A Platform Independent Risk Analysis for Mobile Ad hoc Networks

Antonio Martin (SCA Technica, USA, tony.martin@scatechnica.com)

Boston University Conference on Information Assurance and Cyber Security, Dec 2006

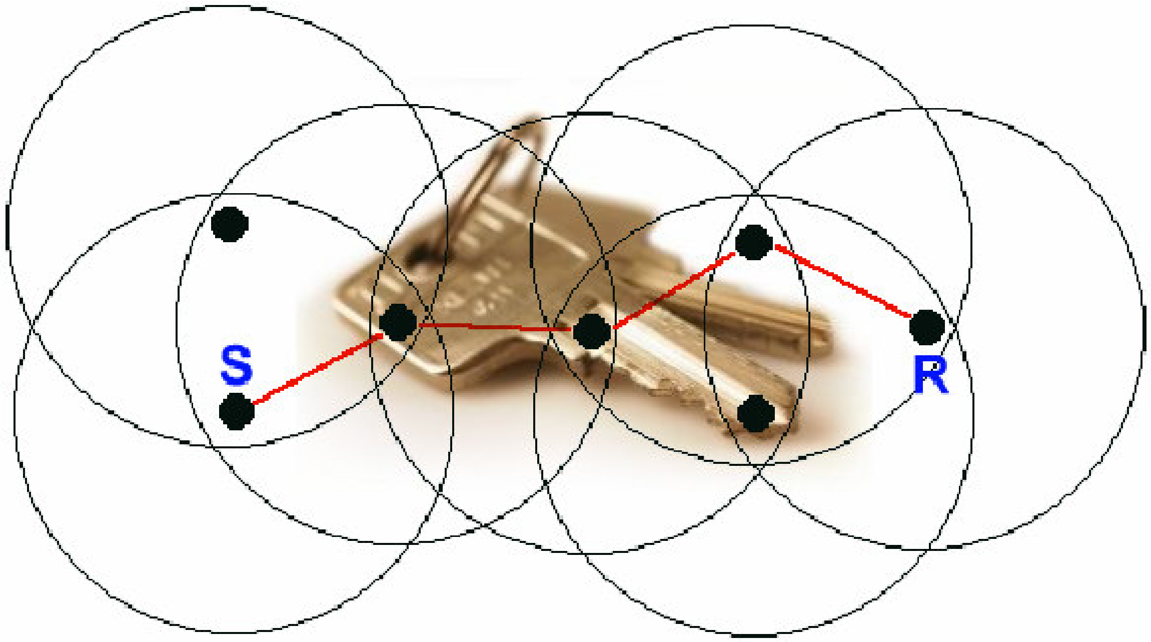
Abstract

Mobile Ad Hoc Networking (MANET) adds a layer on top of wireless communication to assist in multi-hop routing of packets across a network topology. Extensive work has been performed in the field of secure MANET and ad hoc routing with examples found in Secure AODV (SAODV) and Authenticated Routing for Ad hoc Networks (ARAN) [1]. By contrast, in openly published literature, little has been written about threats and risks for MANET networks; a key needed in developing any protection profile and architecture. Without a threat / risk analysis, current MANET security works' effectiveness are difficult to assess. This paper provides a tutorial of MANET specific attacks and a platform independent, risk analysis by identifying assets, vulnerabilities and threats, usable for future MANET deployments and security work.

Introduction

Mobile Ad Hoc Networking (MANET) provides a means of wireless routing; two wireless nodes, out of range, wishing to communicate, can leverage nodes in between to carry packets. This is accomplished by ad hoc routing, the mechanism layered over a network providing a route discovery and recovery mechanism allowing for data to be transported from node to node. There are multiple classifications of ad hoc routing: on demand, pre defined / table driven, geo-location aware, power aware, hybrid, etc

Considering an on demand protocol, when a node must send data to another, if an entry for the destination does not exist in the sender's routing tables, it will broadcast a route request (RREQ) message to propagate until a route is found. A returned route reply (RREP) message communicates the path back to the originating node. In addition, if a route is lost because nodes moved or dropped from the network, a route error (RERR) will propagate back to the sender and a route discovery will be repeated. Utilizing a discovered route, the packet can then be routed from source to destination with the cooperation of chosen nodes or paths. This extra layer on top of a wireless system presents potential security issues that can disrupt effective communication.



Security has been a concern for MANET based system for many years with work on possible attacks and multiple proposed routing protocols offering solutions to selective security issues. In open publications, little has been performed concerning a risk analysis for MANET networking. A risk analysis requires a series of evaluations to enable a developer or researcher to properly understand a system's assets, vulnerabilities and threats and how these interoperate with risks and values. This allows for a risk prioritization; only then can proper and cost effective defensive mechanisms be introduced. A risk analysis is challenging since certain aspects are platform specific; it requires an exact deployment or scenario where values and costs can be considered. Thus, a complete risk analysis is impossible to perform without knowing the given system, algorithms, platform, waveform, network and environment a MANET will be operating within.

Each MANET deployment shares a set of common characteristics that can be described as assets. Because of the complexity of a risk analysis, it is critical to identify those assets specific only to the MANET layer and not the waveform, network or radio layers of a system, simplifying the task into multiple independent considerations. Without concerns for a specific deployment, a more thorough examination of the possible MANET assets, associated asset vulnerabilities, specific attacks and their classification into threats may be evaluated. This requires an examination independent of the platform and of the algorithm; a high level of generalization allows for a risk assessment that can be extended / expanded for platform specific models or deployments. To this extent, the concern will be to examine those Assets, Vulnerabilities and Threats that are MANET specific to a platform independent system.

Assets

A MANET has a series of assets, some wholly owned by the MANET layer and others that are shared between the MANET the radio platform, the waveform, etc... The goal of this exercise is to provide a baseline of asset identification; a platform specific risk analysis will identify more and will require to place value on these assets.

- Algorithm Processing: The resources within a radio used for calculating, maintaining and processing MANET routing.
- Algorithm Storage: The function of holding the algorithms for the radio that are loaded on boot or on request.
- MANET and User 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 on a radio.
- Network Topology and Node Roles: The topology of a network, the behavior and function of individual nodes and their routing loads.
- 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.

Vulnerabilities

A vulnerability of an asset is a vector that can be exploited; all vulnerabilities map to at least one asset.

- Algorithm Processing: The resources required for operation/processing of a radio may be consumed, preventing effective MANET participation.

- Algorithm Storage: MANET information and algorithms may be read or altered in the radio's/node's storage.

- MANET and User Information: Information within the routing protocols necessary for routing calculations may disclose user information and location. Tables on a radio may be maliciously altered. These alterations can then be propagated through routing information sharing. This information may be read or modified.

- Network Topology and Node Roles: The topology is vulnerable in lending insight for an attacker. The behavior of nodes within a MANET can give insight as to their roles within a network such as gateway function, critical nodes for routing, communication patterns, etc… Predictive behavior from known and/or mappable algorithms, in conjunction with route finding message storms, present patterns. In low probability to detect networks, some nodes might be in a silent mode; MANET requests may cause silent or stealthy nodes to chat. Behavior of nodes for given algorithms, timings, sizes and patterns of data flows can lend insight to node type.

- Payload Messages: Data messages require intermediary nodes to help propagate messages to intended receivers. Data messages are intercepted by nodes and rebroadcasted, usually with routing information modifications and is susceptible to unauthorized reading and malicious modification. Route error messages can be improperly enacted signifying a data message was undeliverable. Intermediary nodes must be trusted to forward routing messages properly; improper routing may be disruptive.

- Routing Messages: A route request can generate a broadcast storm where receiving nodes are required to forward the packet until a route is found or some end of life mechanism is reached. As a result, these messages are intercepted by nodes and rebroadcasted, usually with routing information modifications. As a route request message propagates, it traverses many nodes, gathers information along its route and is susceptible to unauthorized reading and malicious modification. Route return messages face similar threats from unauthorized reading and malicious modification. Route error messages can be improperly enacted. Intermediary nodes must be trusted alter and forward routing messages properly.

In these vulnerabilities, the threat to user and MANET information used for routing is listed twice, once with MANET and User Information and a second time in Routing Message as part of the header. This is because in some cases it might be acceptable to expose non-identifying information while User or Node specific routing information might need to be protected better. MANET and User information spans multiple locations/assets and thus is considered and assets for vulnerability and threat assessment.

Attacks

A survey of available attacks reveals a sizable list of both applied and theoretical MANET based network attacks. These attacks are based on the specific characteristics that are inherent in MANET networks. *This list was primarily compiled under the work of Scott, Houle, Martin* [2] *and has been extended.*

The following are some active attacks on MANET networks.

- Altering Radio Route Tables – Hacking the radio and modifying routing tables and the propagation of these alterations. [1] Routing tables are stored locally, thus it is possible for malicious actions to alter these entries. Ad hoc route discovery mechanisms can propagate these table alterations, "infecting" other nodes in the network.

- Black Hole – Complete refusal to participate in a network, can be sudden as an established node in the routing topology and drops out. This type of attack is difficult to detect in dynamic networks with mobile nodes entering and leaving the network. [3] When a node "drops out", all routes it participated in are now broken, thus the network will face the cost of route discovery. Non-malicious actions such as powering down a node or leaving range can behave like a Black Hole.
- Gray Hole / Selective Forwarding– A node in the established routing topology selectively drops packet causing network disruption, can be difficult to detect. [4, 12] Depending on the drop rate and the type of data that is dropped, detection of this type of attack is challenging. A malicious node can participate fully in route discovery, thus inserting itself into the topology, yet it can selectively drop data packets at a low rate. Wireless networking by its nature addresses packet loss; a slight increase in the loss rate can seriously degrade performance while appearing as normal propagation issues. An overloaded node, though no fault of its own might selectively drop packets, thus behaving like a Gray Hole.
- Jamming – Jamming is not a MANAET specific attack; it is the new jamming applications that must be recognized. Selectively jamming routing messages used to build and maintained the network can easily and efficiently prevent communication. Jamming a central node can break down a network.

- Jelly Fish – Active insertion of jitter/delay into packet routing; harms QoS and can deny timely packet delivery. [3]

- Loop Forming – Where the routing is purposefully manipulated, creating a path for a packet to continuously loop. [1]

- Message Injection/Spoofing – Inserting messages into the network without responding back, used for routing manipulation.

- Route Error Falsification – Nodes can generate false route error messages instead of transporting data messages. [1] This delays a packet delivery and can force the sending node to request a node discovery.

- Rushing – An attack where a node "rushes" a corrupt packet identified to match the real packet. The receiving node first accepts the corrupt packet, drops it and then, on receipt of the good packet matches the packet identity to that of the prior, and drops it. [6]

- Sandwich Drain – Two colluding nodes interposed themselves with the victim node(s) in the middle. The attackers then send messages back and forth, forcing the victim(s) to route, consuming resources and potentially draining battery.

- Selfish Node – Nodes that refuse to fully participate in routing.

- Short Circuit / Replay – A node in a network may rebroadcast the energy from a neighboring node, extending its range. Thus node B, hearing the replayed message of A by C, will believe that the shortest route is through A. Nodes A and B have no knowledge that packets are being replayed. This is a type of attack does not require authentication into a network, only the ability to read and rebroadcast energy.

- Sinkhole – Taking on more routing than needed, forcing data thought itself; becoming an overly critical network node. [4, 7] This attack can be difficult to find because the node may be capable of handling all routing without disruption.
- Sybil – Assuming the identify of several nodes in the network. Presenting self with multiple identities or presenting self as neighbors taking on neighbor functions and roles, MAC spoofing. [4, 5]
- Wormhole – At least two conspiring nodes falsely report information about a shorter route, a "short cut" in the network. [5, 6, 7]

Some of these attacks result from normal behavior of nodes within a system. Black and Gray Hole attacks can result from non-malicious behavior on the part of nodes. Route Error Falsification and Selective Drop can be difficult to differentiate. If node A is trying to route a packet to the next hop B and B refuses to acknowledge the acceptance of the packet from A, then A will assume that B cannot be reached and will trigger a false route error.

The following attacks are passive in nature.

- Traffic Analysis – As a result of a MANET networks predictive behavior, nodes are easier to classify. With node identification, resource limited attacks can be more disruptive. Traffic analysis is not about looking at the data within a packet, but the specific flows of energy being broadcasted and their associated characteristics. This can be conducted in fully encrypted networks and critical routing nodes can be identified.

- Silent Node Exposure – Not a specific MANET attack but a result of MANET behavior. A node can responds to a query, broadcasting energy, compromising position.

- Traffic Snooping – A form of eavesdropping where the attacker reads exposed information to gain insight into a node or network's behavior. Unprotected information can disclose node information (location, power, etc) and divulge network topology. While this is not a MANET specific attack, improper implementation of a MANET network might encrypt packet data but expose routing information.

Threats

Many attacks share common vectors that allow them to achieve their ends; understanding how these attacks function allows for better placement of defensive mechanisms. Multiple attacks that can be classified under multiple threat types. Rushing uses the mechanisms of relay with the intent to deny a packet / denial of service. Sinkhole may not be disruptive and thus pose no threat but it does create a future vulnerability in the network to a denial of service if the Sink Hole node leverages another attack.

Threat	**Attack**
Eavesdrop	Traffic Snooping
Traffic Analysis	Traffic Analysis Silent Node Exposure
Modification	Altering Radio Route Table Loop Forming
Masquerade	Spoofing Sybil
Replay	Rushing Short Circuit
Denial of Service	Black Hole Gray Hole Jelly Fish Route Error Falsification Sandwich Drain Selfish Node Sinkhole Wormhole

These attacks are classified into the following threat types:

- Denial of Service: A type of attack intended to deny or delay service to authorized participants. The scope may be a single node or the whole network / group.

- Eavesdrop: Examining the content of messages to gather information.
- Masquerade: Pretending to be multiple nodes within a network; presentation with multiple identities that may or may not already exist.
- Modification: Altering intercepted message content.
- Traffic Analysis: Viewing traffic flows, sizes, timings to gather insight into network topologies and node types.

Each of these attack classifications can be considered a threat against a specific set of vulnerabilities already identified for the given assets. The following chart shows a mapping of these threats to vulnerabilities to assets.

Assets	Vulnerabilities	Threat
Algorithm Processing	Radio resources can be consumed	Modification, DoS, Replay
Algorithm Storage	Storage can be read, corrupted or modified	Eavesdrop, Modification
MANET / User Information	Node or User specific information might be readable Node or User specific information might be modifiable Improper protection mechanisms on routing tables	Eavesdrop Modification DoS, Modification, Eavesdrop
Network Topology and Node Roles	Increased communications amongst nodes needed to supporting routing can expose network topology and node roles.	Traffic Analysis
Payload Messages	Data might be readable Data might be modifiable Nodes must be trusted to transport information Non-compliant routing can be disruptive	Eavesdrop Modification DoS, Eavesdrop, Modification DoS
Routing Messages	Routing information might be readable Routing information might be modifiable Routing information can be malicious Nodes must equally participate Nodes must be trusted to transport information	Eavesdrop Modification DoS, Modification Masquerade, Replay DoS, Eavesdrop, Modification

Risk Assessment

Risk assessment maps the effort it takes to launch an attack, the likelihood that a particular attack will succeed against an asset and consequence of such a successful attack producing a score where Risk = Asset x Vulnerability x Threat. To finalize a risk assessment, assets must be assessed a value, vulnerabilities must be given a rating as to their criticality and threats must be rated as to their possibility and or of existing

With asset values, vulnerabilities and threats rated, it is easier to prioritize the specific threats that must be address for this particular deployment. The threats and vulnerabilities are scored/rated for an open, campus network. This type of network will face students who can be curious of system functionality and attempt pranks. The desire is to protect the network's availability over confidentiality or integrity.

A vulnerability rated as Negligible is of little concern, a Major is great and Minor being in between. A threat rated as Major is a relatively easy threat to launch while a Negligible threat is very difficult to undertake. Assigning a score of 1 to Negligible, 2 for Minor and 3 to Major allows for a simplistic ranking to develop where the risk score is equal to the asset value times vulnerability rating times threat rating.

Considering the asset of Algorithmic Processing; it is typically a student's laptop and thus, from the point of view of the campus network owners, has little value, hence a Minor asset value assignment. The asset has two potential vulnerabilities; the first "radio resources being consumed" is rated as a Minor threat because its impact is limited in scope to the single victim. This vulnerability has three potential threats; considering the second threat, a denial of service can consume processing resources on a platform. In an open network this type of attack is relatively easy to carry out (Major); thus the overall risk factor score for is rated as a 12 (2x2x3).

The Algorithm processing asset has a second vulnerability of buffer overflow; this is considered as a major vulnerability where an attacker is able to take control of the victim's machine using it to extend attacks. The associated threat is to modification, in this case modification to insert malicious code, and is considered a difficult threat to carry out, thus rated as minor.

Assets	**Asset Value**	**Vulnerability**	**Vulner. Rating**	**Threat**	**Threat Rating**	**Risk Score**
Algorithm Processing	Minor	Radio resources can be consumed	Minor	Modification DoS Replay	Minor Minor Minor	8 8 8
		Buffer overflow	Major	Modification	Minor	8
Algorithm Storage	*	Storage can be corrupted or modified	*	Modification	*	*
MANET / User Information	Minor	Node or User specific information might be readable	Negligible	Eavesdrop	Major	6
		Node or User specific information might be modifiable	Minor	Modification	Minor	8
		Improper protection mechanisms on routing tables	Minor	DoS Modification Eavesdrop	Minor Major Major	8 12 12
Network Topology and Node Roles	Negligible	Increased communications amongst nodes needed to supporting routing can expose network topology and node roles.	Minor	Traffic Analysis	Major	6
Payload Messages	Minor	Payload message might be readable	Negligible	Eavesdrop	Major	6
		Payload message might be modifiable	Major	Modification	Minor	12
		Nodes must be trusted to transport information	Major	DoS Eavesdrop Modification	Major Major Minor	18 6 12
		Non-compliant routing can be disruptive	Major	DoS	Major	18
Routing Messages	Major	Routing information might be readable	Negligible	Eavesdrop	Major	9
		Routing information might be modifiable	Major	Modification	Major	27
		Routing information can be malicious	Major	Modification DoS	Minor Minor	18 18
		Nodes must equally participate	Negligible	Masquerade Replay	Minor Minor	6 6
		Nodes must be trusted to transport information	Major	DoS Eavesdrop Modification	Major Major Minor	27 27 18

** Algorithm storage protection is a function of the radio / node's security function and not the MANET. Thus for this deployment, protection of this asset will not be a factor for the MANET risk assessment but of the radio / node assessment.*

The vulnerability of buffer overflow was not found in the prior because it is a result of this specific deployment; the prior platform independent view has no code.

In this deployment, the concerns of eavesdropping or traffic analysis are minimal as it is an open network, yet each threat is rated Major because of the ease of attacks. As a result, eavesdropping threats might have a high risk score. Any protections needed for this asset will be provided by the algorithm selected or other functional layers (network or application layers) or will be acknowledged and purposefully not addressed.

One area of concern is for the assets of Routing Messages, the first vulnerability of routing information modifiable has a threat from Modification with known attacks available. These attacks can quickly and easily disrupt an entire network. Likewise, the second vulnerability for Routing Messages, the routing being malicious, has two threats from Modification and Denial of Service attacks that are relatively simple to perpetrate and whose impact can be very disruptive.

With the individual asset, vulnerability, threat costs assessed, it is now possible to consider solutions that will help minimize the problem and their associated costs.

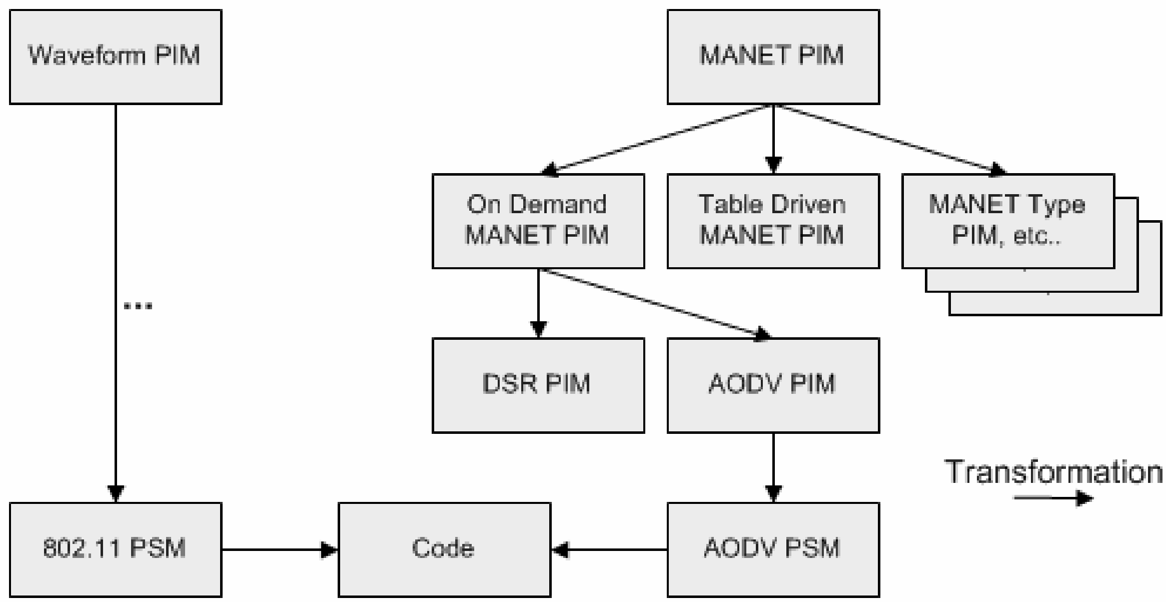
Conclusion

Far too often, security is added after a system is built, this leads to potential vulnerabilities not being secured.

"Security must be built in from the beginning"

While a common phrase it is not correct; it implies that security of a system must considered only when a system is "built." This adds security after a system has been designed when it must be considered from the architectural beginnings and publicly available MANET developments are an example where security was added later. In the case of Secure AODV or ARAN, security was “built” in from the beginning but on and already existing architecture.

It must be noted that this work is lacking as it is based on an incomplete assessment; the attempt to consider MANET from a Platform Independent Model (PIM) fails because it does not reference a PIM that has been developed for MANET. What is needed is a hierarchy of Platform Independent Models for various system functionalities. For MANET, the root node would contain a general MANET PIM, a set of MANET Type PIMs would inherit from this parent and finally a PIM for each MANET algorithm inheriting from the associated MANET Type PIMs. A similar model set would need to be developed for waveforms, with Waveform Type PIMs containing a Networking Waveform, eventually down to an 802.11g PIM. This would allow an architect using available modeling tools and methods to take an AODV MANET PIM, the 802.11g PIM and other PIMs to quickly and correctly generate a code base for a deployable node. Tools and modeling languages and methods exists today to support this modeling concept yet lack the formally verifiable model set.



With a well defined set of PIMs, threat assessments can be conducted for each, allowing for a clear inheritance path from prior threat assessments. For this type of functionality, a UML profile and set of tools would need to be developed, allowing security architects to work with system architects to quickly and securely build systems for deployment. Needed is a set of formal models and associated security models with secure transitions between states allowing for a provable security analysis for every deployment.

References

[1] K. Sanzgiri, B. Dahill, B.N. Levine, E. Royer, and C. Shields. "A Secure Routing Protocol for Ad Hoc Networks" Technical Report 01-37, Department of Computer Science, University of Massachusetts, August 2001

[2] W. Scott, A. Houle, A. Martin. "Information Assurance Issues for an SDR Operating in a MANET Network," SDR Forum, November 2006

[3] I. Aad, J. Hubaux, and E. Knightly. "Denial of Service Resilience in Ad Hoc Networks," ACM MobiCom, September 2004

[4] Y.C. Hu, and A. Perrig, "A Survey of Secure Wireless Ad Hoc Routing," IEEE Security and Privacy Proceedings, pp.28-30, May/June 2004

[5] M. Brumster, and T. Le. "Optimistic Tracing in MANET," Florida State University, Department of Computer Science, March 2006

[6] Y.C. Hu, A. Perrig, and D. Johnson. "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols" Technical Report TR01384, Department of Computer Science, Rice University, June 2002

[7] A. Burg. “Ad hoc Network Specific Attacks,” Ad hoc networking: Concepts, Applications and Security Seminar, Technische Universität München, 2003

3GPP TS 21.133 V4.1.0, “3G Security; Security Threats and Requirements” 3rd Generation Partnership Project, Technical Specification Group Services and Systems Aspects, Release 4, December 2001

A. Patwardhan, et al, “Secure Routing and Intrusion Detection in Ad Hoc Networks,” Proceedings of the 3rd International Conference on Pervasive Computing and Communications, IEEE, March 2005

D. Murotake, and A. Martin. “System Threat Analysis for High Assurance Software Defined Radios,” SDR Forum, November 2004

Evolution of 3GPP System; 3GPP TR 21.902 V6.0.0 (2003-09)

FAQ 1 Information Assurance Recently Asked Questions. National Security Agency Central Security Service http://www.nsa.gov/ia/iaFAQ.cfm