Telecommunications and Information Exchange Between Systems

ISO/IEC JTC 1/SC 6

Document Number:	N14015
Date:	2009-06-10
Replaces:	
Document Type:	Text for CD ballot
Document Title:	Text for CD ballot, ISO/IEC 29180, Security framework for sensor network
Document Source:	SC 6/WG 7 Tokyo meeting
Project Number:	
Document Status:	As per the SC 6 Tokyo resolution 6.7.9, this document is authorized for CD ballot. SC 6 NBs are requested to ballot electronically on www.iso.org/jtc1/sc6 by 2009-09-10.
Action ID:	LB
Due Date:	2009-09-10
No. of Pages:	27

Title: CD Ballot Text of ISO/IEC 29180, Security framework for sensor network

Source: ISO/IEC JTC 1/SC 6/WG 7

This document is an updated text of ISO/IEC CD 29180 for CD ballot processing.

Foreword

This Recommendation | International Standard establishes presentation rules for documents that are intended to be both ITU-T Recommendations and ISO/IEC International Standards.

The rules proposed in this Recommendation | International Standard are based on the "Author's guide for drafting ITU-T Recommendations" and on ISO/IEC Directives, Part 2. Deviations from these documents are proposed only in order to arrive at a common set of presentation rules.

In order to facilitate comparison with other presentation styles, this document has been prepared in accordance with the presentation rules that it mandates. The examples used within the text, such as for references, are for illustrative purposes only. Thus, this document constitutes an example of the proposed presentation style. It is noted that neither an ITU-T Recommendation A.1000 nor an ISO/IEC International Standard 0001 exist.

Introduction

This draft Recommendation | International Standard 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 requirements and security technologies are presented for the Ubiquitous Sensor Network.

Keywords

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

Content

INTERNATIONAL STANDARD ISO/IEC 29180
ITU-T RECOMMENDATION X.usnsec-1

Information technology –Security framework for ubiquitous sensor network

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 security model of the Ubiquitous Sensor Network. Finally, the security requirements and security technologies are presented for the Ubiquitous Sensor Network.

2   Normative references

The following Recommendations and International Standards contain provisions which, through reference in this text, constitute provisions of this Recommendation | International Standard. At the time of publication, the editions indicated were valid. All Recommendations and Standards are subject to revision, and parties to agreements based on this Recommendation | International Standard are encouraged to investigate the possibility of applying the most recent edition of the Recommendations and Standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards. The Telecommunication Standardization Bureau of the ITU maintains a list of currently valid ITU-T Recommendations.

.

2.1   Identical Recommendations | International Standards

2.2   Paired Recommendations | International Standards equivalent in technical content

[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*

[ITU-T Y.2701]   ITU-T Recommendation Y.2701 (2007), *Security Requirements for NGN Release 1*

2.3 Additional references

3 Definitions

For the purposes of this Recommendation | International Standard, the following definitions apply.

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 Actuator[b-ISO/IEC SGSN N049]: a device that changes a measureable physical property in response to an electrical signal.

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

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

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

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

3.1.9 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.

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

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

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

3.1.13 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.

3.1.14 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.

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

3.1.16 Sensor[b-ISO/IEC SGSN N049**]**: a device that generates an electrical signal which represents a measureable physical property.

3.1.17 Sensor network[b-ISO/IEC SGSN N049]: a collection of two or more sensor-network nodes and one or more sensor-network controllers interacting with each other in a single network.

3.1.18 Sensor-network controller[b-ISO/IEC SGSN N049]:a processing system that can receive sensor data from sensor-network nodes, send electrical signals to actuators in sensor-network nodes, and send control signals to sensor-network nodes.

3.1.19 Sensor-network node[b-ISO/IEC SGSN N049]:a device that contains at least one sensor and zero or more actuators, with the capability of 1) using internal sensor data to control any actuators present, or 2) sending sensor data and receiving actuator commands over the network.

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

3.1.21 Ubiquitous Sensor Networks (USN): a conceptual structured network which deliver sensed information and knowledge services to anyone at anywhere and anytime where the information and knowledge is developed by using context awareness. Or A sensor network which either covers a wide geographical area or supports several different applications, or both.

Editors' note: the definition is from the Y.USN-reqts, the ongoing work in SG13. contributions are invited to enhance the definition (e.g. context awareness, anyone at anywhere and anytime)

3.1.22 USN middleware: The common application platform to support various functions on behalf of various USN applications and services to control heterogeneous sensor networks, provide basic query processing, and provide high-level integrated services(context-aware processing, event processing, sensor data mining, integrated sensor data processing)

Editors' Note: the definition is from the F.usn-mw, the ongoing work in SG16. Contributions are invited to enhance the definition

3.2   Terms defined in this Recommendation | International Standard

This document defines the following terms:

3.2.1 Bootstrapping: It refers to a process to establish a security association between the sensor nodes which may have been initialized with key information, enabling the sensor node to securely communicate with other sensor node after deployment of sensor nodes.

3.2.2 Credentials: It refers to an identifiable object that can be used to authenticate the claimant is what it claims to be and authorize the claimant's access rights.

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 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.

4   Abbreviations and acronyms

This contribution uses the following abbreviations:

DDoS – Distributed Denial of Service

ID - Identity

USN – Ubiquitous Sensor Network

SN–Sensor Network

5   Conventions

In this Recommendation | International Standard:

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.
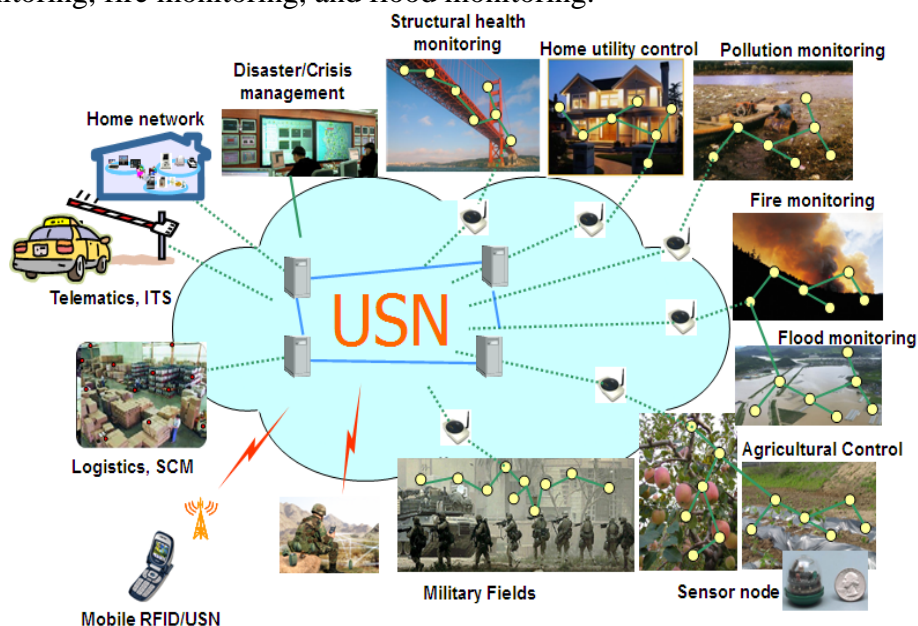
Figure 1 – Application area for USN

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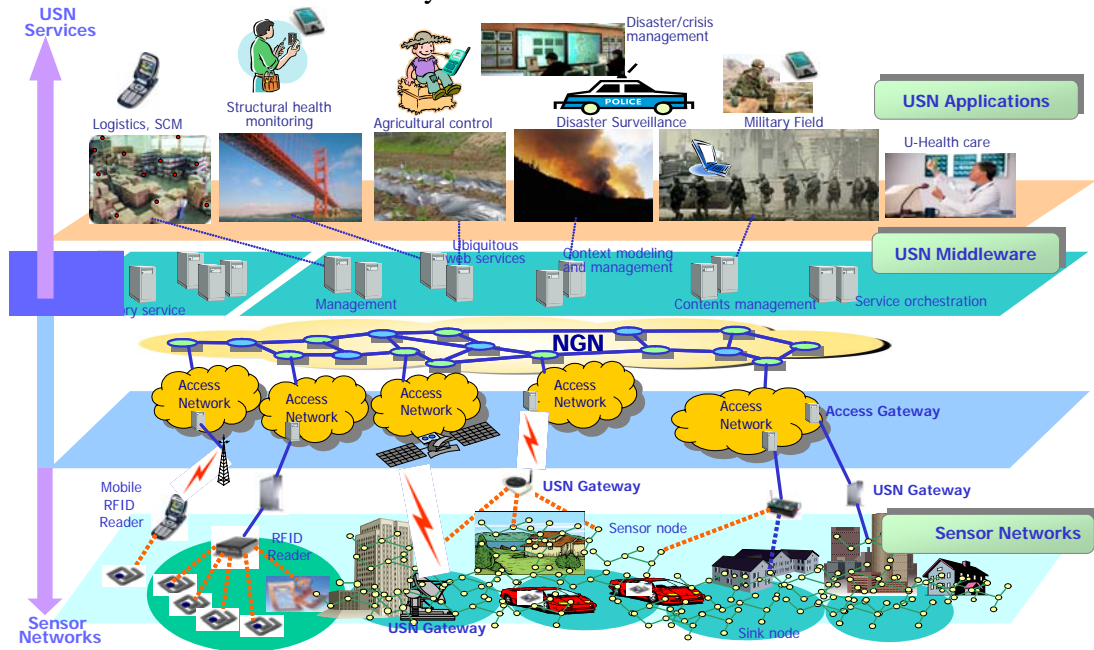

Figure 2 – Overall structure of USN

The sensor networking domain of USN corresponds usually to SN 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 SN as well as IP network.

The communication patterns within our SN fall into three categories:

- Node to base station communication, e.g. sensor readings or special alerts.
- Base station to node communication, e.g. specific requests.

- Base station to all nodes, e.g. routing beacons, queries or reprogramming of entire sensor network.

- Communications among a defined cluster of sensor nodes, e.g. communications between a sensor node and all its neighbors.

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.

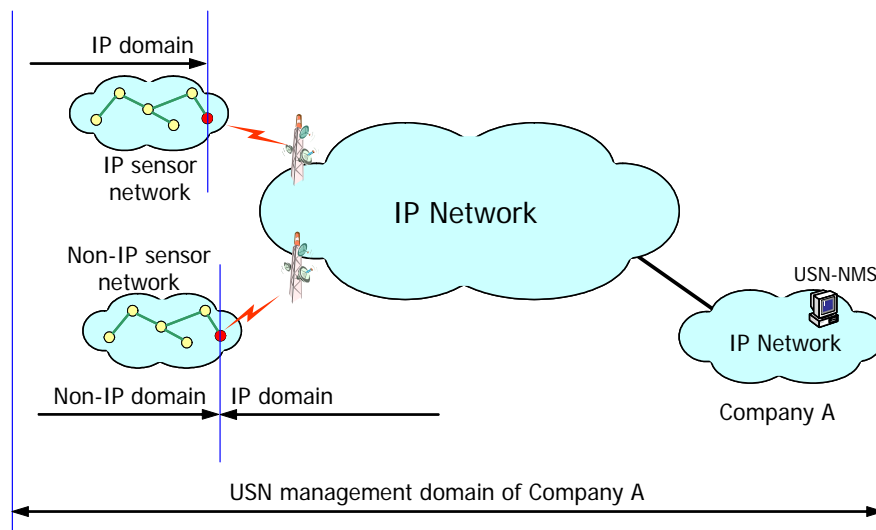So how such network managements are integrated should be taken into account.

Figure 3 – A USN network configuration

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 SN; 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 (SN) 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 SN.

7.1 Threats model in SN

There are two types of attackers in the SN; 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 SN; general threats and routing-related threats. The threats in the SN are applied to the communication between the base station and sensor node, and nodes as described in clause 7.1, and the routing-related threats are applied to the routing message exchange as described in clause 7.2.

7.1.1 General threats in SN

[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 SN:

- 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

[Editor's Note] It is required to be harmonized with X.usnsec-2.

[ITU-T X.800] and [ITU-T X.805] identifies five threats that are applicable to routing-related message exchange in SN. 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 Threats model in IP network

The threats model developed in ITU-T X.805 can be applied to the IP network. Therefore, details can be omitted.

8 Security requirements for USN

To countermeasure the above threats in both SN and IP network, 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 SN 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 SN

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

[Editor's Note] It is required to be harmonized with X.usnsec-2.

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	Acknowle dgement 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

The security threats and security requirements developed in ITU-T X.805 can directly be applied for the secure message exchange through the IP network. Therefore, details about them can be omitted.

10   Security technologies for USN

10.1   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 SN. 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.

10.2   Authenticated Broadcast Message

A broadcast message is targeted to all sensor nodes. A broadcast message authentication scheme allows any targeted nodes to verify the authenticity of the broadcasted messages. Two kinds of techniques can be used to achieve it according to the type of cryptographic algorithm. In case of public key cryptography, digital signature can be used. However, if symmetric cryptography is used, it is necessary to append to the data the verifiable authentication data (i.e., message authentication code) based on the multiple shared secret between the sink node and sensor node. Due to the properties of sensor network, the broadcast authentication method is preferred to one-to-one authentication.

There is a typical scheme to achieve broadcast authentication in sensor networks. The uTESLA protocol [b-SPINS] is the simplified version of TESLA (Timed Efficient Stream Loss-tolerant

Authentication)[b-TESLA]. It basically uses a delayed disclosure of symmetric key. It is assumed that the base station and the sensor nodes are loosely time-synchronized. The operation is as follows; the base station computes MAC on the packet with the key that is secret at that point of time. When a node receives a packet, it can confirm that the base station has not yet disclosed the corresponding MAC key, according to its loosely synchronized clock and time at which the keys are to be disclosed. The node stores the packet in its buffer. When the MAC keys are to be disclosed, the base station broadcasts the MAC keys to all sensor nodes. The sensor node can verify the authenticity of the broadcast message by using the disclosed MAC keys and MAC data stored in the buffer. Each MAC key is a member of a key chain, which has been generated by a one-way function. In order for the base station to generate this key chain, the base station chooses the last key K_n of the key chain randomly, and applies the one-way hash function, H, repeatedly to compute all other keys : $K_i = H(K_{i+1})$, i = 1, …, n-1. The sensor node, which shares K1 with the base station, can verify the correctness of the key and use the disclosed MAC keys and MAC data stored in the buffer to authenticate the packet stored in the buffer.

10.3   Secure Data Aggregation

Data aggregation is a widely used technique in wireless sensor networks.

The security issues, data confidentiality and integrity, in data aggregation become vital when the sensor network is deployed in a hostile environment. There has been many related work proposed to address these security issues.

The secure data aggregation refers to an in-network process which is performed on the aggregator node to securely transfer the aggregation value to sink node(i.e., a base station) 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.

Therefore, it is more useful for the base station or a sensor node to have a capability to aggregate data than individual value from all sensors. By aggregating data, it is possible to reduce the amount of data which needs to be transmitted from one sensor to other sensor. The secure data aggregation can be applied to the sensors that are deployed in a hierarchical structure.

There are two kinds of secure aggregation methods: a hop-by-hop encrypted data aggregation and an end-to-end encrypted data aggregation.

- Hop-by-hop encrypted data aggregation: The operation is based on the hop-by-hop encryption between the neighbor sensor nodes. It is assumed that each pair of neighbor sensor nodes shares a common secret key. The sensed values are encrypted by many sensor nodes. All encrypted values collected are decrypted by the intermediate aggregator nodes. The intermediate aggregator nodes then obtain the aggregated value and encrypt the aggregated value again. This process is repeated until they are reached to sink node. Finally, the sink node obtains the total aggregated value.

- End-to-end encrypted data aggregation: The operation is based the end-to-end encryption between the many sensor nodes and one sink node. It is assumed that common secret is shared between the many sensor nodes and a sink node. The sensing nodes encrypt the sensed values and forward them to intermediate aggregator nodes. The intermediate aggregator nodes only collect them, perform some cryptographic operation on the aggregated values, and forward them since they do not have decryption keys. Finally, the sink node decrypts many encrypted aggregated results.

It is known that the framework for end-to-end encrypted data aggregation has higher computation cost on the sensor nodes, but achieves stronger security, in comparison with the framework for hop-by-hop encrypted data aggregation.

10.4   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

10.5   Tamper Resistant Module

The best well-known technique to protect against the sensor node compromise is to use the tamper-resistant module in sensor node. If each sensor node is equipped with a tamper-resistant module, it may be possible to protect the storage of sensitive data e.g. key data, resulting in the damage following the capture of sensor nodes. The other possible technique to protect against the sensor node is to limit the amount of information obtained by the attacker after reading data from the captured sensor nodes. The former is more expensive than the latter. Therefore, the first option will be limited to applications that are critical enough to be more expensive. If sensor nodes cannot be tamper-resistant, the latter should be implemented to gain probability security.

10.6   USN Middleware security

  Enormous amount of data collected at the sensor network is securely stored, managed and analysed by USN middleware, and USN middleware delivers data to appropriate application through secure channel. As USN middleware communicates with sensor networks or applications over the IP network, USN middleware should consider existing security threats on the IP network. And in order to ensure secure communications against various threats, such as spoofing, sniffing, message modifications, DDoS, etc., security techniques like encryption/decryption, authentication, authorization and access control are considered and applied. Furthermore, encryption/decryption function for data stored in USN middleware is also needed because USN middleware sometimes stores very important and valuable data which cause big problem when they are revealed. Security technique to ensure availability of USN middleware is considered as well.

10.7   IP Network Security

The IP network security technologies in ITU-T X.805 can directly be applied to the secure message exchange through the IP network. Therefore, details about them can be omitted.

11   Specific Security Requirements for USN

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

11.1   Mandatory Requirements

- The SN is required to support the data integrity and message authenticity of sensed data.
- The key management scheme in SN is required to support the key pre-distribution scheme described in clause 10.1.

- The key management is required to support both a pair-wise key establishment and group-wise key establishment.

- The SN is required to authenticate broadcast messages from a base station to all the sensor nodes and vice versa.

- The SN is required to support secure routing protocol with message authentication, ID authentication, data freshness, and data integrity.

- The base station in SN is required to support the capability to mitigate the effects of DoS attacks from both wireless interface and wired interface.

- The USN is required to support USN middleware security described in clause 10.6.

- [Editor's Note: Further requirements will be developed]

11.2   Recommended Requirements

- The SN is recommended to support a secure end-to-end encrypted data aggregation scheme.

- The SN is recommended to support the data freshness for sensed data.

- The SN is recommended to support the confidentiality of sensed data.

- The key management is recommended to support both an ID-based pair-wise key establishment and an ID-based group-wise key establishment.

- The USN is recommended to support the mechanism for ensuring privacy of sensed data.

- [Editor's Note: Further requirements will be developed]

11.3   Optional Requirements

- The sensor node or base station can optionally provide a secure hop-by-hop data aggregation scheme.

- The sensor node can optionally to have tamper –resistant module for protecting credentials, sensed data, or any confidential data.

- The SN can optionally have a capability to mitigate DoS attacks against the sensor node.

[Editor's Note: Further requirements will be developed]

ANNEX A:
Key management in 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.
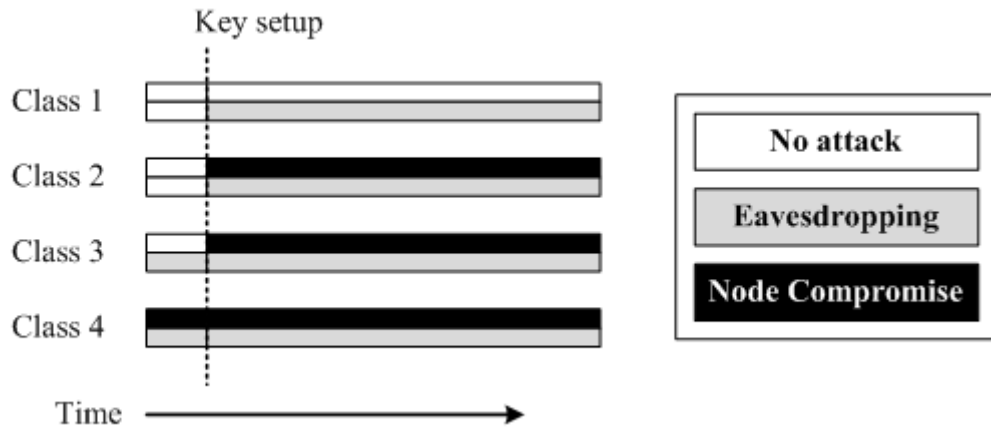
Figure A-1. Key Management Classes

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 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.

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 ubiquitous sensor network (USN) applications and services in NGN environment" (NGN-GSI, 12-22 May 2008).

- [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.*Compuer, pp/99-101, October 2003.

- [b-Karlof] C. Karlrof, D. Wagner, *Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures,* Elsevier, pp.293-315, 2003.

- [b-Akildiz] I.F.Akildiz, W.Su, Y. Sankarasubramaniam, and E.Cayirci, *A Survey on Sensor Networks*, IEEE, pp.102-114, August, 2002.

- [b-TESLA] A.Perrig, R.Canetti, J.D.Tygar, and D. Song, "Efficient authentication and signing of multicast streams over lossy channels," in proceeding of IEEE symposium on Security and Privacy, Berkeley, CA, USA, 2000, pp.56-73.

- [b-ISO/IEC SGSN N049]   Technical Document of ISO/IEC JTC 1 Study Group on Sensor Networks (SGSN)

_____