A PLATFORM INDEPENDENT MODEL AND THREAT ANALYSIS FOR MOBILE AD HOC NETWORKS

Antonio Martin (SCA Technica Inc., NH, USA, tony.martin@scatechnica.com)
Jeffrey Smith (SCA Technica Inc., NH, USA, jeff.smith@scatechnica.com)
Manfred Koethe (88solutions Corp, MA, USA, koethe@88solutions.com)

ABSTRACT

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 topology. While extensive work has been performed in the field of secure MANET, it has been based on select issues or on incomplete assessment of MANET architecture. Security must be addressed at the base level of a system's architecture, prior to build, independent of platform, algorithm or implementation. This paper leverages the Platform Independent Model (PIM) for MANET proposed to the Object Management Group (OMG) to serve as the base architecture for addressing the various MANET specific attacks and present a threat analysis of identified assets, vulnerabilities and threats, usable for future deployments, implementations and security work.

1. 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, a mechanism layered over a network providing route discovery and recovery mechanism allowing for data to be transported from node to node. This extra layer on top of a wireless system presents potential security issues that can disrupt effective communication.

Each MANET deployment shares a set of common characteristics that can be described as assets. 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 model.

A prior work, "A Platform Independent Risk Analysis for Mobile Ad hoc Networks" [1] addressed the need to examine security needs specific to just the MANET functionality, independent of the platform and implementation. The paper concluded its own work was based on an incomplete assessment since a platform independent model (PIM) for MANET did not exist. A recent paper, "A Platform Independent Model for Mobile Ad Hoc Routing" [2] was presented to the OMG where a PIM introduced as a candidate for an request for comments. Leveraging this PIM, an updated threat analysis can now be performed on MANETs.

2. PLATFORM INDEPENDENT MODEL [2]

A platform independent model (PIM) is a model of a system independent of a platform, deployment or a specific implementation; the MANET PIM (figure 1) is such an abstraction and referred to as a ManetNode.

The ManetNode is a subsection/subcomponent of a RadioNode, it 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's communication mechanisms like authentication, encryption, MAC protocols, link controls, firewalls, encoding, interleaving, transmission, reception, 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 it before relaying it to the Router. Furthermore it is capable of altering the radio's state, passing log and state information to users or situaltional awareness engines, etc. via the LocalControlAndData interface. Communication to the NetworkStack via the NetworkStateAndControl interface enables cross layer optimizations and the flow of

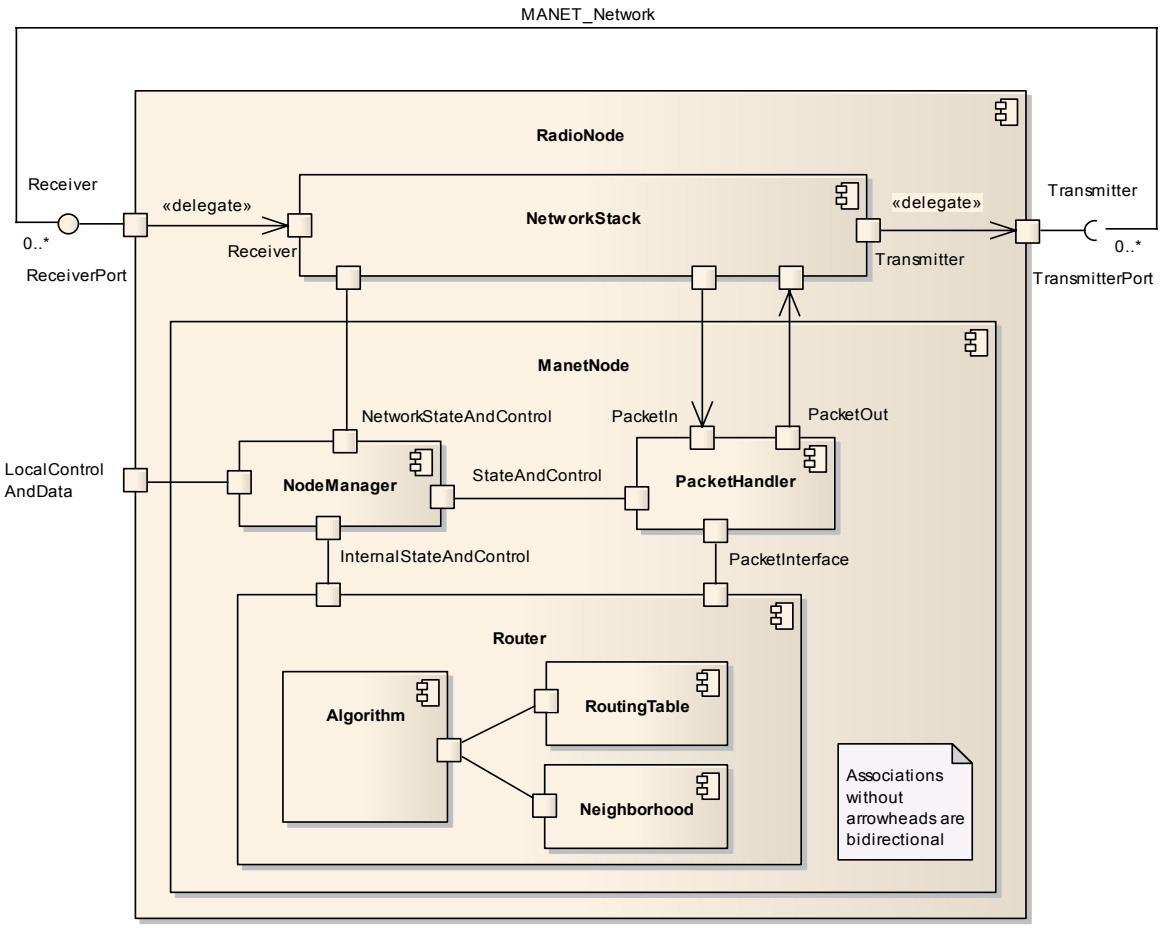

Figure 1: A platform independent model (PIM) for MANET was presented at the September OGM Technical Meeting. [2]

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 and RadioNode (sub)components, considered a "black box" until associated PIMs can be developed.

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 can be to fitted known algorithms 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.

3. MANET ASSETS

Based on the PIM, a clear set of MANET can be identified:

- ManetNode Processing: The resources within a radio used for calculating, maintaining and processing MANET routing.
- ManetNode Storage: The function of holding the algorithms for the radio that are loaded on boot or on request.
- Local Information: Information stored locally in a RadioNode. Assists in routing and 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.
- Manet Over the Air Information: Manet specific information broadcasted OTA. Can be broken into two sub-categories:
- 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, the behavior and function of individual nodes and their routing loads.

4. MANET VULNERABILITIES

A vulnerability of an asset is a vector that can be exploited; all vulnerabilities map to at least one asset. Certain vulnerabilities are as a result of issues in other components of the RadioNode and will be noted as such.

- ManetNode Processing: The resources required for operation/processing of a radio may be consumed, preventing effective MANET/radio participation. The processing of the ManetNode results in this vulnerability.
- ManetNode Processing Storage: MANET information and algorithms may be read or altered in the radio's/node's storage. This vulnerability is outside of the scope of the MANET PIM; the vulnerability lies in the storage mechanisms used for data in the RadioNode.
- Local Information: Information within the routing protocols necessary for routing calculations may disclose user information and location. Tables on a radio may be maliciously altered and alterations can then be propagated through routing information sharing. This information may be read or modified. These vulnerabilities are primarily as a result of mechanisms external to the ManetNode.
- Manet Over the Air Information: Comprised of routing and payload messages. Messages require intermediary nodes to help propagate information to intended receivers. 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 message was undeliverable. 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. Intermediary nodes must be trusted alter and forward routing messages properly; improper routing may be disruptive. The ability to read, modify, spoof and to trust nodes to route are vulnerabilities external to the ManetNode.
- Network Topology and Node Roles: 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. 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. The behavior of the ManetNode results in this vulnerability.

5. MANET ATTACKS

A survey of available attacks reveals a sizable list of both applied and theoretical MANET based network attacks. *This list was primarily compiled under the work of Scott, Houle, Martin [3] and Martin [1]*

Given a PIM for MANET and associated assets, it is then possible to classify the various attacks into two groups, those directly attacking the ManetNode functionality and those attacking other weakness in a radio node.

MANET Specific Attacks:

- Altering Radio Route Tables – Hacking the radio and modifying routing tables and the propagation of these alterations. [4] 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. [5] 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. [6] 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.
- Jelly Fish – Active insertion of jitter/delay into packet routing; harms QoS, can deny timely packet delivery. [5]
- Loop Forming – Where the routing is purposefully manipulated, creating a path for a packet to continuously loop. [4]
- Route Error Falsification – Nodes can generate false route error messages instead of transporting data messages. [4.] This delays a packet delivery and can force the sending node to request a node discovery.
- Selfish Node – Nodes that refuse to fully participate in routing.
- 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.
- Sinkhole – Taking on more routing than needed, forcing data thought itself; becoming an overly critical network node. [6., 7] This attack can be difficult to find because the node may be capable of handling all routing without disruption.
- 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.
- Wormhole – At least two conspiring nodes falsely report information about a shorter route, a "short cut" in the network. [6, 7, 8]

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.

MANET attacks on other radio node resources:

- 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. This is an attack on the over the air waveform and not the functionality of a MANET.
- Message Injection/Spoofing – Inserting messages into the network without responding back, used for routing manipulation. This attack can occur in any network and is not limited to MANET. [5]
- 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. [9] This is a point to point communication attack and is not limited to a MANET network.
- 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. This attack focuses on the energy broadcasted and thus is an attack on the radio node, not the ManetNode.
- Sybil – Assuming the identity of several nodes in the network. Presenting self with multiple identities or presenting self as neighbors taking on neighbor functions and roles, MAC spoofing. [5, 6, 7] Sybil requires nodes to assume multiple identities and thus leverages a weakness in a network's authentication; this is not MANET specific.
- 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.

Assets	Vulnerabilities	Threats
ManetNode Processing	Radio resources can be consumed	Modification, DoS, Replay*
ManetNode Storage	Storage can be read, corrupted or modified*	Eavesdrop*, Modification*
Local 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*, Eavesdrop*, Modification*
Network Topology and Node Roles	Increased communications amongst nodes needed to supporting routing can expose network topology and node roles.	Traffic Analysis
Manet Over the Air Information - Routing	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
Manet Over the Air Information - Payload	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

Table 1: MANET Threat List **-** ** Represents attacks/vulnerabilities on radio components other then MANET*

This is a data protection issue and is not specific to MANET.

While this second set is classified as MANET attacks [1, 5, 6, 7, 8, 9], in view of the PIM, they leverage weakness in other part of the radio node and usually can be effective against point to point, non-MANET networks.

6. MANET 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.

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. Table 1 shows a mapping of these threats to vulnerabilities to assets.

7. BRIEF EXAMINIATION OF EXISTING MANET SECURITY WORK

Several MANET designs have been developed / proposed with security concepts at build / design time but failed to consider the architecture of a MANET independent of platform and implementation. Thus their solutions leveraged existing network stack components but failed to address those weaknesses specific to MANET. Some examples can be found in Secure Routing Protocol (SRP), Secure Efficient Ad hoc Distance Vector Routing Protocol (SEAD), Asiadna, Secure Ad hoc Distance Vector (SAODV) and Authenticated Routing for Ad hoc Networks (ARAN) [4, 6, 10, 11]; all utilize one of many network stack mechanisms (PKI, digital certificates, one way hash functions, authentication mechanisms, etc…) for authentication, integrity and repudiation but these information assurance mechanism are outside of the scope of ManetNode PIM. While they do enhance the security of the network, they do not address the issues specific to MANET; their solutions are limited to hand picked topics and are incomplete for a secure deployment.

8. CONCLUTION

Security must be architected from the beginning, time of build and/or design is too late; it must be considered at the highest level of a system's architecture or a complete threat analysis is not possible. What is needed is a hierarchy of

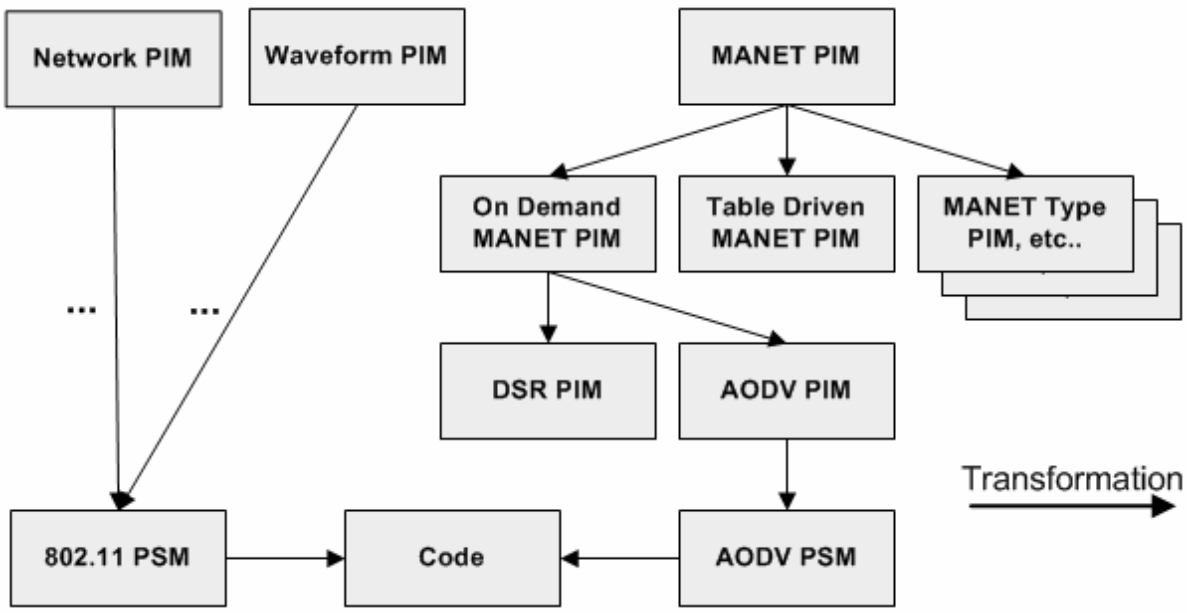

Figure 2: A hierarchy of PIMs and PSMs allows for the rapid and dynamic building of radio nodes from proven, pre-built and tested components. Associated threat models can be conducted, inherited and refined for each PIM/PSM.

Platform Independent Models for various system functionalities. For MANET, the root node would contain a general MANET PIM (figure 2) with child PIMs and platform specific models (PSM) inheriting. A similar model set would need to develop PIMs/PSMs for waveforms, network, stacks, authentication mechanisms, etc., eventually down to specific deployment PSM. This would allow an architect, using available modeling tools and methods, to quickly and correctly generate a code base for a deployable node.

For each PIM / PSM, an associated threat model would be conducted, each threat model inheriting from the prior assessment. A final deployment would have the benefit of an extensive listing of associated threat models allowing for a more through security consideration. With a proper threat analysis, only then is it possible to perform a risk analysis where the likelihood of a threat is weighed against the cost of protecting and assets against such an attack. Once completed, is it possible to correctly apply a balance of information assurance mechanisms [1, 3], routing algorithm selection and/or algorithm modification to protect a radio node and the associated network. This would then allow a deployment to more correctly leverage already existing information assurance mechanisms, more accurately balance security threats in trade off analysis and the designing of individual PIM/PSM architectures and their deployments, inherently more secure.

9. REFERENCES

[1] A. Martin. "A Platform Independent Risk Analysis for Mobile Ad hoc Networks," Boston University Conference on Information Assurance and Cyber Security, Dec 2006

[2] A. Martin, J. Smith Ph.D., M. Koethe, "A Platform Independent Model for Mobile Ad Hoc Routing", Object Management Group Technical Meeting, Sept 2007

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

[4] 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

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

[6] 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

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

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

[9] 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

[10] E. Fonseca, A. Festag, "A Survey of Existing Approaches for Secure Ad Hoc Routing and Their Applicability to VANETS" version 1.1, NEC Technica Report NLE-PR-2006-19, NET Network Laboratories, March 2006

[11] O. A. Khan, "A Survey of Secure Routing Techniques for MANET" National University of Computer and Emerging Sciences, Karachi