ALERT-2
Requirements Specification

Draft Version 0.1
August 25, 2007

Timothy J. Salo
Salo IT Solutions, Inc.
1313 5th Street SE
Minneapolis, MN 55414-4504
salo <at> saloits <dot> com
612-605-6896

This material is based upon work supported by the Department of Commerce under contract number DG133R07-CN-0175. Any opinions, findings, conclusions or recommendations expressed in this publication are those of the author and do not necessarily reflect the views of the Department of Commerce.

Contents

1. Overview

The ALERT-2 protocol suite is a collection of next-generation wireless communication protocols for use in automated flood warning systems (AFWS). The ALERT-2 protocols are expected to provide an alternative to, and to eventually replace, the original ALERT protocol. While the original ALERT protocol is widely deployed, it has a number of limitations.

This document identifies the requirements for the ALERT-2 protocols. It includes "product requirements", high-level requirements that specify the services that the ALERT-2 protocols should provide or other externally visible behaviors that the ALERT-2 protocols should exhibit, and "functional requirements", more detailed requirements that specify how the ALERT-2 protocols may provide the desired services or other behaviors.

This document is available for public review on the ALERT-2 project Web site (http://www.alert-2.com). All versions of this document can be found on the ALERT-2 "Project Documents" page (http://www.alert-2.com/documents.html).

Widespread review of, discussion about, and comments on these requirements will help strengthen this document. A public e-mail list, the "ALERT-2 Requirements Discussion" list, has been created to host online discussions about this document. Anyone may participate in these discussions. Visit the ALERT-2 "Mailing Lists" Web page (http://lists.alert-2.com/mailman/listinfo) to subscribe to this list or to view the list archives. Alternatively, some readers may wish to discuss this material on the Yahoo! "Flood Warning and Flood Warning Systems (Floodsystems)" group. Also feel free to contact the author of this document, Timothy J. (Tim) Salo, at 612-605-6896 or salo <at> saloits <dot> com if you have any questions, comments, or suggestions about the requirements for the ALERT-2 protocols.

Ideally, the final version of this document will reflect a consensus of the automated flood warning systems community, including users of flood warning information, flood warning system operators, government agencies responsible for flood warnings and flood warning systems, and vendors. All of the review comments will be addressed, either by revising the relevant sections of the document, or by explaining why no change was made to the document. Areas where consensus has not been achieved will be identified.

This document is a product of the *ALERT-2 Protocol Development* project, an SBIR Phase I contract awarded to Salo IT Solutions, Inc. (SaloITS) by NOAA. An "ALERT-2 Protocol Specification" document will also be created by this project.

2. ALERT-2 Network Components

This section provides some concepts and language that will facilitate discussions about the requirements for the ALERT-2 protocols. Note that this material does *not* specify requirements for the ALERT-2 protocols or describe the design of the ALERT-2 protocols.

2.1 ALERT-2 Networks

Figure 1 illustrates the configuration of a typical ALERT-2 network. The ALERT-2 network is composed of a number of *network nodes*, or simply *nodes*, namely devices that implement the ALERT-2 wireless communication protocols and use them to communicate with each other.

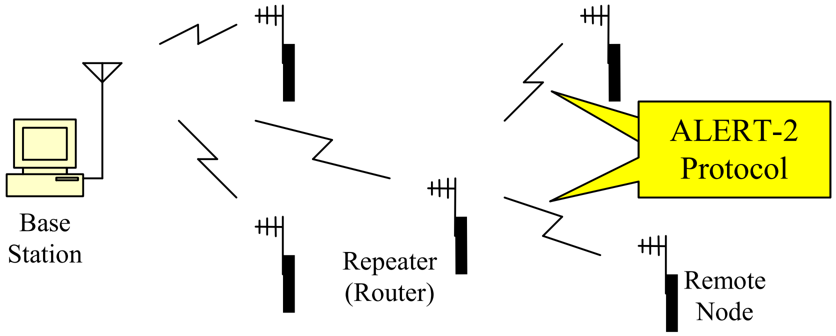

Figure 1. A Typical ALERT-2 Network

The *base station* is the destination towards which the network forwards packets containing sensor data. It is also the node within an ALERT-2 network that is generally responsible for the overall operation of the network. The *remote nodes* collect sensor data and forward them towards the base station. *Repeaters* (or *routers*) receives packets from other remote nodes and transmit them towards the base station (a process called *forwarding*). Routers permit an ALERT-2 network to be larger than the transmission range of individual remote nodes.

2.2 ALERT-2 Software Applications

The ALERT-2 protocol specification will use the concept of a *software application*. Software applications are, from the perspective of the ALERT-2 protocols, the sources and destinations of data – the purpose of an ALERT-2 network is to transport data between software applications on different nodes. A software application is software that executes in a node, performs a specific set of related functions, and uses the ALERT-2 protocols to communicate with applications on other nodes. A node may have several applications, such as a rain gauge reporting application that forwards rain gauge data to the base station, a file transfer application that transfers new software into the remote node, and a network management application that reports the status of the remote node hardware to the base station.

The figure below illustrates how applications use the services provided by the ALERT-2 protocols to communicate with each other and how the ALERT-2 protocols provide services to several applications within a node.

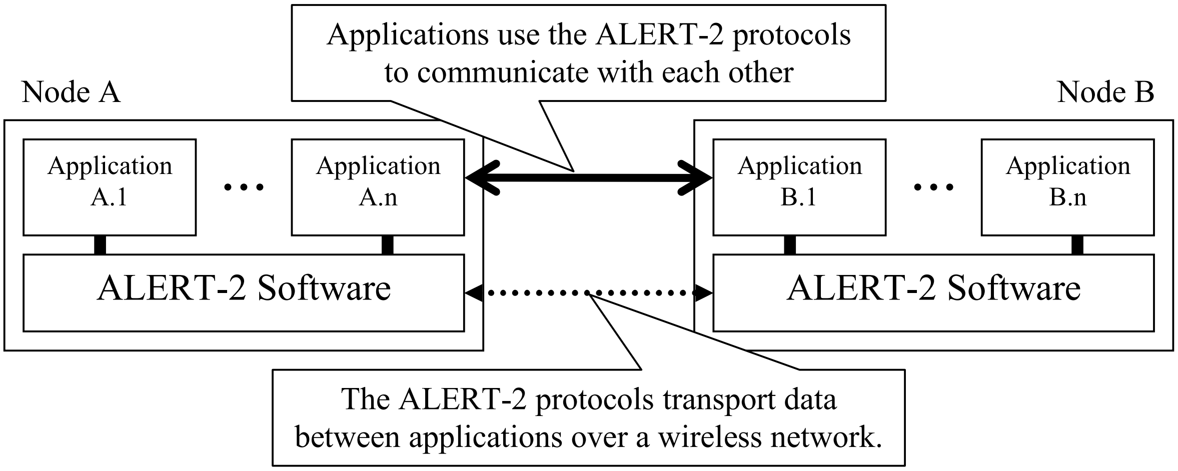
Applications use the ALERT-2 protocols to communicate with each other
Node A
Node B
Application A.1
Application A.n
Application B.1
Application B.n
ALERT-2 Software
ALERT-2 Software
The ALERT-2 protocols transport data between applications over a wireless network.

Figure 2. ALERT-2 Applications.

This model of the ALERT-2 protocols providing generic services to multiple applications provides considerable flexibility. The underlying ALERT-2 protocols are not aware of the format of the data exchanged between applications or of the protocols used by applications. As a result, existing applications can be modified and new applications can be created without making changes to the services provided by the ALERT-2 protocols.

2.3 ALERT-2 Protocol Layers

The functions that are to be performed by the ALERT-2 protocols can be categorized into a number of "protocol layers", where a particular protocol layer provides services to the protocol layer above it and uses services provided by the protocol layer below it. This categorization is presented here solely to offer a framework for discussions about the requirements for the ALERT-2 protocols. The actual ALERT-2 protocols may have an entirely different structure. The hypothetical ALERT-2 protocol layers are described below, starting with the lowest protocol layer.

2.3.1 ALERT-2 Physical Protocol

The ALERT-2 physical protocol is responsible for transmitting bits over a radio frequency (RF) channel. This function is generally implemented in a modem or digital signal processing software.

The original ALERT physical protocol transmitted data at 300 bits-per-second (bps).

The ALERT-2 physical protocol is expected to be based on the 4800 bps modem with forward-error-correction (FEC) capabilities that is being developed by Blue Water Design LLC.

2.3.2 ALERT-2 Media Access Control (MAC) Protocol

The ALERT-2 media access control (MAC) protocol is responsible for determining which node can access (i.e., transmit on) the RF channel at a particular time. Most MAC protocols include features that reduce or eliminate "collisions", simultaneous transmissions by two or more nodes that interfere with each other and as a result prevent the transmitted packets from being successfully received.

The original ALERT protocol essentially had no MAC protocol. Each node transmitted data without regard to any external factors, such as whether another node might be transmitting at the same time. This strategy is known as the "pure ALOHA protocol". Unfortunately, the maximum throughput of the pure ALOHA protocol is about 18%, (i.e., the bandwidth used by the successfully received packets is at most about 18% of the total available bandwidth)[1]. As the rate at which packets are transmitted increases, collisions between packets increase; if the rate at which packets are transmitted is high enough, no packets are successfully received. This is undoubtedly the cause of the large number of lost packets that are experienced in ALERT networks during major rain events.

2.3.3 ALERT-2 Link Protocol

The ALERT-2 link protocol is responsible for the orderly, error-free transmission of packets between two adjacent nodes. Link protocols generally include mechanisms that detect and discard packets that are damaged by transmission errors. Some link protocols retransmit packets that are not successfully received.

The original ALERT protocol transmitted four-byte packets, but otherwise provided only minimal link-layer functionality. It offered extremely limited protection against transmission errors, and so many damaged packets were processed rather than discarded.

2.3.4 ALERT-2 Network Protocol

The ALERT-2 network protocol is responsible for the end-to-end transmission of packets through a network, which may include one or more intermediate nodes (routers) that forward packets towards their destinations. The function of the ALERT-2 network protocol is roughly analogous to that of the Internet Protocol (IP) in the Internet protocol suite.

The original ALERT protocol did not include a network protocol. Repeaters did, however, retransmit packets in an effort to increase the size of ALERT networks.

2.3.5 ALERT-2 Transport Protocols

The ALERT-2 transport protocols are responsible for the end-to-end transmission of data. While many types of transport protocols have been designed, the most common types are unreliable datagram transport protocols and reliable stream transport protocols. An unreliable datagram transport protocol is an extremely limited protocol, which simply transmits a packet in hopes that

[1] See, for example: Tanenbaum, Andres S., *Computer Networks 4e*, Prentice Hall PTR, 2003, pp 251-254.

it will be successfully received by the destination node. The Internet User Datagram Protocol (UDP) is an unreliable datagram protocol. A reliable stream transport protocol ensures that a sequence of bytes, packets or messages is successfully received in the proper order by the destination node. This type of transport protocol typically retransmits data that are not successfully received. The Internet Transmission Control Protocol (TCP) is the most common reliable byte stream transport protocol.

The original ALERT protocol did not include a transport protocol.

2.3.6 ALERT-2 Application Protocols

The ALERT-2 application protocols are responsible for the end-to-end transport of application data, information that is of interest to applications. The Internet includes many different standard application protocols, and uncounted non-standard application protocols. Examples of standard Internet application protocols include the Hypertext Transport Protocol (HTTP), the File Transfer Protocol (FTP), and the Simple Mail Transfer Protocol (SMTP).

The original ALERT protocol could be considered to an application protocol that includes a little bit of functionality that is usually implemented at other protocol layers.

3. ALERT-2 Product Requirements

This section identifies the product requirements for the ALERT-2 protocols. These are high-level requirements that specify the services that the ALERT-2 protocols should provide or other externally visible behaviors that the ALERT-2 protocols should exhibit.

3.1 Equipment Requirements

The ALERT-2 protocols assume that remote nodes are capable of receiving packets as well as transmitting packets. This contrasts with the original ALERT protocol, which implicitly assumes that remote nodes will only transmit packets, but that remote nodes do not need to be able to receive packets.

The ALERT-2 protocols should:

- **Support bidirectional communication.** The ALERT-2 protocols should permit remote nodes to receive, as well as transmit, packets. The protocols should also enable remote nodes to receive data (e.g., application data) as well as to originate data.

- **Not *require* remote nodes to receive.** The ALERT-protocols should operate, perhaps with a significant loss of functionality, in networks in which remote nodes can not receive packets.

3.2 Performance Requirements

The ALERT-2 protocols should:

- **Provide enhanced throughput.** The ALERT-2 protocols should ensure that a larger number of messages can be transmitted per hour than is possible with the original ALERT protocol. They should ensure that at least TBD messages per hour can be successfully transmitted on a single RF channel.

- **Ensure better channel utilization.** The ALERT-2 protocols should ensure that channel utilization of at least TBD percent can be achieved, where utilization is measured as the number of bits of link-layer payload data successfully received compared to the raw bandwidth.

- **Support larger networks.** The ALERT-2 protocols should support networks that include up 1023 nodes.

- **Support more sensors.** The ALERT-2 protocols should not limit the number of sensors that an individual node can support or that a network can support (although applications and application protocols may impose limits on the number of sensors that they can support).

- **Support more software applications.** The ALERT-2 protocols should support at least 255 software applications per node (e.g., a rain gauge reporting application, a network management application, etc.).

- **Support more networks per channel.** The ALERT-2 protocols should permit up to 15 networks to share a single RF channel (where a network is a base station and the remote nodes that forward sensor data towards that base station).

- **Ensure minimum latency.** The ALERT-2 protocols should ensure that the network latency is less than TBD seconds, as measured between the time that a remote station has data to transmit and the time that those data are received by the base station.

3.3 Reliability Requirements

The ALERT-2 protocols should:

- **Reduce or eliminate packet loss due to congestion.** The ALERT-2 protocols should be able to prevent, at least at certain times or for certain types of data, packets from being lost because more than one node tries to transmit at the same time.

- **Detect and discard packets that contain transmission errors.** The ALERT-2 protocols should prevent damaged packets from being forwarded to applications or otherwise being processed.

- **Minimize the number of packets that are lost as a result of congestion or transmission errors.** The ALERT-2 protocols should, optionally and when appropriate, retransmit packets that are not successfully received.

3.4 Naming and Addressing Requirements

The ALERT-2 protocols should:

- **Ensure that every ALERT-2 node is assigned a permanent, globally unique identifier.** The globally unique identifier should be assigned by the vendor, and could be similar to an IEEE MAC address. Software on the local node should be able to read this identifier. A node should be able to ask another node for its globally unique identifier.

- **Permit every ALERT-2 node to be configured with a text identifier.** Each node should have an identifier that can be configured by the network administrator. This identifier should be a text string with some reasonable minimum length. Software on the local node should be able to read this identifier, and a node should be able to ask another node for its text identifier.

- **Use a short address for most purposes.** The ALERT-2 protocols should use short addresses (e.g., 16-bits) that are unique only within a network, in order to save bandwidth and energy.

3.5 Application Services Requirements

The purpose of an ALERT-2 network is to transport data between software applications that reside on different nodes. Software applications are the ultimate source and destination of most information transmitted by an ALERT-2 network.

The ALERT-2 protocols should:

- **Permit a specific application to be addressed.** The ALERT-2 protocols should permit data to be addressed for delivery to a specific application on a particular node. For example, an application may request an ALERT-2 network to forward data to the network management application on node 216.

- **Support multiple applications.** The ALERT-2 protocols should support multiple software applications within a node (e.g., a rain gauge sensor application, a file transfer application, etc.). Each application may be the source or destination of data, or both.

- **Support multiple application protocols.** The ALERT-2 protocols should permit each application to potentially use a different application protocol (all of which use the services provided by the ALERT-2 protocols).

- **Provide a datagram service.** The ALERT-2 protocols should forward through the network a single packet that contains application-provided information (a datagram). The ALERT-2 protocols should make reasonable efforts to ensure that the datagram is successfully received by the application to which it is sent. This is a generalization of the service provided by the original ALERT protocol.

- **Provide a reliable transport service.** The ALERT-2 protocols should reliably transport through the network a sequence of bytes (e.g., a file). All of the bytes provided by the sending application should be received by the destination application, in order, and without any of the bytes being corrupted. This service should transport any type of data (e.g., binary files, such as new software or images, or text files, such as log files or configuration files).

3.6 Application Protocol Requirements

Software applications will implement application protocols, which will use the services provided by the underlying ALERT-2 protocols (e.g., the datagram service and the reliable transport service). Many of the product requirements for the application protocols are specific to the particular application (e.g., a rain gauge application should use engineering units, rather than raw sensor data).

Future versions of this document will include requirements for at least some application protocols.

3.7 Interoperability and Compatibility Requirements

The ALERT-2 protocols should:

- **Ensure interoperability between implementations and vendors.** The ALERT-2 protocol specification should be written with the clarity and level of detail necessary to ensure that products that conform to the specification will be assured of interoperating with each other.

- **Share an RF channel with the original ALERT protocol.** However, significant ALERT-2 functionality may not be available in mixed ALERT/ALERT-2 networks.

- **Support existing transmitters and transceivers.** However, significant ALERT-2 functionality may not be available in networks in which some nodes do not receive packets.

3.8 Extensibility Requirements

The ALERT-2 protocols should:

- **Permit new versions of the ALERT-2 protocol to be deployed incrementally.** That is, it should be possible to deploy a new version of the ALERT-2 protocols one node at a time in an ALERT-2 network, rather than upgrading all of the nodes at the same time.

- **Permit new applications and new application protocols to be deployed without changes to the underlying ALERT-2 protocols.**

3.9 Network Administration and Management Requirements

The ALERT-2 protocols should:

- **Support remote network management.** The ALERT-2 protocols should enable an ALERT-2 network to be managed from the base station. Specifically, the need to physically visit a remote node to manage the network (e.g., to upgrade or reconfigure the software in the remote node) should be eliminated.

- **Permit passive base stations.** The ALERT-2 protocols should enable additional base stations to passively monitor the traffic on an ALERT-2 network.

- **Support base station fail-over.** The ALERT-2 protocols should permit a second base station to assume the responsibility for network, in the event that the primary base station fails.

- **Support automatic base station fail-over.** The ALERT-2 protocols should ensure that an available back-up base station automatically assumes responsibility for an ALERT-2 network, without the need for human intervention, in the event that the primary base station fails.

- **Minimize manual configuration**. The ALERT-2 protocols should, wherever practical, avoid requiring manual configuration. That is, the ALERT-2 protocols should configure themselves wherever practical.

- **Configure routers and routing automatically**. Routers in an ALERT-2 network should configure themselves, without the need for manual configuration. Routers should reconfigure themselves, in the event that a router or a link fails or becomes unreliable.

3.10 Energy Conservation Requirements

Energy conservation is an important objective in many ALERT-2 networks, because many remote nodes are powered by batteries that are recharged by solar panels. The ALERT-2 protocols should:

- **Permit remote nodes to sleep.** The ALERT-2 protocols should permit remote nodes to sleep for long periods of time, although base stations and routers may be expected to be active and prepared to receive and transmit packets all of the time.

- **Operate with limited computational power and storage capacity.** The ALERT-2 protocols should not require remote nodes to have substantial computational power or storage capacity.

3.11 Security Requirements

The ALERT-2 protocols should:

- **Optionally ensure the integrity of data.** That is, the protocols should optionally ensure that data packets have not been altered or otherwise tampered with.

- **Optionally prevent disclosure of data.** That is, the protocols should optionally prevent unauthorized parties from receiving (at least in any understandable form) data transported by the network.

- **Optionally ensure that the source of data is identified.** That is, the protocols should optionally ensure that data actually originated from the node that claims to have sent it.

- **Optionally ensure that data packets cannot be replayed.** That is, the protocols should optionally ensure that packets that were transmitted at some previous time cannot be transmitted at a later time without being detected.

- **Optionally authenticate users or applications.** For example, the protocols may optionally ensure that a person or application is actually who it claims to be.

- **Optionally authorize operations.** For example, the protocols may optionally determine which users, applications or nodes are permitted to load new software into a remote node.

3.12 Intellectual Property Requirements

The ALERT-2 protocol should:

- **Permit implementation without paying fees.** Vendors should be free to implement the ALERT-2 protocols without paying for the right to implement or use the protocol.

4. ALERT-2 Functional Requirements

The ALERT-2 functional requirements are more detailed or more technical requirements. For the most part, they are refinements of or derived from the ALERT-2 product requirements.

This material will be included in future versions of this document.