Network Working Group
Internet-Draft
Intended status: Informational
Expires: August 22, 2013

J. Nguyen
R. Cole
U.S. Army CERDEC
U. Herberg
Fujitsu Laboratories of America
J. Yi
LIX, Ecole Polytechnique
J. Dean
Naval Research Laboratory

February 18, 2013

Network Management of Mobile Ad hoc Networks (MANET): Architecture, Use Cases, and Applicability
draft-nguyen-manet-management-00

Abstract

This document aims at providing an extended architecture, use case and applicability statement for management of MANETs, as a guideline for how to manage MANETs. This document describes different management activities, such as network configuration, monitoring of state, monitoring of performance, fault management, and software upgrades. Different aspects of a MANET management architecture are illustrated (e.g., distributed vs. centralized management, flat vs. hierarchical management, management of an entire network vs. an individual router, etc.) and contrasted to the NMS architecture in the Internet. A desciption of typical MANET use cases relevant for management is followed by an overview of current standard management protocols that can be used in MANETs.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

MANET routing protocols are commonly assumed to be entirely self-managing: routers, running such a protocol, perceive the topology of the MANET by means of control message exchange. Any change to the topology is reflected in the local routing tables of each router after a bounded convergence time, which allows forwarding of data traffic towards its intended destination. Usually, no human interaction is required, as all variable parameters required by the routing protocol are either negotiated in the control traffic exchange, or are only of local importance to each router (i.e. do not influence interoperability).

However, external management and monitoring of a MANET routing protocol may be desirable to optimize parameters of the routing protocol. Such an optimization may lead to a more stable perceived topology and to a lower control traffic overhead, and therefore to a higher delivery success ratio of data packets, a lower end-to-end delay, and less unnecessary bandwidth and energy usage. Such optimizations facilitate to scale the network to a large number of routers.

In the following, requirements for MANET management are illustrated using an example, the Optimized Link State Routing Protocol version 2 [I-D.OLSRv2]: Fundamentally, the only parameter upon which agreement is required between OLSRv2 routers is C - a constant, used to fix the scale and granularity of validity and interval time values, as included in protocol control messages. [RFC5497] proposes a value for this constant; the symbol C is chosen to indicate it to be a "constant of nature" inside an OLSRv2 network, to which all routers must adhere. As control messages carry validity time and interval time values, a recipient OLSRv2 router can behave appropriately, even if it uses vastly different values itself, as long as the recipient and sender use the same value for C.

Link admittance, by way of the hysteresis values and link quality estimation, requires no agreement; these are used for an individual router to determine a suitable threshold for "considering that a link could be a candidate for being advertised as usable". Still, external monitoring and management may be desirable in an OLSRv2 network. A network may benefit from having its control message emission tuned according to the network dynamics: in a mostly static network, i.e. a network in which the topology remains stable over long durations, the control message emission frequency could be decreased in order to consume less bandwidth or less energy. Conversely, of course, in a highly dynamic network, the emission frequency could be increased from improved responsiveness. Concerning the hysteresis and link quality estimation, a management application might detect a region of an OLSRv2 network with a high link density - but also a high degree of "flapping": links coming "up" (SYM) only to disappear as LOST shortly thereafter. Detecting such behavior, on a global level and for multiple routers in the same region, could enable appropriately "tuning" the thresholds towards more stable links and, thus, a more stable routing structure in the network.

These are but two examples, and have as common that a more "global view" of the network, than that of a single OLSRv2 router, is required - i.e. entail that a Network Management System is able to inquire as to various performance values of the network, and to set various router parameters.

1.1. Objective of this Document

As MANETs are a relatively new kind of network, experience with large-scale deployments, and in particular management of such deployments, is limited. This document aims at providing an extended architecture, use case and applicability statement for management of MANETs, as a guideline for how to manage MANETs. This document describes different management activities, such as network configuration, monitoring of state, monitoring of performance, fault management, and software upgrades. Different aspects of a MANET management architecture are illustrated (e.g., distributed vs. centralized management, flat vs. hierarchical management, management of an entire network vs. an individual router, etc.) and contrasted to the NMS architecture in the Internet. A desciption of typical MANET use cases relevant for management is followed by an overview of current standard management protocols that can be used in MANETs.

A related document that discusses other use cases and requirements of constrained networks and constrained devices (not focused on MANETs) is currently being developed in [I-D.ersue-constrained-mgmt].

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

3. Challenges and Problem Statement

Management of MANETs is more difficult than in the Internet, for multiple reasons. This section outlines these challenges for management of MANETs.

3.1. [CLG1] Distributed Ownership

Depending on the user case, there may not be a network administrator of the MANET, e.g., in the use case of Section 7.3, where each inhabitant owns its own router. This means that the router may be completely protected against external access, or at least only allows limited access to it. Moreover, there may be issues of privacy, but these are out of scope of this document.

3.2. [CLG2] Ad Hoc Topology

As the topology of a MANET may frequently change over time, no a priori topology planning is possible for the network administrator. Therefore, new routers may join at any time, and other may leave. This leads to a change of topology as well as IP addresses, depending on the IP address allocation policy or mechanism.

Depending on the routing protocol used in the MANET, it may not be known to a network management station which IP addresses are available in the network, e.g., when using a reactive protocol, which only discovers routes on demand. Moreover, because of changes of the topology, it is possible that there is no route between two MANET routers because they are in different connected components of the network graph representing the network topology.

3.3. [CLG3] Infrastructureless

In some use cases of MANETs, such as descibed in Section 7.3, there may not be a "controller" or "server". Even if there is, connectivity may be interrupted because of the ad hoc topology, described above. This entails that a distributed management may be desired instead of a centralized one. Routers could, e.g., monitor their neighbors and report failures on behalf of them once they have connectivity to a logging station; or they keep that information locally until requested by a user remotely. A decentralized management may lead to an increased coordination complexity. For example, it needs to be defined to which NMS notifications are sent from routers.

3.4. [CLG4] Network Performance

Whereas in classical network management of the Internet, administrators typically connect to a single router in order to configure parameters or to monitor its performance, MANETs may have performance problems because of a whole group of malconfigured routers. Also, the performance measures of a larger number of routers may be more relevant than that of a single router. In order to do that, different protocols would need to be used to manage a region of a network (e.g., using multicast connections, collection trees etc.)

Typically in wired networks, performance monitoring is accomplished through periodic polling for state and counter data, from which performance reports are generated. In MANETs, due to dynamics, individual routers may be disconnected from a management station handling the periodic polling for performance data. Hence, architectures need to be developed which allow for remote control of reporting functions, but local generation of performance reports to allow for continuous collection during periods of disconnection.

3.5. [CLG5] Low Bandwidth / Lossy Channel

Due to the nature of wireless channels, bandwidths may be far lower than in the Internet, and packet loss rates orders of magnitude higher. In terms of management applications requiring delivery of large volumes of data, e.g., new configuration files or software upgrades, may not be viable if running over reliable transport protocols. Standard TCP implementations are known to have poor performance characteristics in lossy MANETs.

4. Management Functions

This section describes several management activities that are relevant for management of networks in general (not only MANETs).

4.1. [ACT1] Network Configuration

Section 1 gives an example for network configuration for OLSRv2. Most network protocols allow for setting parameters, e.g., message intervals, timeouts, metric types, security parameters etc. These parameters can affect interoperability of the protocols, as well as protocol performance and efficiency. Managing such parameters remotely allows quick updates of parameters remotely, e.g., as a reaction to a change in topology by changing message intervals as described in the example in Section 1.

4.2. [ACT2] Monitoring of State

Many network protocols maintain state during operation. For example for routing protocols, the state consists of information about destinations in the network, neighbors of a router, local interfaces etc. Monitoring such information remotely by means of a management protocol can provide insight into the current operation of the protocol (e.g., the network topology), help to discover problems, calculate statistics, etc. Monitoring may require continous feedback of the current state for analyzing long-term behavior of the protocol, as well as to observe frequencies of changes of the state.

4.3. [ACT3] Monitoring of Performance

Monitoring of performance is related to Section 4.2. Network operators may not only be interest in changing coonfiguration of a protocol or observer the state, but investigate performance issues, such as slow convergence of a protocol or (unncesseary) large network bandwidth consumption. While this information may be directly accessible by observing the state of the router, management protocols may help to provide complete reports, statistics, counters etc. to the network operator. For example, RMON [RFC4502] allows for gathering statistics based on counters and generating reports that are sent back to the network operator.

4.4. [ACT4] Notifications and Fault Management

In case of criticial malfunctions or warnings, notifications may be actively sent to a network operator (e.g., via email or using a network management protocol). The notification will typically include the reason for the notification, the source address, related information, the time of the incident etc., and is sent to a preconfigured server (e.g., a network management station).

4.5. [ACT5] Software Upgrades (Out of Scope)

During deployment of a device, it may be necessary to upgrade the firmware of the device, e.g., in order to fix security holes. Management protocols may allow a remote upgrade of the software by monitoring new versions of the firmware, downloading the upgrade in case there is a new version and verifying integrity of the downlaoded file, backing up the existing firmware, installing the firmware, verifying correct installation and providing feedback about the successful installation.

As firmware upgrades are very different in terms of requirements, use cases, and protocols, they are out of scope for this document.

4.6. [ACT6] Security Configuration (Out of Scope)

IETF protocols are required to provide sufficient security protection against malicious attacks. Before secure communication between devices over an unsecured network is possible, parameters such as cryptographic keys, cipher algorithms, trusted authorities, revoked keys etc. must be exchanged betwen devices.

As security configuration is very different in terms of requirements, use cases, and protocols, it is out of scope for this document.

5. MANET Management Scenarios

This section discusses several management scenarios for the various types of MANETs identified previously. Management Scenarios represent applications of the Management Activities to abstracted MANET Use Cases, which combined identify a set of current and desired management capabilities. The list is non-exhaustive.

In the following, the term "node" is used for either a host or router. The term "unit" or "mobile unit" is a unit that may contain multiple routers, hosts, and/or other IP-based communication devices.

5.1. [SCE1] Pre-Deployment Configuration

Configuration of MANET devices once they have been deployed can be a very tricky endeavor. Hence, one common approach is the pre-configuration the MANET nodes prior to their deployment, followed by monitoring of their state and performance once they are deployed. This is often performed in the ’Parking Lot Staging Area’. MANET nodes are shipped to a remote location, along with a fixed Network Operations Center (NOC), where they are all connected over traditional wired or wireless networks. The Fixed NOC then performs mass-configuration and evaluation of configuration processes similar to configuration of networked devices in Enterprise Networks. Once all units are successfully configured, they are ready to be deployed. Once deployed, monitoring of the state and performance of the nodes is attempted at the fixed NOC.

```
   +---------+             +--------+
   |  Fixed  |<---+------->| unit_1 |
   |   NOC   |    |        +--------+
   +---------+    |
                  |        +--------+
                  +------->| unit_2 |
                  |        +--------+
                  |            .
                  |            .
                  |            .
                  |        +--------+
                  +------->| unit_N |
                           +--------+
```

Figure 1: Parking Lot Staging Area

5.2. [SCE2] Out-of-Band Management

Configuration management is relatively straightforward in Enterprise Networks due to the possibility of Out-of-Band Management. Here, in the event of mis-configuration, the manager can access the mis-configured device(s) out-of-band and correct, or back out of, the incorrect configuration(s). In MANETs, the equivalent capability can be achieved, to a certain extent, when multiple radio, satellite, or other interfaces exist on the MANET devices. An example of this scenario is management with satellite reach-back. Here, a fixed NOC and the MANET are connected through an On-The-Move (OTM) satellite communications capability. Vehicles carrying MANET routers can support multiple types of wireless interfaces, including high capacity short range radio interfaces as well as low capacity OTM satellite interfaces. The radio interfaces are the preferred interfaces for carrying data traffic due to their relatively high capacity, but the range is limiting with respect to connectivity to a Fixed NOC. Hence, OTM satellite interfaces offer a more persistent but lower capacity reach-back capability. The existence of a more persistent satellite reach-back capability offers the NOC the ability to monitor and manage the MANET routers over the air. This affords the NOC the ability to perform state and performance monitoring and receive notifications, but also allows the NOC to perform some amount of configuration management safely while the MANET nodes are on the move.

```
                                 ---   +--+    ---
                                /  /---|SC|---/  /
                                ---    +--+   ---
   +---------+                           |
   |  Fixed  |<--------------------------+
   |   NOC   |            +--------------|
   +---------+            |              +-------------------+
                          |              |                   |
                      +--------+         |              +--------+
                      | unit_1 |         +---------+    | unit_N |
                      +--------+         |         |    +--------+
                          *              |         |      *   *
                          *        +--------+      |      *   *
                          *********| unit_2 |******|*******   *
                                   +--------+      |          *
                                        *          |          *
                                        *       +--------+    *
                                        ********| unit_3 |*****
                                                +--------+

         --- show SatCom links
         *** show Radio links
```

Figure 2: Monitoring with one-hop SatCom Reachback network

5.3. [SCE3] Management of Mobile Nodes of Networks

It is common to find mobile vehicles carrying a rather complex set of networking devices, including routers running MANET control protocols. In this scenario, the MANET mobile unit has a rather complex internal architecture where a local manager within the unit is responsible for local management. The local management includes management of the MANET router and control protocols, the firewall, servers, proxies, hosts and applications. Here, a standard Enterprise Management interface is applicable in this scenario. Moreover, in addition to being able to utilize a standard management interface into the components comprising the MANET nodal network, the local manager can be responsible for local monitoring and the generation of periodic reports back to the Fixed NOC.

```
                               Interface
                               |
                               V
   +---------+             +-------------------------+
   |  Fixed  |  Interface  | +---+     +---+         |
   |   NOC   |<---+------->| | R |--+--| F |         |
   +---------+    |        | +---+  |  +---+         |
                  |        |        |    |  +---+    |
                  |        | +---+  |    +--| P |    |
                  |        | | M |--+    |  +---+    |
                  |        | +---+       |           |
                  |        |             |  +---+    |
                  |        |             +--| D |    |
                  |        |             |  +---+    |
                  |        |             |           |
                  |        |             |  +---+    |
                  |        |             +--| H |    |
                  |        |                +---+    |
                  |        | unit_1                  |
                  |        +-------------------------+
                  |
                  |
                  |        +--------+
                  +------->| unit_2 |
                  |        +--------+
                  |            .
                  |            .
                  |            .
                  |        +--------+
                  +------->| unit_N |
                           +--------+


         Key: R-Router
              F-Firewall
              P-PEP (Performance Enhancing Proxy)
              D-Servers, e.g., DNS
              H-hosts
              M-Local Manager
```

Figure 3: Hierarchical Management Nodes

5.4. [SCE4] In-Band Network Management

In future MANET operations, it would be useful to achieve full management of the MANET over In-Band access over potentially lossy, intermittent and large delay links. In this case, there are a number of issues that would arise and need to be addressed, including:

1. Validating the network configuration (and local configuration) becomes a complex task, e.g., when to cut-over the network to the new configuration becomes an interesting question.

2. Bandwidth considerations may become important when attempting to push large configuration changes to a large number of MANET nodes over the wireless infrastructure.

3. Typically the state of the devices comprising the MANET would be in various states of operations, e.g., ON/OFF, etc., and synchronizing these nodes to the new network configuration would be problematic.

4. Pushing large data files, e.g., software upgrades, over a lossy network, would be problematic,e.g., the TCP over lossy links issue previously discussed.

```
   +---------+             +--------+
   |  Mobile |<----------->| unit_1 |
   |   NOC   |?--+         +--------+
   +---------+    |
         ^        |        +--------+
         |        +------->| unit_2 |
         |                 +--------+
         |                     .
         |                     .
         |                     .
         |                 +--------+
         +---------------->| unit_N |
                           +--------+
```

In-Band Management over Lossy/intermittent Links

6. Management Architecture

6.1. Typical Network Management Architecture in the Internet

6.2. Distributed Architecture [ARC1] vs Centralized Architecture [ARC2]

6.3. Flat Architecture [ARC3] vs Hierarchical Architecture [ARC4]

6.4. Entire Network Management [ARC5] vs Individual Router Management [ARC6]

6.5. Connectivity Assumptions

6.6. Notification Destination (Fault Management)

7. MANET Use Cases

This section lists several use cases of MANETs. Each case is introduced with a brief description of the application, role of MANET in such application, and maybe some example deployments in the real world. Required management activities, related challenges and management scenarios are illustrated with a reference to previous section. For example, [ACT3] stands for section 4.3 Monitoring of Performance.

This list is non-exhaustive.

7.1. Military Networks

Military tactical networks are characterized by their domain of operations. Networks are required to support a broad range of mobilities (e.g., ground, air and space vehicles), are required to support a broad range of sizes (e.g., from small squad level networks to divisional level deployments of tens of thousands of nodes), are required to operate in very hostile environments (e.g., all climates), in very critical situations (e.g., warfare), and do so under explicit attacks (e.g., kinetic and non-kinetic) by hostiles. Military tactical networks are primarily wireless and hence must operate with intermittent and lossy connectivity with little or no infrastructure. These networks are required to provide highly reliable and robust communications; it is not possible to simply provide monetary rebates to customers in the event of a failure-to-operate.

Military networks must provide a robust Quality-of-Service in order to both support the presentation of a broad range of realtime and non-realtime applications and to support the triage of information in situations of network congestion.

Current military MANETs range from upper echelon deployments such as the Warfighter Information Network-Tactical (WIN-T) [WIN-T]. WIN-T is a vehicular-based MANET, where vehicles of various sizes are supported depending upon the echelon level, e.g., high capacity trucks carrying multiple computers, routers, radio and satellite systems, high power generation systems, etc., versus small capacity car-sized or unmanned ground and air vehicles with one or two computers and a single radio system with minimal power storage capabilities. Other military MANETs are comprised of networks of single radio systems such as the Joint Tactical Radio System (JTRS) [JTRS]. JTRS systems are typically carried as individual mobile radio nodes of various sizes and platforms. The JTRS Ground Mobile Radio (GMR) is a larger high power high bandwidth radio carried on vehicular systems. While the JTRS Handheld, Manpack and Small Form Fit (HMS) radio is a small hand held system.

NOTE: the following is just an example to illustrate the refs!

Derived challenges: [CLG2][CLG3][CLG5]

Derived management activities: [ACT1][ACT2][ACT3][ACT4][ACT5]

Derived management scenarios: [SCE1]

Derived management architecture: [ARC1][ARC2][ARC4][ARC5]

7.2. Emmergency or Disaster Situations

Establishing basic communication after an emergency such as a flood, earthquake or nuclear accident, is difficult when the communication infrastructure is damaged. Mobile phones require nearby infrastructure that provide connectivity, which may not work any more. Even if the infrastructure is still available, the increased use of mobile phones after an emergency can saturate the network. The cable telephone network may be malfunctioning when cables are broken, satellite phones are rarely available and expensive. In addition to voice communication, data collection on the emergency site is desirable. Information, such as temperature, humidity or radioactivity of the disaster area, can help understanding the degree of the disaster, and to coordinate help accordingly. One such deployment that establishes communication in emergency situations is the SKYMESH project of Niigata University [SKYMESH], which is aimed at establishing communication between several unmanned balloons in order to rapidly create communication networks for rescuers. A small computer, together with a GPS device and a camera, is attached to the balloon, which floats in a height of 50 to 100m over ground, allowing remote wide area monitoring of the disaster area, as well as establishing communication (voice or data) using the ad hoc network. Another deployment in emergency situations is to drop large numbers of sensors from an airplane. The sensors can then establish an ad hoc network, once they are on the ground, without the necessity for humans to enter the disaster site and to deploy the sensors manually.

7.3. Community Networks

Community networks are comprised of constrained routers in a multi-hop mesh topology, communicating over a lossy, and often wireless channel. While the routers are mostly non-mobile, the topology may be very dynamic because of fluctuations in link quality of the (wireless) channel caused by, e.g., obstacles, or other nearby radio transmissions. Depending on the routers that are used in the community network, the resources of the routers (memory, CPU) may be more or less constrained - available resources may range from only a few kilobytes of RAM to several megabytes or more, and CPUs may be small and embedded, or more powerful general-purpose processors. Examples of such community networks are the FunkFeuer network (Vienna, Austria), FreiFunk (Berlin, Germany), Seattle Wireless (Seattle, USA), and AWMN (Athens, Greece). These community networks are public and non-regulated, allowing their users to connect to each other and - through an uplink to an ISP - to the Internet. No fee, other than the initial purchase of a wireless router, is charged for these services. Applications of these community networks can be diverse, e.g., location based services, free Internet access, file sharing between users, distributed chat services, social networking etc, video sharing etc.

As an example of a community network, the FunkFeuer network comprises several hundred routers, many of which have several radio interfaces (with omnidirectional and some directed antennas). The routers of the network are small-sized wireless routers, such as the Linksys WRT54GL, available in 2011 for less than 50 Euros. These routers, with 16 MB of RAM and 264 MHz of CPU power, are mounted on the rooftops of the users. When new users want to connect to the network, they acquire a wireless router, install the appropriate firmware and routing protocol, and mount the router on the rooftop. IP addresses for the router are assigned manually from a list of addresses (because of the lack of autoconfiguration standards for mesh networks in the IETF).

While the routers are non-mobile, fluctuations in link quality require an ad hoc routing protocol that allows for quick convergence to reflect the effective topology of the network (such as [RFC6130] and [I-D.OLSRv2]). Usually, no human interaction is required for these protocols, as all variable parameters required by the routing protocol are either negotiated in the control traffic exchange, or are only of local importance to each router (i.e. do not influence interoperability). However, external management and monitoring of an ad hoc routing protocol may be desirable to optimize parameters of the routing protocol. Such an optimization may lead to a more stable perceived topology and to a lower control traffic overhead, and therefore to a higher delivery success ratio of data packets, a lower end-to-end delay, and less unnecessary bandwidth and energy usage.

Different use cases for the management of community networks are possible:

- One single Network Management Station (NMS), e.g. a border gateway providing connectivity to the Internet, requires managing or monitoring routers in the community network, in order to investigate problems (monitoring) or to improve performance by changing parameters (managing). As the topology of the network is dynamic, constant connectivity of each router towards the management station cannot be guaranteed. Current network management protocols, such as SNMP and NETCONF, may be used (e.g., using interfaces such as the NHDP-MIB [RFC6779]). However, when routers in the community network are constrained, existing protocols may require too many resources in terms of memory and CPU; and more importantly, the bandwidth requirements may exceed the available channel capacity in wireless mesh networks. Moreover, management and monitoring may be unfeasible if the connection between the NMS and the routers is frequently interrupted.

- A distributed network monitoring, in which more than one management station monitors or manages other routers. Because connectivity to a server cannot be guaranteed at all times, a distributed approach may provide a higher reliability, at the cost of increased complexity. Within the IETF, several standard exists for distributed monitoring and management, including Remote Monitoring (RMON) and DIStributed MANagement (DISMAN). This will be discussed in the Management Architectures section below.

- Monitoring and management of a whole network or a group of routers. Monitoring the performance of a community network may require more information than what can be acquired from a single router using a network management protocol. Statistics, such as topology changes over time, data throughput along certain routing paths, congestion etc., are of interest for a group of routers (or the routing domain) as a whole. As of 2012, no IETF standard allows for monitoring or managing whole networks, instead of single routers.

7.3.1. Public Interent access

7.3.2. Public Safety

7.3.3. Opportunistic networks for developing areas

7.4. Wireless Sensor Networks

The general context for Wireless Sensor Networks (WSNs) is small, cheap devices whose primary function is data acquisition, with communications capabilities enabling them to send data to a controller, using a wireless multi-hop topology. As an example, a WSN deployed for environmental monitoring might contain a set of temperature sensors, sending "notifications" to a central controller when the temperature exceeds certain thresholds. Compared to a network of wired sensors, WSNs offer the advantage of enabling mobility to sensors, as well as reducing cost and space requirements for the installation of cables. The properties of WSNs are similar to the ad hoc network presented in section 1.3.1, with the following differences: (1) hardware resources (in terms of CPU and memory) of sensor routers are even more constrained than ad hoc routers in the FunkFeuer network, (2) unlike the routers in the FunkFeuer network, sensor routers may be battery driven, and (3) sensor network topologies are often optimized for particular traffic patterns.

As for (1), a typical sensor router may be equipped with no more than 50 KByte of flash, 5 KByte of RAM, and a few Megahertz of CPU speed (e.g., the Scatterweb MSB430). Compared to the routers in the FunkFeuer network, these sensor routers have much more constrained resources, and thus require special care when designing protocols for these sensor routers, minimizing required memory space and CPU power. As for (2), sensor nodes are often battery-driven, constraining their life-time compared to routers with a permanent energy supply. This implies that protocols for such sensors should have the objective to maximize resource savings (e.g. by reducing the frequency of message transmissions). As for (3), a major use case for sensors is measuring a set of environmental data and sending it through the network to a central controller. This traffic flow assumption allows to construct specific, optimized network topologies which focus on connections from a sensor to the controller (versus sensor-to-sensor or controller-to-sensor).

7.4.1. Habitat and Environmental Monitoring

7.4.2. Health monitoring

7.4.3. Tracking applications

7.4.4. Wildlife monitoring

7.5. Vehicular Networks

7.5.1. Intelligent Transportation Systems

7.5.2. Vehicular to vehicular networks

8. Standard Management Protocols Currently Used in MANETs

The IETF has already offered an array of solutions to manage IP networks. These range from the Simple Network Management Protocol (SNMP) [RFC1157] and related capabilities, to more recent management capabilities based upon the NETwork CONFiguration Protocol (NETCONF) [RFC6241] and associated capabilities and other tools, e.g., Constrained Application Protocol (CoAP) or DIStributed MANagement (DISMAN).

8.1. Managing with Simple Network Management Protocol (SNMP)

8.1.1. Overview of the Protocol

SNMP was purposely designed at the application level to manage different devices built by different vendors. SNMP uses the concept of a manager and agents for managing devices using the TCP/IP protocol suite. It provides a set of network operations for configuring, monitoring, and managing networks. In SNMP frameworks, a manager station, which runs the SNMP client program, controls a set of agents. An agent residing on the device runs the SNMP server program.

The management process is achieved either through a simple session-less User Datagram Protocol (UDP) or a session-oriented Transport Control Protocol (TCP), communication between a manager and an agent. SNMP uses two other protocols for handling management tasks: Structure of Management Information (SMI) as a language to describe management model and Management Information Bases (MIBs) as instances of management models. SMI defines general rules for naming the objects, defining object types, and showing how to encode objects and values. MIB modules model a collection of named objects and their relationship to each other. SNMP can provide capabilities of configuring the network devices and monitoring functionality by providing network states, performance data, and notifications through a set of packet types (GET, GET-NEXT, SET, GET-BULK, TRAP, INFORM, RESPONSE, and REPORT).

8.1.2. Applicability for MANETs

SNMP is used on a broad range of networks, from a small number of network devices to networks with large numbers of network devices. SNMP has a minimal impact on the managed nodes, places minimal transport requirements, and continues working when most other network applications fail. These characteristics allow for SNMP applications on MANET as well. Using SNMP, we can monitor network performance, track network usage, detect network faults, detect inappropriate access, and remotely configure MANET nodes. These network management activities help to optimize MANET network performance. In the following, scenarios are listed where SNMP can be useful in the management of MANETs:

- Pre-deployment situation is the most common practice when all MANET routers are deployed at a fixed location for initial configuration. The configuration is conducted by a fixed management station. SNMP configuration methods are necessary to be performed for this situation.

- Once MANET routers are deployed or being used in the field where low bandwidth is available, SNMP performance and state management, and fault management methods are necessary to be used for this situation.

- MANET routers can be managed from a Centralized Network Management Station where is usually a fixed location. SNMP configuration, monitoring, and fault management methods are necessary to be applied here.

- In some cases when a MANET router is required to be reset to its initial configuration, this is often accomplished by a local network management manager that resides within the MANET router. SNMP configuration, monitoring, and fault management methods are necessary to be applied here.

8.2. Managing MANET with NETwork CONFiguration Protocol (NETCONF)

8.2.1. Overview of the Protocol

NETCONF is a promising technology emerging from the IETF as a potential method of standardizing network management that is directed to improve the configuration process for network based devices. The NETCONF protocol was designed as a means of addressing the drawbacks and limitations of SNMP as a mode of initializing, manipulating and deleting configuration data. It accomplishes this through a set of standard Remote Procedure Calls (RPCs) that interact with a NETCONF enabled device. Some of the features it boasts over SNMP are:

- Separation of configuration and state data

- Three distinct configuration sets for running, start-up and candidate (uncommitted scratch set)

- Ability to extend the functionality beyond the core RPCs

It should be noted that NETCONF is not intended to be a complete replacement for SNMP. NETCONF is tailored specifically for its configuration functionality while SNMP would still be the dominate method of polling for performance and monitoring. The protocols are designed to work side by side to provide a complete network management solution. The current version of NETCONF can run over four secure transport protocols: Secure Shell (SSH) which is mandatory. The configuration data exchanged by NETCONF is modeled using YANG [RFC6022] and coded in modules. These modules can be broken down into sub modules to reduce complexity. Data is encoded using a set of pre-defined data types and stored in a tree/leaf structure.

8.2.2. Applicability for MANETs

With the advantage of configuration and security over SNMP, NETCONF has recently been supported and utilized by network management community. SNMP configuration methods in the old days can now be replaced with NETCONF configuration methods. In the following, scenarios are listed where NETCONF managing methods are useful:

Pre-deployment configuration - NETCONF can be best useful in this situation when stable and reliable connectivity exists.

Configuration changes done by a Centralized Network Management Station - although NETCONF can certainly be useful here, but high latency can be a problem if there is high latency.

Configuration changes done by Local Network Management Manager - NETCONF configuration methods are necessary to be deployed for this management framework.

8.3. Managing MANET with DISMAN

8.3.1. Overview

TBD

8.3.2. Applicability for MANETs

TBD

8.4. Managing MANET with CoAP

8.4.1. Overview

TBD

8.4.2. Applicability for MANETs

TBD

9. References

[I-D.OLSRv2] Clausen, T., Dearlove, C., Jacquet, P., and U. Herberg, "The Optimized Link State Routing Protocol version 2", draft-ietf-manet-olsr-17 (work in progress), October 2012.

[I-D.ersue-constrained-mgmt] Ersue, M., Romascanu, R., and J. Schoenwaelder, "Management of Networks with Constrained Devices: Use Cases and Requirements", draft-ersue-constrained-mgmt-02 (work in progress), October 2012.

[JTRS] "Wikipedia: Joint tactical Radio System", January 2013.

[RFC1157] Case, J., Fedor, M., Schoffstall, M., and J. Davin, "Simple Network Management Protocol (SNMP)", STD 15, RFC 1157, May 1990.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, BCP 14, March 1997.

[RFC4502] Waldbusser, S., "Remote Network Monitoring Management Information Base Version 2", RFC 4502, May 2006.

[RFC5497] Clausen, T. and C. Dearlove, "Representing Multi-Value Time in Mobile Ad Hoc Networks (MANETs)", RFC 5497, March 2009.

[RFC6022] Scott, M. and M. Bjorklund, "YANG Module for NETCONF Monitoring", RFC 6022, October 2010.

[RFC6130] Clausen, T., Dean, J., and C. Dearlove, "Mobile Ad Hoc Network (MANET) Neighborhood Discovery Protocol (NHDP)", RFC 6130, April 2011.

[RFC6241] Enns, R., Bjorklund, M., Schoenwaelder, J., and A. Bierman, "Network Configuration Protocol (NETCONF)", RFC 6241, June 2011.

[RFC6779] Herberg, U., Cole, R., and I. Chakeres, "Definition of Managed Objects for the Neighborhood Discovery Protocol", RFC 6779, October 2012.

[SKYMESH] Suzuki, H., Kaneko, Y., Mase, K., Yamazaki, S., and H. Makino, "An Ad Hoc Network in the Sky, SKYMESH, for Large-Scale Disaster Recovery", Proceedings of the 64th IEEE Vehicular Technology Conference, September 2006.

[WIN-T] "Wikipedia: Warfighter Information Network - Tactical", January 2013.

Authors' Addresses

James Nguyen
U.S. Army CERDEC
6010 Frankfort St
Aberdeen Proving Ground,
USA

Phone: +1-443-395-5628
Email: james.h.nguyen4.civ@mail.mil
URI:

Robert G. Cole
U.S. Army CERDEC
6010 Frankfort St
Aberdeen Proving Ground,
USA

Phone: +1-443-395-8744
Email: robert.g.cole.civ@mail.mil
URI:

Ulrich Herberg
Fujitsu Laboratories of America
1240 East Arques Avenue
Sunnyvale, CA
USA

Phone: +1 408 530 4528
Email: ulrich@herberg.name
URI: http://www.herberg.name

Jiazi Yi
LIX, Ecole Polytechnique
Route de Saclay
Palaiseau,
France

Phone:
Email: jiazi@jiaziyi.com
URI: http://www.jiaziyi.com/

Justin Dean
Naval Research Laboratory

Phone:
Email: jdean@itd.nrl.navy.mil
URI: http://cs.itd.nrl.navy.mil/