International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1313

(10/2012)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Secure applications and services – Ubiquitous sensor network security

Security requirements for wireless sensor network routing

Recommendation ITU-T X.1313

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	**X.1310–X.1339**
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1313

Security requirements for wireless sensor network routing

Summary

Recommendation ITU-T X.1313 provides the security requirements for wireless sensor network routing. It explains the general network topologies and routing protocols in ubiquitous sensor networks. In addition, this Recommendation analyses the security threats facing wireless sensor networks.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X.1313	2012-10-14	17

Keywords

Routing, security, USN, WSN.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T X.1313

Security requirements for wireless sensor network routing

1 Scope

Recommendation ITU-T X.1313 describes the security requirements for wireless sensor network routing and also covers the following:

– general network topologies and routing protocols for wireless sensor networks (WSN)

– security threats faced by WSN routing

– security requirements for WSN routing.

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 regularly published. The 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] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[ITU-T X.805] Recommendation ITU-T X.805 (2003), *Security architecture for systems providing end-to-end communications*.

[ITU-T X.1311] Recommendation ITU-T X.1311| ISO/IEC 29180:2011, *Information Technology — Security framework for ubiquitous sensor networks*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 authentication [ITU-T X.800]: See data origin authentication and peer-entity authentication in [ITU-T X.800].

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

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

3.1.4 key [ITU-T X.800]: A sequence of symbols that controls the operation of encipherment and decipherment.

3.1.5 sensor [b-ITU-T Y.2221]: An electronic device that senses a physical condition or chemical compound and delivers an electronic signal proportional to the observed characteristic.

3.1.6 sensor network [b-ITU-T Y.2221]: A network comprised of interconnected sensor nodes exchanging sensed data by wired or wireless communication.

3.1.7 threat [ITU-T X.800]: A potential violation of security.

3.1.8 ubiquitous sensor network (USN) [b-ITU-T Y.2221]: A conceptual network built over existing physical networks which makes use of sensed data and provides knowledge services to anyone, anywhere and at any time, and where information is generated by using context awareness.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 actuator: A receiving and transmitting for sensed data.

3.2.2 ad hoc on-demand distance vector (AODV): An on-demand routing protocol that discovers routes on an "as-needed" basis for wireless ad hoc networks and wireless sensor networks. AODV builds routes using a route request (RREQ) and a route reply (RREP) query cycle. When a source node desires a route to a destination for which it does not already have a route, it broadcasts a route request (RREQ) packet across the network. Nodes receiving this packet update their information for the source node and set up backward pointers to the source node in the route tables.

3.2.3 node integrity: The property wherein the node has not been altered or destroyed in an unauthorized manner.

3.2.4 routing: The process for establishing a communication association between the sensor nodes. Routing involves determining the path, and transporting information through the network.

3.2.5 sensor network node: 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.

3.2.6 topology: The physical and logical arrangement of the elements of a sensor network. In a WSN, it is represented as a collection of sensor nodes and gateways, some of which are connected by wireless links.

3.2.7 wireless sensor network (WSN): A network that consists of a base station and a large number of sensor nodes with wireless transmission capability in the sensor networking domain of the USN.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations:

ACQUIRE	Active query forwarding In sensor networks
AES	Advanced Encryption Standard
AODV	Ad hoc On-demand Distance Vector
APTEEN	Adaptive Periodic Threshold-sensitive Energy-Efficient sensor Network protocol
BS	Base Station
CADR	Constrained Anisotropic Diffusion Routing
CDMA	Code Division Multiple Access
CH	Cluster Head
DAG	Directed Acyclic Graph
DAM	Distributed Aggregate Management
DC	Data-Centric
DODAG	Destination Oriented DAG
DoS	Denial of Service

EBAM	Energy-Based Activity Monitoring
EMLAM	Expectation-Maximization Like Activity Monitoring
GBR	Gradient-Based Routing
GPS	Global Positioning System
ID	Identity
IDS	Intrusion Detection System
IDSQ	Information-Driven Sensor Querying
IPS	Intrusion Prevention System
LEACH	Low Energy Adaptive Clustering Hierarchy
LML	Local Markov Loops
MAC	Medium Access Control
MAC	Message Authentication Code
MCFA	Minimum Cost Forwarding Algorithm
MECN	small Minimum Energy Communication Network
OS	Operating System
PEGASIS	Power-Efficient Gathering in Sensor Information Systems
PHY	Physical
RPL	IPv6 Routing Protocol for Low-power and Lossy networks
RREP	Route Reply
RREQ	Route Request
RTLS	Real-Time Locating Systems
SN	Sensor Network
SOP	Self-Organizing Protocol
SPIN	Sensor Protocols for Information via Negotiation
TDMA	Time Division Multiple Access
TEEN	Threshold-sensitive Energy-Efficient sensor Network protocols
TPM	Trusted Platform Module
USN	Ubiquitous Sensor Network
WPAN	Wireless Personal Area 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 Recommendation | International Standard 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 Recommendation | International Standard 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 that the vendor may optionally provide the feature and still claim conformance with this Recommendation.

6 Characteristics of general network topologies and routing protocols on security considerations for wireless sensor networks (WSN)

A WSN can be composed of more than one base station and several sensors. The base station can be a wired node with many resources, or it can have mobility with less computing resources and batteries. The sensors can be dust types for only sensing data, or they can store or route sensed information, for example, a clustering head or parent node which has more computing resources to enable the acquisition of sensed information from its child sensors, and to enable routing on the configured network topologies.

6.1 General features of routing in the configuration of network topology

Routing is initialised as a neighbour discovery procedure. In WSNs, a base station(s) and many sensors are neighbours. The discovery procedure differs as determined by the relationship with each composed node on configuring the network topology. Also, redundancy and mobility of the base station should be considered.

6.2 General network topologies in the WSN

The WSN nodes are typically organized into one of three types of network topology: the star, tree or mesh topology. Figure 1 shows the three basic types of network topology. In a star topology, each node is directly connected to a central node called the base station.

In star networking, all sensors communicate with their base station. Neighbour discovery is thus performed between the base station and the sensors. The base station advertises its existence with its ID and location information periodically, and the sensors send their response register to the base station with their IDs. To maintain the network status actively, the current state would be exchanged between the base station and the sensor. If the base station or any sensor has failed, shut down or moved, the neighbour discovery would be started. As a result, control packets for neighbour discovery should be considered for security aspects.

In a cluster tree network, the base station and sensors advertise their existence by making it known to each other so that the tree network can be configured. Here, intermediate sensors have batteries and more computing resources for routing to their parents or to the base station than leaf sensors that are responsible for sensing data.

In a mesh topology network, there are at least two nodes with two or more paths between them. This type of topology allows for most transmissions to be distributed, and is reliable due to its multiple paths, even though it may be difficult and expensive to maintain the redundant connections between nodes.

Sensors advertise themselves and solicit their neighbour with a one-hop distance, and are fully or partially connected with other sensors or base station(s) within their possible one-hop propagation. A mesh topology needs sensors with more computing resources and batteries than is required in a tree topology. A periodical neighbour discovery is needed to maintain a mesh network.

In some cases, hybrid topologies exist that are a mix of at least two types of the three basic topologies with clustering. In such a case, clustering would be configured in the form of one or more than three network topologies.

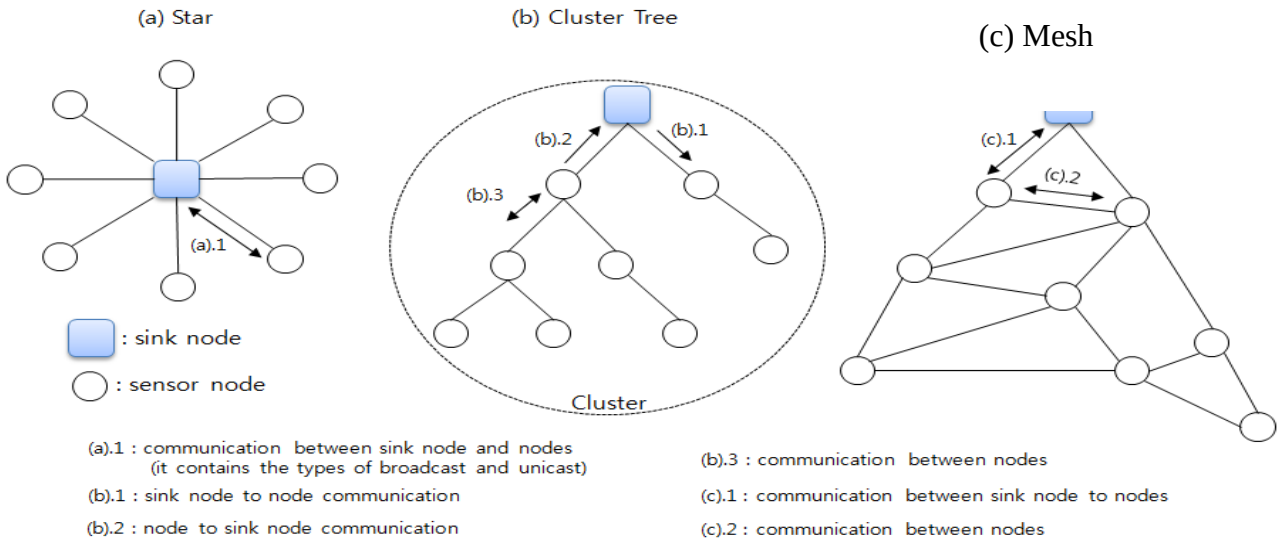

Figure 1 – Three general network topologies for a WSN-base station

6.3 Characteristics of routing protocols in WSN

6.3.1 General features of routing set-up features

In the star topology, routing set-up is not needed because the sensors only send the sensed data to its base station. The address will be an IPv6 address of 6lowpan, a ZigBee address, or a user defined ID for delivering packets.

In a tree and mesh topology, including clustering, each sensor finds its route to its base station for setting up the routing table after neighbour discovery. At this step, the tree join and leave operations from a parent node are performed by the sensors by treating the base station as a root node. Furthermore, the parent node checks the routing table for updating the current status, either periodically or on demand. Each node connects to a higher node in the tree and then to the base station, and data is routed from the leaf node to the base station via several intermediate nodes, which constitute the tree topology. In the tree topology network, a hierarchical routing scheme can be implemented. Also, an address is used for delivering packets between sensors to the base station. The address is used for the delivery of packets.

At this stage, their IDs and routing metric values, which could be battery status, propagation delay, location, or network bandwidth, are used. Therefore, control packets containing the routing information, ID and routing path should be considered for security.

For tree and clustering networking in particular, a parent node and cluster head exist, with the parent and head performing the functions of data aggregation and management of their child nodes. Therefore, their security should be more carefully considered.

6.3.2 Security considerations for WSN routing

Table 1 summarizes the above security considerations for routing features:

Table 1 – Security considerations for routing actions

Topology	Targets of security				Existing protocols	Remarks
	Node	Neighbour discovery	Routing set-up	Packet delivery		
Star	Base station(s) /Sensors	Advertisement control packets, which are triggered periodically and moved; and contain ID and location by BS registration packets by sensors.	N/A	Address, ID, data, next node	Zigbee [b-Zigbee], IEEE 802.16.4 [b-IEEE 802.1.6.4]	
Tree/ Cluster	Base station(s) /Parent sensors (cluster head sensors), child sensors	Advertisement control packets, which are triggered periodically and moved; and contain ID and location by BS and parent nodes.	Join and leave packets containing routing metric values between parent and child nodes with a root node as the BS on initialization and movement, reconstruction phase.	Address, ID, data, next node, routing table	LEACH protocol [b-Heinzelman] PEGASIS [b-Lindsey], TEEN and APTEEN [b-Manjeshwar-1], [b-Manjeshwar-2], MECN [b-Rodoplu], SOP [b-Subramanian], Sensor aggregates routing [b-Fang]	
Mesh	Base station(s) /Sensors	Advertisement control packets from base stations and sensors containing ID location.	Routing set-up packets containing routing metric values on initialization and movement, reconstruction phase.	Address, ID, data, next node, routing table	SPIN [b-Chandrakasan], [b-Kulik], Directed diffusion [b-Intanagonwiwat], Rumor routing [b-Braginsky], MCFA [b-Ye], Gradient-based routing [b-Schurgers], ACQUIRE [b-Sadagopan], Energy aware routing [b-Shah], Routing protocols with random walks [b-Servetto]	

7 Requirements for secure routing

[ITU-T X.1311] describes security threats (clause 7.1.2) and dimensions (clause 9.1) in USN routing aspects. It includes the functional requirements on routing actions, as in Table 1, with the dimensions (clause 9.1). The requirements are shown in clause 11 of [ITU-T X.1311].

7.1 Requirements for sensor and base station

For secure routing, each sensor node and base station should be self-reliable. However, because the sensors are lightweight, certain performance considerations must be addressed to satisfy the security dimensions [ITU-T X.1311].

As the base station is more powerful than the sensors in terms of stored information and the management of WSN networks, it should be protected from DoS attacks and physical tampering to ensure its availability and reliability. Therefore, it should have tamper-proofing and a fault tolerant mechanism. Also, an IDS/IPS or a firewall would be provided in its wired/wireless network as separate systems or virtual forms. The requirements for each sensor and the base station are as follows:

– The base station and sensor are each required to have an authenticator and the key to identify and authenticate each other initially.

– Information stored in the base station and all sensors – especially information on sensed data, ID, and location is required for encryption and authentication.

– To counter insider attacks, it is recommended that the base station guarantees node integrity such as TPM.

– It is recommended that the base stations are allowed the sensor-node list initially for access control before configuration of the sensor network.

– It is recommended that the sensor authorizes the ID for access control before configuration of the sensor network.

– It is recommended that the base station be fault-tolerant, i.e., with regard to duplication and smooth replacement.

– It is recommended that the base station is recommended to have a tamper-proofing mechanism installed in its hardware support, secure bootstrapping, OS enhancements, and software authentication and validation, i.e., by using TPM or sandbox technology.

– The sensor can optionally have fault-tolerance or tamper-proofing.

– The base station can optionally be protected by IDS/IPS or a firewall if it is a wire-lined device.

– For countering insider attacks, sensors can optionally support node integrity.

7.2 Security requirements for the neighbour discovery procedure

Neighbour discovery could be started through broadcasting messages from the base station. So this clause considers the security dimensions and threats for messages broadcast from a base station to all sensor nodes [ITU-T X.1311]. Also, the sensors could use the one-hop broadcasting way to discover its neighbours. After the procedure, all base stations and sensors could form multicast groups for efficient communication.

• The base station is required to have an authorization method for sensors with a secrecy value i.e., a predefined authenticator, key material and ID.

• Each sensor is required to adopt a lightweight authentication mechanism to confirm each other. If, after authenticating with the base station, the group is formed, then the authentication would be performed on the group identifier and a common secrecy value is encrypted with their group key.

- Upon receipt of the broadcast messages, source and message authentication is required to be verified. An advertisement message is required to be authenticated to all the other nodes in a group-aware way on the sensor network.
- As it is a form of response to the advertisement message from the sensors, a unicast message is required to be authenticated at the source.
- For secure communication to protect ID, location information and computing resources, the encryption and key management mechanism is required to be needed for advertisement and solicitation.
- Intermediate sensors can optionally check their authority using the lightweight access control method in the same way as for the group-aware common authenticator.

7.3 Security requirements for routing set-up and packet delivery

The security requirements are described depending on the security dimensions and the threats posed by insider and outsider attacks [ITU-T X.1311]. When a route to the base station is set up, a routing metric such as the shortest path or delay can be used; furthermore, a cluster head or parent ID can be used as the routing metric on the defined routing topology and method. A reconstruction of the routing path is performed whenever the base station or sensors are moved, exhausted or there is a change of the head or parent node joining or leaving the sensor network.

- The base station and all sensors are required to check the authority of their neighbour nodes to determine which is the next node to communicate with the base station. If cluster heads or parent nodes are elected, node authentication for the representative is required to be performed to prevent a sinkhole attack by disguising the node.
- It is recommended that for routing configuration messages on routing information flooding, joining and leaving messages are required to be verified for integrity and source authority in a one-to-one manner. If a group is formed during the phase of neighbour discovery, the authentication key could be a group key for greater efficiency.
- Routing configuration messages containing ID, location and metric information are required to be protected by the encryption and key management methods.
- To provide fault-tolerance and avoid sinkhole or wormhole attacks, multi-paths for the base station can be optionally configured with different key materials for source and message authentication, and encryption.
- It is recommended that, after completing routing set-up, packets through the routing paths are recommended to be encrypted and authenticated using proper key management, encryption and authentication mechanisms. The encryption and authentication methods for sensors are more lightweight than those for the base station.
- When the data aggregation procedure is performed by cluster heads or parent nodes, key material and the methods for authentication and encryption of routing set-up or data delivery, can be optionally different in subgroups clustered by the heads or parents.

7.4 Security dimensions and requirements for secure routing

This clause defines the functions which satisfy the security requirements under performance considerations. The requirements are described using the classification of targets for security in Table 1. Also, this clause refers to security techniques used in ubiquitous sensor networks and specific security requirements for USNs in [ITU-T X.1311].

7.4.1 Base station and sensor aspects

The base station(s) could have an access control list with each secrecy value and ID of the sensors for initially checking their authentication and authorization together with the shared key information. The key could be pre-shared or generated by the secrecy value or third-party. Also, the

nodes could have an encryption ability for stored information. The base station(s) and some sensors for data aggregation should have secure storage for privacy and confidentiality. The key management, rekey and revocation of the group key could be required for authentication and authorization; this is the same for the unique key for each secured storage. In particular, if the base station is wire-lined, IPS/IDS functions could be provided.

A tamper-resistant module and trusted platform module for the nodes could be needed for hardware aspects.

Table 2 – Security dimensions and requirements

Security dimensions	Node-specific requirements					
	Encryption	**Key management**	**Secure storage**	**Initial access control, authentication, authorization**	**Tamper-proofed, TPM**	**IDS/IPS**
Access control				Y		
Authentication	Y	Y		Y		
Non-repudiation				Y		
Confidentiality	Y	Y	Y			
Communication security	Y	Y	Y			
Data integrity	Y					
Availability					Y	Y
Privacy	Y	Y	Y			
Resilience to attacks	Y				Y	Y

7.4.2 Neighbour discovery aspects

Authenticated advertisements should be broadcast. An authentication method is provided to initially send the advertisement. Here, ID information could be an authenticated anonymously or hidden within a continuously changing ID using a hash chain. In response, the registration message could be encrypted for protecting ID, location and routing metric information. Here, key material for packet delivery should be different from neighbour discovery to the routing set-up phase. Key management should include rekey and revocation procedures.

Table 3 – Security dimensions and requirements

Security dimensions	Neighbour discovery requirements				
	Encryption	**Key management**	**Source and message authentication**	**Data freshness**	**TPM, Fault-tolerant**
Access control			Y	Y	
Authentication		Y	Y	Y	
Non-repudiation			Y		
Confidentiality	Y	Y			
Communication security	Y	Y			

Table 3 – Security dimensions and requirements

Security dimensions	Neighbour discovery requirements				
	Encryption	**Key management**	**Source and message authentication**	**Data freshness**	**TPM, Fault-tolerant**
Data integrity			Y	Y	
Availability					Y
Privacy	Y	Y	Y		
Resilience to attacks					Y

7.4.3 Routing set-up and packet delivery aspects

Regarding the topological features, there are some parents or cluster heads election and join/leave procedures for routing set-up. While setting up the routes, ID, location and routing metrics should be hidden or encrypted and authenticated; therefore encryption, ID anonymous, and key management procedures should be provided. In particular, key management contains creation, rekey and revocation for each routing set-up and packet delivery.

Table 4 – Security dimensions and requirements

Security dimensions	Routing set-up and packet delivery requirements					
	Encryption	**Key management**	**Source and message authentication**	**Data freshness**	**Secure data aggregation**	**TPM, Fault-tolerant**
Access control			Y	Y		
Authentication		Y	Y	Y	Y	
Non-repudiation			Y			
Confidentiality	Y	Y			Y	
Communication security	Y	Y			Y	
Data integrity			Y	Y	Y	
Availability						Y
Privacy	Y	Y	Y		Y	
Resilience to attacks						Y

Appendix I

Overview of wireless sensor routing protocols

(This appendix does not form an integral part of this Recommendation.)

I.1 Examples of existing routing protocols

Many mechanisms have been proposed for the routing of sensor networks. These routing mechanisms have taken into consideration the inherent features of sensor networks along with application and topological requirements. The task of finding and maintaining routes in sensor networks, while considering energy consumption, effectiveness of routing, reliability of data, and security, is not trivial.

The following are the existing routing protocols.

- Sensor protocols for information via negotiation (SPIN) [b-Heinzelman] [b-Chandrakasan] and [b-Kulik]

  This refers to a family of adaptive protocols called sensor protocols for information via negotiation (SPIN) that disseminate all the information of each node to every node in the network assuming that all nodes in the network are potential base stations. This enables a user to query any node and obtain the required information immediately. These protocols make use of the property that nodes in close proximity have similar data, and hence there is a need to only distribute the data that other nodes do not possess.

- Directed diffusion [b-Intanagonwiwat]

  This refers to a popular data aggregation paradigm for WSNs, called directed diffusion. Directed diffusion is a data-centric (DC) and application-aware paradigm in the sense that all data generated by sensor nodes is named by attribute-value pairs. The main idea of the DC paradigm is to combine the data coming from different sources en route (in-network aggregation) by eliminating redundancy, minimizing the number of transmissions; thus saving network energy and prolonging its lifetime. Unlike traditional end-to-end routing, DC routing finds routes from multiple sources to a single destination that allows in-network consolidation of redundant data.

- Rumour routing [b-Braginsky]

  Rumour routing is a variation of directed diffusion and is mainly intended for applications where geographic routing is not feasible. In general, directed diffusion uses flooding to inject the query to the entire network when there is no geographic criterion to diffuse tasks. However, in some cases there is only a small amount of data requested from the nodes, and thus the use of flooding is unnecessary. An alternative approach is to flood the events if the number of events is small and the number of queries is large. The key idea is to route the queries to the nodes that have observed a particular event rather than flooding the entire network to retrieve information about occurring events. In order to flood events through the network, the rumour routing algorithm employs long-lived packets, called agents. When a node detects an event, it adds such an event to its local table, called events table, and generates an agent.

- MCFA [b-Ye]

  The MCFA (minimum cost forwarding algorithm) exploits the fact that the direction of routing is always known, that is, towards the fixed external base station. Hence, a sensor node need not have a unique ID or maintain a routing table. Instead, each node maintains the least cost estimate from itself to the base station. Each message to be forwarded by the sensor node is broadcast to its neighbours. When a node receives the message, it checks if it is on the least cost path between the source sensor node and the base station. If this is the

case, it re-broadcasts the message to its neighbours. This process is repeated until the base station is reached.

- Gradient-based routing [b-Schurgers]

  This refers to another variant of directed diffusion, called gradient-based routing (GBR). The key idea in GBR is to memorize the number of hops when *the interest* is diffused through the whole network. As such, each node can calculate a parameter called the height of the node, which is the minimum number of hops to reach the base station (BS).

- Information-driven sensor querying (IDSQ) and constrained anisotropic diffusion routing (CADR) [b-Chu]

  Two routing techniques, namely, information-driven sensor querying (IDSQ) and constrained anisotropic diffusion routing (CADR) were proposed in [b-Chu]. CADR aims to be a general form of directed diffusion. The key idea is to query sensors and route data in the network so that the information gain is maximized while latency and bandwidth are minimized. CADR diffuses queries by using a set of information criteria to select which sensors can get the data. This is achieved by activating only the sensors that are close to a particular event and dynamically adjusting data routes. The main difference between this mechanism and directed diffusion is the consideration of information gain in addition to the communication cost. In CADR, each node evaluates an information/cost objective and route data based on the local information/cost gradient and end-user requirements. In IDSQ, the querying node can determine which node can provide the most useful information with the additional advantage of balancing the energy cost. However, IDSQ does not specifically define how the query and the information are routed between sensors and the BS. Therefore, IDSQ can be seen as a complementary optimization procedure. Simulated results have shown that these approaches are more energy-efficient than directed diffusion where queries are diffused in an isotropic fashion and reach the nearest neighbours first.

- COUGAR [b-Yao]

  Another data-centric protocol called COUGAR, is named by author; it views the network as a huge distributed database system. The key idea is to use declarative queries in order to abstract query processing from the network layer functions such as the selection of relevant sensors and so on. COUGAR utilizes in-network data aggregation to obtain more energy saving. The abstraction is supported through an additional query layer that lies between the network and application layers. COUGAR incorporates an architecture for the sensor database system where sensor nodes select a leader node to perform aggregation and transmit the data to the BS. The BS is responsible for generating a query plan, which specifies the necessary information about the data flow and in-network computation for the incoming query and send it to the relevant nodes. The query plan also describes how to select a leader for the query. The architecture provides an in-network computation ability that can provide energy efficiency in situations where the generated data is huge. COUGAR has provided network-layer independent methods for data query.

- ACQUIRE [b-Sadagopan]

  This refers to a technique for querying sensor networks called active query forwarding in sensor networks (ACQUIRE). Similar to COUGAR, ACQUIRE views the network as a distributed database where complex queries can be further divided into several sub-queries. The operation of ACQUIRE can be described as follows. The BS node sends a query, which is then forwarded by each node receiving the query. During this process, each node tries to respond to the query partially by using its pre-cached information and then forwards it to another sensor node. If the pre-cached information is not up-to-date, the nodes gather information from their neighbours within a look-ahead of d hops. Once the query has been completely resolved, it is sent back through either the reverse or shortest-path to the BS.

Hence, ACQUIRE can deal with complex queries by allowing many nodes to send responses.

- Energy-aware routing [b-Shah]

  The objective of energy-aware routing protocol, a destination-initiated reactive protocol, is to increase the network lifetime. Although this protocol is similar to directed diffusion, it differs in the sense that it maintains a set of paths instead of maintaining or enforcing one optimal path at higher rates. These paths are maintained and chosen by means of a certain probability. The value of this probability depends on how low the energy consumption of each path can be achieved. By having paths chosen at different times, the energy of any single path will not deplete quickly. This can achieve longer network lifetime as energy is dissipated more equally among all nodes.

- Routing protocols with random walks [b-Servetto]

  The objective of the random walks-based routing technique is to achieve load balancing in a statistical sense and by making use of multi-path routing in WSNs. This technique considers only large scale networks where nodes have very limited mobility. In this protocol, it is assumed that sensor nodes can be turned on or off at random times. Furthermore, each node has a unique identifier but no location information is needed. Nodes were arranged so that each node falls exactly on one crossing point of a regular grid on a plane, but the topology can be irregular. To find a route from a source to its destination, the location information or lattice coordination is obtained by computing distances between nodes using the distributed asynchronous version of the well-known Bellman-Ford algorithm [b-Bellman]. An intermediate node would select as the next hop the neighbouring node that is closer to the destination according to a computed probability. By carefully manipulating this probability, some kind of load balancing can be obtained in the network. The routing algorithm is simple as nodes are required to maintain little state information. Moreover, different routes are chosen at different times even for the same pair of source and destination nodes.

- LEACH protocol [b-Heinzelman], [b-Chandrakasan]

  This introduces a hierarchical clustering algorithm for sensor networks, called low energy adaptive clustering hierarchy (LEACH). LEACH is a cluster-based protocol, which includes distributed cluster formation. LEACH randomly selects a few sensor nodes as cluster heads (CHs) and rotates this role to evenly distribute the energy load among the sensors in the network. In LEACH, the cluster head (CH) nodes compress data arriving from nodes that belong to the respective cluster, and send an aggregated packet to the base station in order to reduce the amount of information that must be transmitted to the base station. LEACH uses a TDMA (time division multiple access)/CDMA (code division multiple access) MAC to reduce inter-cluster and intra-cluster collisions. However, data collection is centralized and is performed periodically. Therefore, this protocol is most appropriate when there is a need for constant monitoring by the sensor network.

- Power-efficient gathering in sensor information systems (PEGASIS) [b-Lindsey]

  An enhancement over the LEACH protocol was proposed. The protocol, called power-efficient gathering in sensor information systems (PEGASIS), is a near optimal chain-based protocol. The basic idea of the protocol is that in order to extend network lifetime, nodes need only communicate with their closest neighbours and they take turns in communicating with the base station. When the round of all nodes communicating with the base station ends, a new round will start and so on. This reduces the power required to transmit data per round as the power draining is spread uniformly over all nodes.

- Threshold-sensitive energy-efficient sensor network protocols (TEEN) and adaptive periodic threshold-sensitive energy-efficient sensor network protocol (TEEN and (APTEEN), [b-Manjeshwar-1] and [b-Manjeshwar-2].

Two hierarchical routing protocols called TEEN (threshold-sensitive energy-efficient sensor network protocol), and APTEEN (adaptive periodic threshold-sensitive energy-efficient sensor network protocol) are proposed respectively. These protocols were proposed for time-critical applications. In TEEN, sensor nodes sense the medium continuously, but the data transmission is done less frequently. A cluster head sensor sends its members a hard threshold, which is the threshold value of the sensed attribute and a soft threshold, which is a small change in the value of the sensed attribute that triggers the node to switch on its transmitter and transmit. Thus, the hard threshold tries to reduce the number of transmissions by allowing the nodes to transmit only when the sensed attribute is in the range of interest.

APTEEN is a hybrid protocol that changes the periodicity or threshold values used in the TEEN protocol according to user needs and the type of the application. In APTEEN, the cluster-heads broadcasts attributes, thresholds, schedule, and count time. The node senses the environment continuously, and only those nodes which sense a data value at or beyond the hard threshold transmit.

- Small minimum energy communication network (MECN) [b-Rodoplu]

  A protocol is proposed that computes an energy-efficient subnetwork, namely the minimum energy communication network (MECN) for a certain sensor network by utilizing a low power global positioning system (GPS). MECN identifies a relay region for every node. The relay region consists of nodes in a surrounding area where transmitting through those nodes is more energy-efficient than direct transmission.

- Self-organizing protocol (SOP) [b-Subramanian]

  This describes a self-organizing protocol and an application taxonomy that was used to build architecture used to support heterogeneous sensors. Furthermore, these sensors can be mobile or stationary. Some sensors probe the environment and forward the data to a designated set of nodes that act as routers. Router nodes are stationary and form the backbone for communication. Collected data are forwarded through the routers to the more powerful BS nodes. Each sensing node should be able to reach a router in order to be part of the network. A routing architecture that requires the addressing of each sensor node has been proposed. Sensing nodes are identifiable through the address of the router node they are connected to. The routing architecture is hierarchical where groups of nodes are formed and merge when needed. The local Markov loops (LML) algorithm, which performs a random walk on spanning trees of a graph, was used to support fault tolerance and as a means of broadcasting.

- Sensor aggregates routing [b-Fang]

  A set of algorithms for constructing and maintaining sensor aggregates were proposed. The objective is to collectively monitor target activity in a certain environment (target tracking applications). A sensor aggregate comprises those nodes in a network that satisfy a grouping predicate for a collaborative processing task.

  Three algorithms were proposed in [b-Fang]. The first algorithm is a lightweight protocol, distributed aggregate management (DAM), for forming sensor aggregates for a target monitoring task. The protocol comprises a decision predicate P for each node to decide if it should participate in an aggregate, and a message exchange scheme M for which it determines how the grouping predicate is applied to nodes. A node determines if it belongs to an aggregate based on the result of applying the predicate to the data of the node as well as information from other nodes. Aggregates are formed when the process eventually converges.

The second algorithm, energy-based activity monitoring (EBAM) algorithm, estimates the energy level at each node by computing the signal impact area, combining a weighted form of the detected target energy at each impacted sensor assuming that each target sensor has an equal or constant energy level.

The third algorithm, expectation-maximization like activity monitoring (EMLAM), removes the constant and equal target energy level assumption. EMLAM estimates the target positions and signal energy using received signals, and uses the resulting estimates to predict how signals from the targets may be mixed at each sensor. This process is iterated, until the estimate is sufficiently good.

- RPL: IPv6 routing protocol for low- power and lossy networks [b-IETF RFC 6550]

  RPL organizes a topology as a directed acyclic graph (DAG) that is partitioned into one or more destination oriented DAGs (DODAGs). RPL works on two different layers; packet processing and forwarding, and routing optimization. Furthermore, RPL has three security options: unsecured, pre-installed key and authenticated. Pre-installed keys enable the nodes to process and generate secure RPL messages. With the authenticated option, nodes can join as leaves using only the pre-installed key. Joining as a router requires obtaining a key from an authenticated authority. Here in 'unsecured' mode, there is no security mechanisms applied.

Bibliography

[b-ITU-T Y.2221] Recommendation ITU-T Y.2221 (2010), *Requirements for support of ubiquitous sensor network (USN) applications and services in the NGN environment*.

[b-IEEE 802.16.2] IEEE 802.16.2™ (2004), *Recommended Practice for Local and metropolitan area networks: Coexistence of Fixed Broadband Wireless Access Systems*, IEEE.

[b-IETF RFC 6650] IETF RFC 6550 (2012), RPL: IPv6 Routing Protocol for Low-Power and *Lossy Networks*.

[b-ISO/IEC 11889-1] ISO/IEC 11889-1 (2009), *Information technology – Trusted Platform Module – Part 1: Overview*.

[b-Bellman] Bellman, R. (1958), *On a route problem,* Quarterly of Applied Mathematics Vol. 16, pp. 87-90.

[b-Braginsky] Braginsky, D., and Estrin, D. (2002), *Rumor routing algorithm for Sensor Networks,* Proceedings of the First Workshop on Sensor Networks and Applications (WSNA), Atlanta, GA.

[b-Chandrakasan] Heinzelman, W. R., Chandrakasan, A., and Balakrishnan, H. (2000), *Energy-efficient communication protocol for wireless microsensor networks*, Proceedings of the 33rd Annual Hawaii International Conference on System Sciences (HICSS'00).

[b-Chu] Chu, M., Haussecker, H., and Zhao, F. (2002), *Scalable Information-Driven Sensor Querying and Routing for Ad Hoc Heterogeneous Sensor Networks*, The International Journal of High Performance Computing Applications, Vol. 16, No. 3, pp. 293-313.

[b-Fang] Fang, Q., Zhao, F., and Guibas, L. (2003), *Lightweight sensing and communication protocols for target enumeration and aggregation*, Proceedings of the 4th ACM international symposium on Mobile ad hoc networking and computing (MOBIHOC), pp. 165-176.

[b-Heinzelman] Heinzelman, W., Kulik, J., and Balakrishnan, H. (1999), *Adaptive Protocols for Information Dissemination in Wireless Sensor Networks*, Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking (MobiCom'99), pp. 174-85, Seattle, WA.

[b-Intanagonwiwat] Intanagonwiwat, C., Govindan, R., and Estrin, D. (2000), *Directed diffusion: a scalable and robust communication paradigm for sensor networks*, Proceedings of the 6th annual international conference on Mobile computing and networkingMobiCom'00, pp. 56-67, Boston, MA.

[b-Kulik] Kulik, J., Heinzelman, W.R., and Balakrishnan, H. (2002), *Negotiation-based protocols for disseminating information in wireless sensor networks*, Wireless Networks, Vol. 8, No. 2/3, pp. 169-185.

[b-Lindsey] Lindsey, S., and Raghavendra, C. (2002), *PEGASIS: Power-efficient gathering in sensor information systems*, Aerospace Conference Proceedings, IEEE, Vol. 3, pp. 1125-1130.

[b-Manjeshwar-1] Manjeshwar, A., and Agarwal, D.P. (2000), *TEEN: a routing protocol for enhanced efficiency in wireless sensor networks*, Parallel and Distributed Processing Symposium, Proceedings 15th International, pp. 2009-2015.

[b-Manjeshwar-2] Manjeshwar, A., and Agarwal, D.P. (2002), *APTEEN:a hybrid protocol for efficient routing and comprehensive information retrieval in wireless sensor networks*, Parallel and Distributed Processing Symposium, Proceedings International, IPDPS, pp. 195-202.

[b-Rodoplu] Rodoplu, V., and Meng, T.H. (1999), *Minimum Energy Mobile Wireless Networks*, IEEE Journal Selected Areas in Communications, Vol. 17, No. 8, August, pp. 1333-1344.

[b-Sadagopan] Sadagopan, N. Krishnamachari, B., and Helmy, A. (2003), *The ACQUIRE mechanism for efficient querying in sensor networks*, in the Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications, Anchorage, Alaska, May.

[b-Schurgers] Schurgers, C., and Srivastava, M.B. (2001), *Energy efficient routing in wireless sensor networks*, Military Communications Conference, 2001. MILCOM 2001. Communications for Network-Centric Operations: Creating the Information Force. IEEE, Vol.1, pp. 357-361.

[b-Servetto] Servetto, S., and Barrenechea, G. (2002), *Constrained random walks on random graphs: routing algorithms for large scale wireless sensor networks*, Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications, pp. 12-21, Atlanta, Georgia, USA.

[b-Shah] Shah, R.C., and Rabaey, J. (2002), *Energy aware routing for low energy ad hoc sensor networks*, Wireless Communications and Networking Conference (WCNC), March, IEEE, Orlando, FL.

[b-Subramanian] Subramanian, L., and Katz, R.H. (200), *An architecture for building self-configurable systems*, Proceedings of the 1st ACM international symposium on Mobile ad hoc networking & computing, MobiHoc '00, August, Boston, MA.

[b-Yao] Yao, Y., and Gehrke, J. (2002), *The cougar approach to in-network query processing in sensor networks*, ACM SIGMOD Record, Vol. 31, No. 3, pp. 9-18.

[b-Ye] Ye, F., Chen, A., Liu, S., and Zhang, L. (2001), *A scalable solution to minimum cost forwarding in large sensor networks*, Proceedings of the tenth International Conference on Computer Communications and Networks (ICCCN), pp. 304-309.

[b-Zigbee] Zigbee, <http://www.zigbee.org/Standards/Downloads.aspx>.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2013