are limited memories in each sensor node, it is very difficult to store unique keys with each other sensor nodes in the network. In addition, typical sensor node has low capability of transmission bandwidth and power to communicate with neighbour nodes.

- **Single point of failure of a base station**: In a sensor network, a base station is a gateway to communicate the sensed information with an application server through the IP-based core network. The trust of the sensor network relies on that of the base station. Hence a base station is a source of trust, tempting to invite various attacks of the attackers on the base station.

7 Threats model for USN

The threats for USN are composed of two parts: one for IP network and the other for WSN.

7.1 General threats in WSN

There are two types of attackers in the WSN; mote-type attacker and laptop-type attacker. In the former case, the attacker has a capability similar to the sensor node and can have access to few sensor nodes. An attacker with mote-type device might able to jam the radio link in its vicinity of attacker. In the latter case, attacker may have access to more powerful devices like laptop computer. An attacker with laptop-type device may eavesdrop on the communication in the sensor network, have a high-bandwidth, low-latency communications channel, and can jam the entire sensor network using high power transmitter. There are two types of threats for WSN; general threats and routing-related threats. The threats in the WSN are applied to the communication between the base station and sensor node, and nodes as described in clause 6.1, and the routing-related threats are applied to the routing message exchange as described in clause 6.2.

7.1.1 General threats in WSN

[ITU-T X.800] and [ITU-T X.805] identify the following security threats to the networks, and which are also security threats that are applicable to WSN:

- Destruction of information and/or other resources;
- Corruption or modification of information;
- Theft, removal or loss of information and/or other resources;
- Disclosure of information; and
- Interruption of services.

In addition to them, there are a lot of sensor node specific threats like sensor mode compromise, eavesdropping, privacy of sensed data, denial of service attack, and malicious use of commodity network were identified.[b-Chan]

- **Sensor node compromise:** We expect sensor networks to consist of hundreds or thousands of sensor nodes. Each node represents a potential point of attack, making it impractical to monitor and protect each individual sensor from either physical or logical attack. The networks may be dispersed over a large area, further exposing them to attackers who capture and reprogram individual sensor nodes. Attackers can also obtain their own commodity sensor nodes and induce the network to accept them as legitimate nodes, or they can claim multiple identities for an altered node. Once in control of a few nodes inside the network, the adversary can then mount a variety of attacks—for example, falsification of sensor data, extraction of private sensed information from sensor network readings, and denial of service. Addressing the problem of sensor node compromise requires technological solutions. For example, cheap tamper- resistant hardware could make it challenging to reprogram captured sensor nodes. However, making nodes robust to tampering is not economically viable. We must therefore assume that an attacker can compromise a subset of the sensor nodes. Hence, at the software level, sensor networks need new capabilities to ensure secure operation even in the presence of a small number of malicious network nodes. *Node-to-node authentication*

is one basic building block for enabling network nodes to prove their identity to each other. *Node revocation* can then exclude malicious nodes. Achieving these goals on resource limited hardware will require lightweight security protocols. Further, all communications and data-processing protocols used in sensor networks must be made *resilient*—that is, able to function at high effectiveness even with a small number of malicious nodes. For example, routing protocols must be resilient against compromised nodes that behave maliciously.

- **Eavesdropping:** In wireless sensor network communications, an adversary can gain access to private information by monitoring transmissions between nodes. For example, a few wireless receivers placed outside a house might be able to monitor the light and temperature readings of sensor networks inside the house, thus revealing detailed information about the occupants' personal daily activities. Encrypting sensor node communications partly solves eavesdropping problems but requires a robust key exchange and distribution scheme. The scheme must be simple for the network owner to execute and feasible for the limited sensor node hardware to implement. It must also maintain secrecy in the rest of the network when an adversary compromises a few sensor nodes and exposes their secret keys. Ideally, these schemes would also allow revocation of known exposed keys and rekeying of sensor nodes. The large number of communicating nodes makes end-to-end encryption usually impractical since sensor node hardware can rarely store a large number of unique encryption keys. Instead, sensor network designers may choose hop-by-hop encryption, where each sensor node stores only encryption keys shared with its immediate neighbors. In this case, adversary control of a communication node eliminates encryption's effectiveness for any communications directed through the compromised node. This situation could be exacerbated if an adversary manipulates the routing infrastructure to send many communications through a malicious node. More robust routing protocols are one solution to this problem. Another solution is *multipath routing*, which routes parts of a message over multiple disjoint paths and reassembles them at the destination. Efficient discovery of the best disjoint paths to use for such an operation is another research challenge.
- **Privacy of sensed data:** Sensor networks are tools for collecting information, and an adversary can gain access to sensitive information either by accessing stored sensor data or by querying or eavesdropping on the network. Adversaries can use even seemingly innocuous data to derive sensitive information if they know how to correlate multiple sensor inputs. For example, an adversary that gains access to both the indoor and outdoor sensors of a home may be able to isolate internal noise from external noise and thus extract details about the inhabitants' private activities. The main privacy problem, however, is not that sensor networks enable the collection of information that would otherwise be impossible. In fact, much information from sensor networks could probably be collected through direct site surveillance. Rather, sensor networks aggravate the privacy problem because they make large volumes of information easily available through remote access. Hence, adversaries need not be physically present to maintain surveillance. They can gather information in a low-risk, anonymous manner. Remote access also allows a single adversary to monitor multiple sites simultaneously. Ensuring that sensed information stays within the sensor network and is accessible only to trusted parties is an essential step toward achieving privacy. Data encryption and access control is one approach. Another is to restrict the network's ability to gather data at a detail level that could compromise privacy. For example, a sensor network might anonymize data by reporting only aggregate temperatures over a wide area or approximate locations of sensed individuals. A system stores the sensed data in an anonymized database, removing the details that an adversary might find useful. Another approach is to process queries in the sensor network in a distributed manner so that no single node can observe the query results in their entirety. This approach guards against potential

system abuse by compromised malicious nodes.

- **DOS attacks:** As safety-critical applications use more sensor networks, the potential damage of operational disruptions becomes significant. Defending against denial-of-service attacks which aim to destroy network functionality rather than subverting it or using the sensed information, is extremely difficult. DoS attacks can occur at the physical layer—for example, via radio jamming. They can also involve malicious transmissions into the network to interfere with sensor network protocols or physically destroy central network nodes. Attackers can induce battery exhaustion in sensor nodes—for example, by sending a sustained series of useless communications that the targeted nodes will expend energy processing and may also forward to other nodes. More insidious attacks can occur from inside the sensor network if attackers can compromise the sensor nodes. For example, they could create routing loops that will eventually exhaust all nodes in the loop. Potential defenses against denial-of service attacks are as varied as the attacks themselves. Techniques such as spread-spectrum communication or frequency hopping can counteract jamming attacks. Proper authentication can prevent injected messages from being accepted by the network. However, the protocols involved must be efficient so that they themselves do not become targets for an energy exhaustion attack. For example, using signatures based on asymmetric cryptography can provide message authentication. However, the creation and verification of asymmetric signatures are highly computationally intensive, and attackers that can induce a large number of these operations can mount an effective energy-exhaustion attack.
- **Malicious commodity networks:** The proliferation of sensor networks will inevitably extend to criminals who can use them for illegal purposes. For example, thieves can spread sensors on the grounds of a private home to detect the inhabitants' presence. If the sensors are small enough, they can also plant them on computers and cell phones to extract private information and passwords. With widespread use, the cost and availability barriers that discourage such attacks will drop. Sensor detectors offer one possible defense against such attacks. A detector must be able not only to detect the presence of potentially hostile wireless communications within an area that may have significant levels of radio interference but also to differentiate between the transmissions of authorized and unauthorized sensor networks and other devices. Such technologies might not prevent unauthorized parties from deploying sensor networks in sensitive areas, but they would make it more costly, thus alleviating the problem somewhat.

7.1.2 Routing-specific threats

[ITU-T X.800] and [ITU-T X.805] identifies five threats that are applicable to routing-related message exchange in WSN. In addition to them, there are seven threats against the routing messages which are exchanged between the sensor nodes.

- **Spoofed, altered, replayed routing information:** The attacker is able to spoof, alter, reply the routing information resulting creating routing loop, attracting network traffic, extending source routing, and increasing end-to-end latency.
- **Selective forwarding:** It refers to an attack in which a compromised node by an attacker may refuse to forward certain messages and drop them, stopping propagating any further.
- **Sinkhole attack**: It refers to attack in which the attacker attracts all the traffic from a particular area through compromised node.
- **Sybil attacks**: It refers to attack in which a single node presents multiple identities to other nodes in the network convincing every node that an adversary exists in more than one place

at once.

- **Wormhole attacks**: In the wormhole attack, an adversary tunnels messages received in one part over a low latency link and replays then in a different part. Wormhole attacks will involve two distinct malicious nodes colluding to understate their distance from each other by replaying packet along an out-of-band channel available only to the attacks.
- **HELLO flood attacks**: It refers to the attack in which a laptop-type attacker broadcasts the HELLO packets convincing every node in the network that an adversary was its neighbor.
- **Acknowledgement spoofing**: In acknowledgement spoofing, an adversary can spoof link layer acknowledgement for "overheard" packet addressed to neighboring node convincing the sender that a weak link is strong or a dead or disabled node is alive.

7.2 General threats in IP network

The threats model for IP network is similar to ITU-T X.805 Recommendation.

[Editor's Note] Descriptions to be added

8 Security requirements for USN

To countermeasure the above threats, the following security requirements in ITU-T X.805 can be applicable:

- **Data Confidentiality:** A sensor network should not leak sensor readings to neighboring networks. In many applications (e.g. key distribution) nodes communicate highly sensitive data. The standard approach for keeping sensitive data secret is to encrypt the data with a secret key that only intended receivers possess, hence achieving confidentiality.
- **Data Authentication:** Message authentication is important for many applications in sensor networks. Within the building sensor network, authentication is necessary for many administrative tasks (e.g. network reprogramming or controlling sensor node duty cycle). At the same time, an adversary can easily inject messages, so the receiver needs to make sure that the data used in any decision-making process originates from the correct source. Informally, *data authentication* allows a receiver to verify that the data really was sent by the claimed sender. In the two-party communication case, data authentication can be achieved through a purely symmetric mechanism: The sender and the receiver share a secret key to compute a message authentication code (MAC) of all communicated data. When a message with a correct MAC arrives, the receiver knows that it must have been sent by the sender. This style of authentication cannot be applied to a broadcast setting, without placing much stronger trust assumptions on the network nodes. If one sender wants to send authentic data to mutually untrusted receivers, using a symmetric MAC is insecure: Any one of the receivers knows the MAC key, and hence could impersonate the sender and forge messages to other receivers. Hence, we need an asymmetric mechanism to achieve authenticated broadcast. One of our contributions is to construct authenticated broadcast from symmetric primitives only, and introduce asymmetry with delayed key disclosure and one-way function key chains.
- **Data Integrity:** In communication, *data integrity* ensures the receiver that the received data is not altered in transit by an adversary.
- **Access control**[ITU-T X.805] Access control ensure that only authorized user or entity is allowed to gain access to information, resource, or services.

- **Non-repudiation**[ITU-T X.805] Non-repudiation ensure that no entity or user can not deny the activities in the network done by themselves.
- **Communication security**[ITU-T X.805] Communication security ensure that the information only flows from source to destination.
- **Availability**[ITU-T X.805] Availability ensure that information, service, and application are available to legitimate users any time.
- **Privacy**[ITU-T X.805] Privacy ensure that identifier of user or entities and network usage is kept secret.

9 Security requirements and threats in USN

The message exchange in WSN can be grouped into three types; message exchange between nodes, message exchange between a base station and a node, message exchange for routing –related message.

9.1 Security requirement and threats for the message exchange in WSN

9.1.1 Security requirement and threats for the message exchange between the sensor nodes

Table 1 lists the Security requirements and describes mapping of Security Dimensions to security threats identified in ITU-T X.805: the letter 'Y' in a cell formed by the intersection of the table's columns and rows designate that a particular security threat is opposed by a corresponding security dimension.

Table 1: Mapping of security dimensions to security threats

Security dimension	Security threat				
	Destruction of information or other resources	**Corruption or modification of information**	**Theft, removal or loss of information and other resources**	**Disclosure of information**	**Interruption of services**
Access control	Y	Y	Y	Y	
Authentication			Y	Y	
Non-repudiation	Y	Y	Y	Y	Y
Confidentiality			Y	Y	
Communication Security			Y	Y	
Data Integrity	Y	Y			
Availability	Y				Y
Privacy				Y	

Table 2 lists the Security requirements and describes mapping of Security Dimensions to sensor node specific threats for the message exchange between the nodes: the letter 'Y' in a cell formed by the intersection of the table's columns and rows designate that a particular security threat is opposed by a corresponding security dimension.

Table 2: Security requirements to sensor node specific threats

Security requirements	Sensor node specific threats				
	Sensor node compromise	Privacy of sensed data	DoS	Malicious commodity network	Replay attack
Access control					
Authentication			Y		Y
Non-repudiation					
Confidentiality		Y		Y	
Communication Security	Y				
Data Integrity					
Availability			Y		
Privacy					

9.1.2 Security requirement and threats for the broadcast message from a base station to all sensor nodes

Table 3 lists the Security Dimensions and describes mapping of Security requirements to security threats against the broadcast message by a base station to all the sensor nodes: the letter 'Y' in a cell formed by the intersection of the table's columns and rows designate that a particular security threat is opposed by a corresponding security dimension.

Table 3: security requirements to security threats against broadcast message

Security dimension	Security threats against broadcast message from a base station to all nodes				
	Destruction of information	Corruption or modification of information	Theft, removal or loss of information	Disclosure of information	Interruption of services, DoS
Access control	Y	Y	Y	Y	
Authentication		Y	Y	Y	
Non-repudiation	Y		Y		Y
Confidentiality			Y	Y	
Communication Security			Y	Y	
Data Integrity	Y	Y			
Availability	Y				Y
Privacy				Y	

9.1.3 Security requirement and threats for the routing message exchange

The threats can be classified into two categories: insider attacks and outsider attacks. Insider attacks can be launched by the insider, i.e. the attacker has knowledge of the sensitive information stored in the sensor node, i.e. key information for the secure channel. Insider attacks are composed of sybil attack, HELLO flood attack, wormhole and sink hole attack, selective forwarding attack, and DoS attack. Table 4 lists the Security Dimensions and describes mapping of Security

requirements to security threats of the routing message exchange launched by insider attack: the letter 'Y' in a cell formed by the intersection of the table's columns and rows designate that a particular security threat is opposed by a corresponding security dimension.

Table 4: Mapping of security dimensions to security threats for the insider attack

Security requrements	Security threat					
	Sybil attack	**HELLO flood**	**Wormhole and sinkhole**	**Selective forwarding**	**DoS**	**Acknowledgement spoofing**
Access control	Y	Y	Y	Y		
Message Authentication		Y				
Identification Authentication	Y	Y	Y	Y		
Non-repudiation						
Confidentiality			Y	Y		
Communication Security			Y	Y		
Data Integrity	Y	Y				
Availability						
Privacy			Y	Y		

Table 5 lists the Security Dimensions and describes mapping of Security requirements to security threats of the routing message exchange launched by outsider attack: the letter 'Y' in a cell formed by the intersection of the table's columns and rows designate that a particular security threat is opposed by a corresponding security dimension.

Table 5: Mapping of security dimensions to security threats for the outsider attack

Security dimension	Security threat					
	Sybil attack	**HELLO flood**	**Wormhole and sinkhole**	**Selective forwarding**	**DoS**	Acknowledgement spoofing
Access control				Y		
Message Authentication						
Identification Authentication	Y	Y	Y	Y		
Non-repudiation						
Confidentiality			Y	Y		
Communication Security			Y	Y		
Data Integrity		Y				
Availability						
Privacy			Y	Y		

9.2 Security requirement and threats for the message exchange in IP network

[Editor's Note] Descriptions to be added.

10 Relationship between the security requirement and security function

These security functions are used to satisfy some of the security requirements. Table 5, copied form ITU-T X.1111, shows some set of security functions to satisfy specific security requirements. In table 6, the letter 'Y' ' in a cell formed by the intersection of the table's columns and rows designates that a particular security service can be opposed by a corresponding security function, the letter 'K' means that the security service could be supplemented or reinforced by a marked security mechanism, and the letter 'X' means that a specified security service can be provided by one of the optional security functions. For example, access control function can be grouped into two access control functions; physical access control and technical access control.

Table 5– Illustration of relationship between security requirements and security functions

Security Requirement \ Security function		Encipherment	Integrity	MAC	Entity authentication	Digital Signature	Notarization	Access control		Key management	Anti-availability	
								Physical	Technical		Physical	Technical
Confidentiality	Communication .data	Y						K		Y		
	Stored data	Y						K		Y		
Integrity	Communication .data		X	X		X	X			Y		
	Stored data		X	X		X	X			Y		
Authentication	Entity				Y					Y		
	Message			X		X	X			Y		
Non-repudiation						Y	Y			Y		
Access control	Communication .data	K						K		K		
	Stored data	K		Y	Y	Y		K	Y	Y		
Availability	Communication .data							X			X	Y
	Stored data			X	X	X			K	Y		Y
Privacy	Communication .data	Y						K		Y		
	Stored data	Y		X	X	X		K	Y	Y		
Communication flow security			X	X	X			K	Y	Y		

11 Security technologies for USN

11.1 Key management

It refers to the generation, distribution, sharing, rekeying, and revocation of cryptographic keys for data confidentiality service, data integrity, data freshness, and data authentication in the WSN. The security of key management forms a foundation of security of other security services. In sensor network, it is very important to share or distribute a pair-wise key between the sensor nodes and a group-wise key among a set of sensor nodes. It is sometimes called a key agreement scheme.

In general, there are three types of key agreement: trusted server scheme, self enforcing scheme, and key pre-distribution scheme. The trusted server scheme uses the central trusted server to share the pair-wise key between the sensor nodes or group-wise key among the sensor nodes. The typical example of this scheme is Kerboros. However, this type of scheme is not adequate for the sensor network since there is no trusted infrastructure in the sensor network. The self enforcing scheme uses the public key algorithm to share the pair-wise key or group-wise key in the sensor network. The typical algorithm of public key algorithm includes Diffie-Hellman key agreement algorithm and RSA key transport algorithm. However, this scheme can not be employed in the sensor network due to the limited memory and computational complexity of the sensor node. The key pre-distribution scheme pre-distributes the key information among all sensor nodes prior to deployment. The deployment of most sensor nodes is random. That is, it is not assumed that a priori knowledge about the exact location of sensor node is not known prior to deployment. This scheme has a low communication overhead. In addition, it is resilient to node compromise and does not rely on the trust of base station. Therefore, this scheme is very suitable to wireless sensor network.

There are a number of key pre-distribution schemes that do not assume to have a knowledge of deployment of sensor node. The simple scheme is master key based pre-distribution scheme. In this scheme, all nodes have a single common master key that is pre-deployed to each sensor node. Any two nodes use this global master key to obtain the common pair-wise key by exchanging the random nonces. This scheme does not provide desirable resilience to node compromise since if a node is compromised, the entire sensor network is compromised. The second scheme is called pair-wise key pre-distribution scheme. This scheme is to let each sensor node have N-1 secret pair-wise keys, each of which is only known to this sensor node and one of the other N-1 sensor nodes, where N is the total number of sensor nodes in the network. This scheme gives a perfect resilience against the node compromise since a compromised node does not affect security of any other node. However, it gives no scalability since adding new nodes to the existing sensor node is impossible since the existing node does not have a new pair-wise key. In addition, this scheme is not practical since the memory size is limited when the number of sensor node is very large. The third scheme is a random key pre-distribution scheme. In this scheme, the subset of keys from large key pool are stored before deployment of sensor node, two nodes find a common key, and use that common key as shared session key between the two sensor nodes.

The requirements of key management in a sensor network should be as follows;

- **Scalable key management**; The key management scheme should support a large sensor network. In addition, it should be flexible when there is a substantial increase of sensor nodes even after deployment of sensor node.
- **Efficiency of memory size, processing capability, and communication overhead required for key management**: The key management scheme should have efficient storage complexity, i.e. minimum memory size to sore the key in the sensor node, a efficient computation complexity required to establish the key, a efficient communication overhead, i.e. the number of message exchanged during key generation process.
- **High pair-wise key establishment**: The key management scheme should have a high probability that two sensor nodes establish the common key and key material.
- **Resilience against node compromise**: The key management scheme should have a capability to resistant against node compromise. Compromise of security credential should not reveal least information about security of other link in the sensor network, that is, higher resilience indicates lower number of compromised links.

The detail on key management is described in ANNEX A.

11.2 Authenticated Broadcast

<TBD>

11.3 Secure Data Aggregation

<TBD>

11.4 Data Freshness

Given that all sensor networks stream some forms of time varying measurements, it is not enough to guarantee confidentiality and authentication; we also must ensure each message is *fresh*. Informally, data freshness implies that the data is recent, and it ensures that no adversary replayed old messages. We identify two types of freshness: weak freshness, which provides partial message ordering, but carries no delay information, and strong freshness, which provides a total order on a request-response pair, and allows for delay estimation. Weak freshness is required by sensor measurements, while strong freshness is useful for time synchronization

11.5 Tamper Resistant Module

<TBD>

11.6 Middleware security for IP network

<TBD>

12 Specific security function requirement for each entity

This clause specifies various levels of security requirements that pertain, individually or collectively, to WSN security.

12.1 Mandatory Requirements

- The key management scheme of WSN is required to have a good scalability, a high resilience to node compromise, a high pair-wise establishment, an efficient memory size, a low computational complexity, a low communication overhead.
- The key management is required to have an efficient pair-wise key establishment and group-wise key establishment.
- The WSN is required to support authenticated broadcast from a base station to all the sensor nodes.
- The WSN is required to support secure routing protocol with message authentication, ID authentication, and data integrity.
- The base station in WSN is required to support the countering mechanisms to protect from DoS attack from both wireless interface and wired interface.
- [Editor Note: Further requirements will be developed]

12.2 Recommended Requirements

- The WSN is recommended to have a secure end-to-end data aggregation scheme.
- [Editor Note: Further requirements will be developed]

12.3 Optional Requirements

- The WSN can optionally have a hop-by-hop data aggregation function.
- The WSN can optionally implement the tamper resistant sensor node.
- [Editor Note: Further requirements will be developed]

Bibliography

- [b-ITU-T C22] ITU-T TSAG – C 22 – E, A preliminary study on the Ubiquitous Sensor Network, Feb. 2007.
- [b-Y.USN-reqts] Draft Recommendation *Y.USN-reqts*, "Requirements for support of USN applications and services in NGN environment," (Geneva, 11-21 September 2007), submitted by ETRI, Republic of Korea, at: http://www.itu.int/md/T05-NGN.GSI-DOC-0266/en.
- [b-SPINS] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J. D. Tygar, SPINS: *Security Protocols for Sensor Networks*
- [b-Chan] Haowen Chan and Adrian Perrig, *Security and Privacy in Sensor Networks*
- [b-Karlof] C. Karlrof, D. Wagner, *Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures*
- [b-Akildiz] I.F.Akildiz, W.Su, Y. Sankarasubramaniam, and E.Cayirci, *A Survey on Sensor Networks*

ANNEX A:
Key management in Wireless Sensor Networks

A.1 Threat Time

Once deployed, in order to ensure key's security, nodes establish a pair-wise key in a short time so that it is crucial whether the phase of key setup is exposed to an adversary or not because sensitive information, such as random number or identity information of node, is open during this phase. An adversary may get ready to attack in advance before key setup. This adversary can analyze communication between nodes or get the physical access to node during key setup. This adversary is regarded as strong and intensive. It means the application requiring a high security level must design a key scheme as assuming a prepared adversary.

On the contrary, to make an application more flexible and usable, key management scheme with low security level can be taken. In this case, after a key is established, an attack is possible. It is hard that an adversary, who does not know deployed time and is unable to access to deployed place, tries an attack during key setup. This is a very real case despite loose attack. On the application where loose or no attacks during key setup are launched, it is reasonable to design a key scheme to improve efficiency and scalability as providing only loose security.

A.2 Key Management classes

By above two criterion, two threats and threat time, 4 key management classes are defined.

A.2.1 Class 1

This class assumes that an adversary can eavesdrop after key setup. There is not any other threat like node capture all along the network life. Thus, this class considers the weakest adversary.

A.2.1 Class 2

This class assumes that an adversary can eavesdrop or capture and reprogram nodes for node compromise after key setup. In other words, during key setup, there are no threats in place and eavesdropping hardly exists. After key setup, an adversary is capable of eavesdropping or obtaining secret information through node capture.

A.2.3 Class 3

This class assumes that an adversary can eavesdrop the communications when nodes are deployed and, after key establishment, he is prepared for all attacks including node capture.

A.2.4 Class 4

An active adversary always waits for node deployment. It means that eavesdropping and node capture happen already in the phase that nodes are deployed. This class, considering the strongest adversaries, is a general assumption but requires an expensive cost.

Generally, if an adversary is able to attack including node capture, he is considered to have the enough ability to eavesdrop transmitted data. Accordingly, other classes need not to be considered: the case that node compromise is always possible but eavesdropping is practical only after key setup, and the case that all the attacks except eavesdropping are possible only after key setup. Moreover, the higher a class level is, the stronger an adversary is. If a key scheme in higher class is secure, it is also secure in lower class. The key scheme classes are as Figure 1.

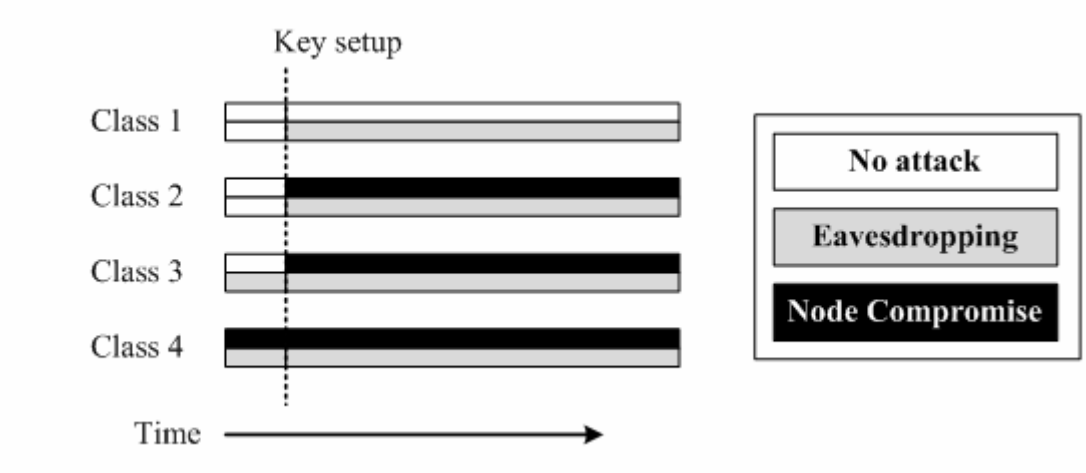

Figure A-1. Key Management Classes

A.3 Key Schemes

A.3.1 Key Management Mechanisms

A.3.1.1 PAIR-WISE KEY PRE-DISTRIBUTION

A pair-wise key between a pair of nodes is directly stored, pre-distributed, in each node before node deployment (hereafter Pair-wise key scheme). Since each node in this scheme stores its pairwise keys, it has perfect resilience against node capture which means even if a node is captured, the keys of non-captured nodes are never compromised. However, scalability is limited because network scale depends on the memory of node where potential keys are stored.

A.3.1.2 MASTER KEY BASED PRE-DISTRIBUTION

A pair-wise key is derived from both a random number exchanged between each node and a single master key pre-distributed into each node (hereafter Master key scheme). It results in great key connectivity and a little memory required. However, resilience is very low since all the pair-wise keys can be compromised when the master key is exposed to an adversary. Unlike Master key scheme which does not erase a master key after key setup, in `LEAP' a master key is erased completely after a pair-wise key is established. Although resilience is improved by erasing a master key of deployed nodes, there is still the risk of compromising a master key during node addition since added nodes store a master key.

A.3.1.3 BASE STATION PARTICIPATION

`SPINS' is included in this mechanism. In SPINS, each node is given its shared key with the base station. The base station directly transmits a pair-wise key respectively encrypted with each node's shared key. In other words, the base station intermediates in key setup. This scheme supports not only full connection but also perfect resilience. However, it is not scalable because of the terrible traffic volume resulting from intermediation.

A.3.1.4 PROBABILISTIC KEY PRE-DISTRIBUTION

For large networks, a probabilistic method is more efficient than a deterministic method. This mechanism results from the concept all the nodes in the entire networks are connected with the 0.9997 probability- almost fully connected- if the probability each node can establish a pair-wise key with its neighbour nodes is 0.33. A key ring is stored in each node before deployment (a key

ring *k* is randomly selected from key pool *P* which is randomly selected from huge key space). A common key in both key rings of a pair of nodes is used as their pair-wise key. It guarantees enough resilience even though not perfect resilience, because the probability of breaking communication link is *k/P*. Moreover, it supports the large scale networks. The representative scheme is `EG scheme'. Its variants are proposed like a combination of the EG scheme and the Blundo scheme and a combination of the EG scheme and the Blom scheme which significantly enhance the security.

A.3.1.5 NO KEY PRE-DISTRIBUTION

This mechanism is considering the reality of wireless sensor networks. If an adversary does not know where and when nodes are deployed, it is difficult to launch active attack at an early phase. It can be a good trade-off to improve efficiency instead of a little node loss due to attacks during key setup. `Key infection' is a representative scheme. In Key infection, key setup is completed in a relatively short time through a few transmissions. The advantage in this mechanism is the base station does not take part in a key setup so that it consumes relatively less energy. Unlike the pre-distribution schemes above, it need not load potential keys into a node, which results in the low cost of network organization. However, it is only strong when an adversary does not observe communication during key setup and it cannot add nodes since a pair-wise key is established through exchanged data during key setup.

A.4 Key Management Schemes in Class 1

[Editor’s note] Key schemes will be shown in class 1.

A.4.1 Key Management Schemes in Class 2

[Editor’s note] Key schemes will be shown in class 2.

A.4.2 Key Management Schemes in Class 3

[Editor’s note] Key schemes will be shown in class 3.

A.4.3 Key Management Schemes in Class 4

[Editor’s note] Key schemes will be shown in class 4.

_____