A Platform Independent Model for Mobile Ad Hoc Routing

Antonio Martin[1], Jeffrey Smith[2], Manfred Koethe[3]

Abstract

A Mobile Ad Hoc Networking (MANET) is a layer on top of an existing wireless network to assist in discovery and multi-hop routing of packets across a network. While extensive work has been performed in the field of MANET security, it has been based on select issues or on an incomplete MANET architecture assessment.

This paper will refactor the commonality in MANET approaches as a simpler classification mechanism and propose a Platform Independent Model (PIM) to serve as a base architecture capable of addressing various MANET specific attacks and identification of assets. The MANET PIM will be eventually proposed as a UML Profile. Given the PIM assets, a threat analysis for MANETs can be completed by addressing the asset's vulnerabilities and associated threats. The model and threat analysis will serve as a foundation to address security-first analysis at the base level of a system's architecture, independent of the platform, the algorithm or implementation, and usable for future secure research.

Introduction

This paper is based on three related observations. First, there have been many MANET algorithm survey papers that share similar methods of classification [e.g. MA, TK, Wiki, etc.]. Second, the process of deriving secure variants from these classical MANET algorithms (e.g. SAODV from AODV) have been incomplete as security-last design approaches deal with diverse types of security traversing all layers of the OSI stack. Third, though at first glance, it may seem that security is difficult to implement due to factors e.g. dynamic topology, physical access to nodes, etc., MANET peculiar attacks and vulnerabilities typically deal with one specific location between layers 2 and 3 of the OSI stack.

These observations are related in the thesis that if one could capture MANET algorithm common properties and relationships in a PIM, and include security properties as first class meta-model elements, then one could compose verifiable Platform Specific Models (PSMs) with respect to the MANET meta-model that intrinsically include requisite security properties (for at lest the static building blocks of MANET design rather than dynamic parametric alteration [AC]).

[1] SCA Technica, tony.martin@scatechnica.com
[2] Composable Logic, Inc., jesmith@ComposableLogic.com
[3] 88solutions Corp., koethe@88solutions.com

This paper is a prelude to an RFP, leading to a PIM that will serve as the base architecture to address the various MANET specific attacks. The rationale for this is to 1) refactor the commonality in MANET approaches as a simpler classification mechanism and serve as a base profile to describe novel algorithms, 2) provide greater insight in uniformity into classification of existing and anticipated MANET algorithms for reusability and search, 3) facilitate custom composition of new algorithm instances from existing model parts, base architectural structure for given constraints e.g. topology, specific attacks, node types, etc. and a desired MANET feature list and 4) provide the ability to verify MANET algorithm instances against the PIM.

The MANET PIM will be proposed as an OMG standard UML Profile. The first step is the submission of the MANET UML Profile RFP. The initial RFP can use IETF RFCs 3561 (AODV), 4728 (DSR), 3684 (TBRBF) and 3636 (OLSR) as a basis of requirements [IETF RFCs]. Given this Profile, we will describe threat analysis, identifying assets, vulnerabilities and threats, usable for future deployments. This architecture and threat analysis will serve as a foundation to address security-first analysis at the base level of a system's architecture, prior to build, independent of the platform, the algorithm or implementation.

Candidate architectural approaches for a MANET PIM

There are several abstraction possibilities for a MANET PIM. One possibility is to begin with the classification of meta-modeling elements by showing the relationships among MANET asset candidates e.g. Processing, Storage, Information, Packets, Network Topology and Node Roles [AM]. A functional approach starts with core meta-modeling elements encapsulating core functions common to all MANETs, and models a hierarchy of PIMs [AM]. A classification approach would yield more of a taxonomy, lumping MANET types by classical "piles" e.g. types that are proactive vs. reactive, hierarchical vs. flat, power and/or security aware, multicast vs. unicast vs. geocast, stateful vs. stateless, network vs. source centered, duplex support, etc. [Wiki, TL, MA]. A fourth approach was to perform a classification based on different deployment scenarios e.g. MANETs connected to potentially different MANETs below the IP level, isolated MANETs (with no router), interconnected MANETs as one network, stub MANETs to a fixed infrastructure and layered MANETs (similar to interconnected except the top layer is a MANET vs. fixed infrastructure) [IETF-1, AC].

Given the range of PIM architectural choices, we considered a MANET network as a collection of architecturally equivalent nodes, with the ability to communicate directly with each other. In the MANET PIM, each node is represented by a ManetNode component [alternatively UML2 Encapsulated/Structured Classifier or SysML Block].

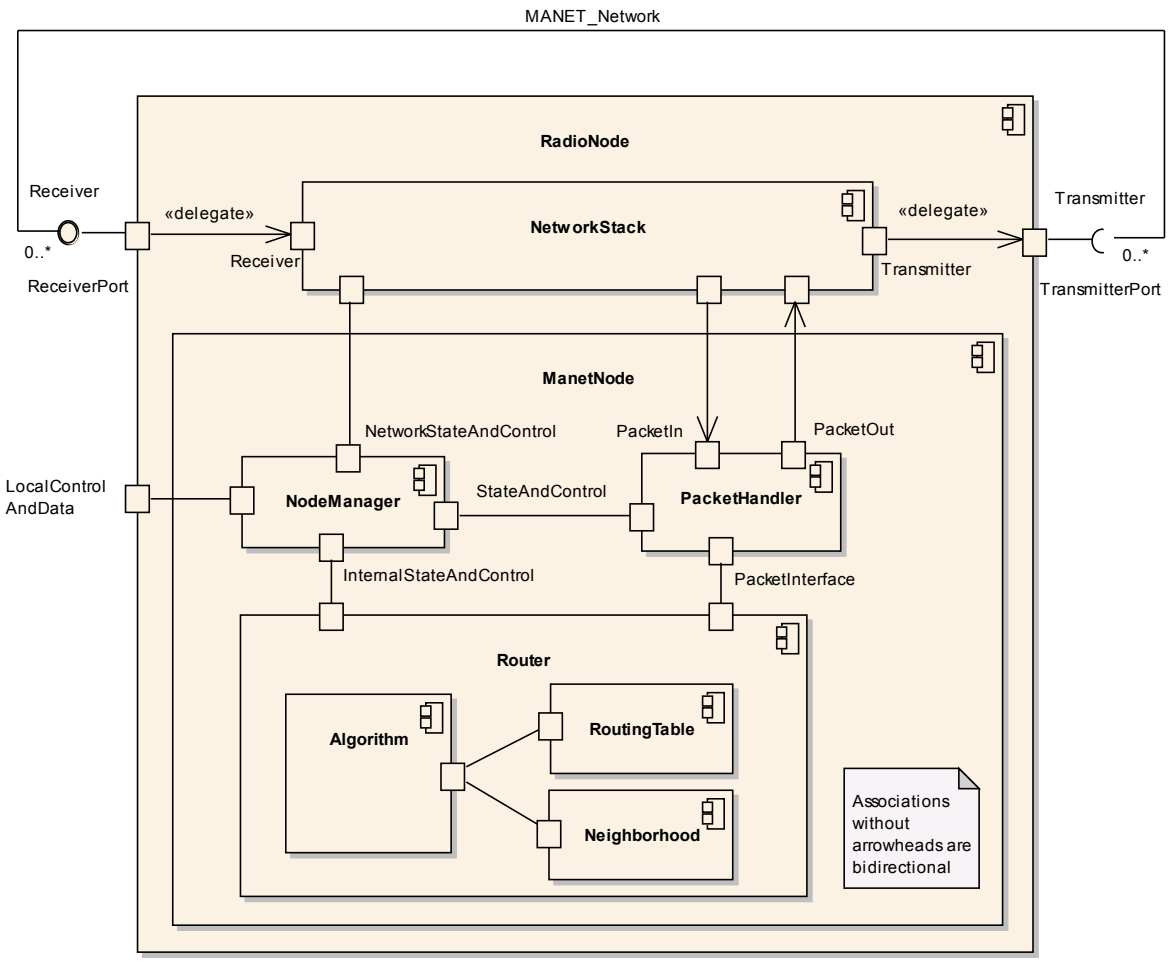


Figure 1 is the proposed component model for a MANET platform independent model.

A ManetNode is a subsection/subcomponent of a RadioNode that exists within the scope of a radio. Its function is to provide the multi hop and discovery mechanisms classically associated with ad hoc routing and must interact with existing networking capabilities of the RadioNode. This interaction is defined in the component interaction between the ManetNode and a radio's preexisting NetworkStack; this could be an IP stack, or other such communication protocol stack, allowing radio nodes to communicate with each other. The ManetNode acts as an enhancement to an already existing communication node and relies on existing stack communication mechanisms like authentication, encryption, MAC protocols, link controls, firewalls, encoding, interleaving, etc.

To this end, a ManetNode is primarily constructed of three components:

The NodeManager is responsible for abstracting the interfaces to the radio and NetworkStack for the Router and PacketHandler. It accepts information from external sources and parses the information before relaying it to the Router. Furthermore it is capable of altering the radio's state, passing log and state information to users or situational awareness engines, etc. via the LocalControlAndData interface.

Communication to the NetworkStack via the NetworkStateAndControl interface enables cross layer optimizations and the flow of routing information and paths. The NodeManager can control the PacketHandler's queues through the StateAndControl interface. The NodeManager interfaces and abstracts all local RadioNode data.

PacketHandler represents all aspects of creating, handling and manipulating network packets, inclusive packet buffering. The PacketHandler abstracts the structure, handling, altering, queuing, parsing and digesting of packets or data from NetworkStack and the MANET route (re)discovery mechanisms. The PacketHandler's PacketIn and PacketOut interfaces are separated because of their inherently different entry points in the up and down flow of a NetworkStack. The PacketHandler interfaces and abstracts all Packet and other RadioNode's information; the information and handling of data traversing to and from the RadioNode to the network.

The Router is responsible for calculating routes on demand from the PacketHandler or the NodeManager and/or it may update/refresh its own routing metrics, proactively. The router is comprised of a routing Algorithm for calculating paths/routes, a RoutingTable for storing routes and a NeighborTable holding information about other nodes in the network. The Router accepts inputs only from the NodeManager and the PacketHandler; by this means, all external interfaces are abstracted from the Router and various different Router mechanisms can be interchanged.

The Router has two interfaces, the first InternalStateAndControl to the NodeManager for all internal radio and NetworkStack specific information / control and a second, PacketInterface for all external packet based information. This selection of subcomponents allows a strict separation of concerns between functionality associated only with the MANET layer and functionality provided by underlying network stack. The ManetNode component with its contained sub-components represents only the MANET layer of the network stack. All aspects of the communication are encapsulated by the NetworkStack subcomponent, considered a "black box" in this paper.

Modeling these elements as components allows an for an adaptation to existing and future routing protocols, while keeping the key internal and external interfaces constant and independent from routing protocol details. Interestingly, the PIM is not specific to MANET but also can be applied to any Mesh like network mechanism where the behavior of the components dictates the classification of the Node.

Naturally, the above diagram is merely an overview to keep the concept simple. Within the Router, the Algorithm, RoutingTable and Neighborhood are only the major subcomponents; there are many more subcomponents e.g. a hierarchy of timers, queues, agents, etc. Our bottom up refinement of this PIM would be to fitted known algorithms [IETF] and described each as an instantiation of the above PIM adding components as necessary. This way we can guarantee a common set of object across MANETs that are distinguished by different states/transitions.

MANET assets

From PIM point of view, a MANET has a series of assets. Identifying the set of these assets is critical. It is through the vulnerabilities of these assets (enumerated below) that a MANET enabled system can be attacked.

- ManetNode Processing: The resources within a radio used for calculating, maintaining and processing MANET routing, this includes interfaces to external to the ManetNode components.
- ManetNode Storage: The algorithm repository for the radio that are loaded on boot or request.
- Local Information: Tables, node state information, the run time, active information used by a ManetNode in operation.
- MANET Specific Packet Information: Information shared between nodes to assist in routing. This can contain information such as radio/node location, power availability, node speed and direction, radio profiles, user profiles, etc. This also includes the routing tables stored in a radio. This formation can be broken down into:

    Payload Messages: Messages containing the data in need of routing and delivery, usually with routing information attached to the message's header. The purpose of a MANET is to deliver said information.

    Routing Messages: Route discovery, update and reporting messages that are critical for a MANET to successfully maintain connectivity and routing capabilities. These are protocol specific messages or alterations to prior networking messages.

- Network topology and Node Roles: The topology of a network; MANET changes the behavior of a network and the functions of various nodes.

Requirements

A discussion of requirements prior to to submission of a MANET Profile is necessary and required prior to submittal of an RFP. The following list is candidate requirements is meant to stimulate this discussion. Requirements contributions to the RFP are expected from other sources including the SDR Forum. The MANET PIM shall:

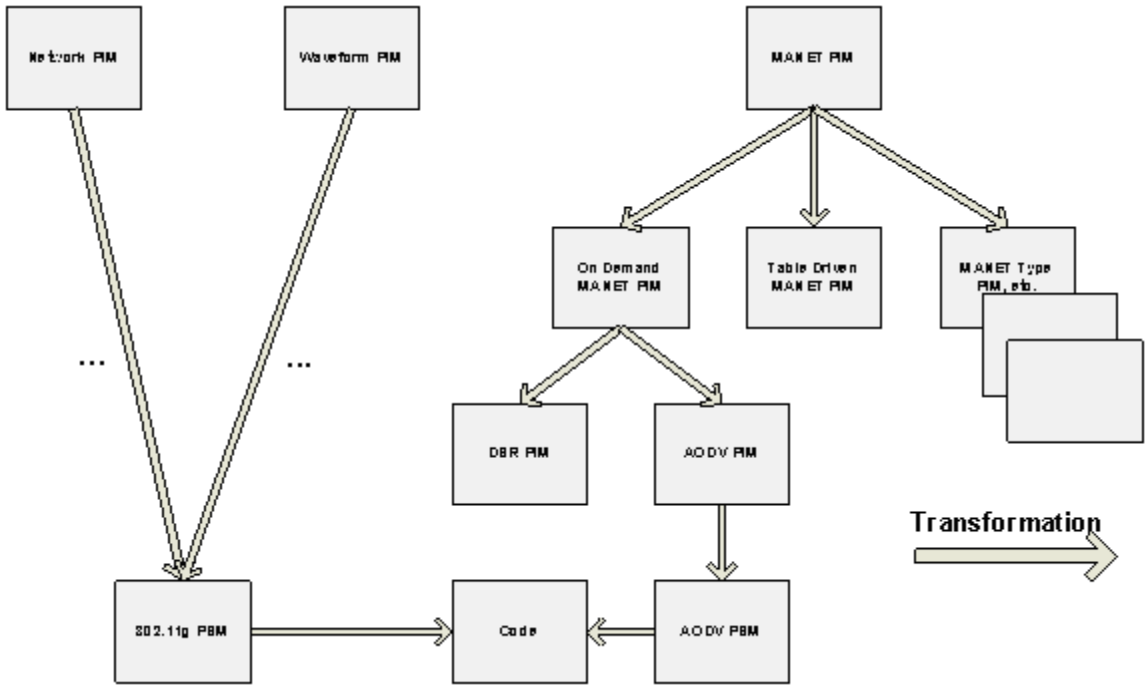
- be capable of being added to an existing software radio and/or network stack and provide support for dynamic network discovery, reconfiguration and data routing for mobile nodes.
- be language, operating environment and middleware neutral, platform, network and waveform independent.
- provide for scalability to support various sized systems.
- serve as the reference model from which future, more specific MANET PIM/PSM shall inherit.
- support proactive, reactive, hybrid, flow, geographic, multicast and geo-multicast protocols including AODV, DSR, OLSR, OSPF implementations.

- allow for the control of radio resources including power levels, beam forming, network stack routing, media access control layer.
- be capable of interacting with Information Assurance mechanisms.
- allow for the providing of external data interfaces like GPS.
- allow for the reporting of status information.
- be capable of inheriting the “High Level Security Requirements (SDRF-06-A-0002-V0.00, January 2006).
- not to exclude QoS mechanisms for MANET specific needs.
- support Type 1 – 4 architectures.
- provide packet, radio node, network stack abstractions.
- be limited to the design of MANET only and shall no cover the design of a network stack nor associated radio node and information assurance component.
- abstract external interfaces and communication from the routing algorithm/ mechanism.

Future Work

The first step in the OMG standardization process for the MANET MDA process is to discuss the RFP for the MANET Profile, propose the RFP and then to respond to it. Step one will occur 9/25/07. We will continually be building up our response to this RFP, collecting input from the SDRF, industry and academia.

It is conceivable that the entire structure of a radio could be defined by individual PIMs and PSMs. This hierarchy, a set of formal models (depicted below) could then allow for the rapid and dynamic building of radio nodes from proven, pre-built and tested components. MANET PIM is the first step is defining a small part of an overall system allowing for a close examination without being overwhelmed by the complexity of the entire system. By the nature of MANET, an overlay over an existing network, it is a perfect “case study” for a completely library of network and radio components.



A well defined API is needed between the three component interfaces (InternalStateAndControl PacketInterface and StateAndControl and the undefined interfaces between Algorithm and RoutingTable and Neighborhood.) so that various components and algorithms can be more easily interchanged for rapid redeployment and adaptation.

When this paper is completed, it will contain an example, instatiable from the previously given PIM, of a common MANET algorithm or two. This work will be validated through Network Simulator 2. We will take this step after a more complete compilation of requirements.

Summary

We have introduced a preliminary PIM for MANETs, along with a candidate set of requirements, to catalyze a pre-RFP discussion and solicit input for a MANET Profile submission. The specification that will result from these responses to this RFP will help in the classification, development and threat analysis of MANET applications and will provide uniform architectural connections to other domain and platform profiles (e.g. SDR and security related specifications). The authors are working on a parallel paper for the SDR Forum, focused on MANET security, leveraging this work's model to identify assets specific to the MANET and identifying associated threats.

References

[TL] T. Larrson and N. Hedman, “Routing Protocols in Wireless Ad-hoc Networks – A Simulation Study”, Masters Thesis at Lulea Tekniska University, 1998, http://www.ietf.org/proceedings/99mar/slides/manet-thesis-99mar.pdf.

[MA] M. Abolhasan, T. Wysocki and E. Dutkiewicz, “A Review of Routing Protocols for Mobile Ad Hoc Networks”, Ad Hoc Networks 2 (2004) 1–22.

[WS] W. Scott, A. Houle, T. Martin, “Information Assurance Issues for an SDR Operating in a MANET Network”, Invited SDR Forum Paper, Nov. 2006, http://www.friendsglobal.com/papers/Information_Assuance_SDR_Security_MANET.pdf.

[AM] A. Martin, “A Platform Independent Risk Analysis for Mobile Ad hoc Networks”, Boston University Conference on Information Assurance and Cyber Security, Dec 2006, http://www.friendsglobal.com/papers/Platform_Independent_Risk_Analysis_for_Mobile_Adhoc_Networks.pdf.

[Wiki] Ad hoc Routing Protocol List, http://en.wikipedia.org/wiki/Ad_hoc_protocol_list

[IETF] IETF Manet Protocol Standards, http://www.ietf.org/ids.by.wg/manet.html.

[IETF RFCs] http://www.ietf.org/rfc.html

[IETF1] IETF WG paper, Infinity Networks, http://tools.ietf.org/html/draft-boot-manet-nemo-analysis-01, 6/07.

[AC] A. Casteigts and S. Chaumette, Dynamicity Aware Graph Relabing Systems, a local computation Based Model to Describe MANET Algorithms, http://www.labri.fr.