

INFORMATION ASSURANCE ISSUES FOR AN SDR OPERATING IN A MANET NETWORK

WILLIAM T SCOTT (GENERAL DYNAMICS C4 SYSTEMS, USA,
WILL.SCOTT@GDC4S.COM)

ALAIN C. HOULE (UNIVERSITÉ DE SHERBROOKE, CANADA,
ALAIN.HOULE@USHERBROOKE.CA)

ANTONIO MARTIN (SCA TECHNICA, USA,
TONY.MARTIN@SCATECHNICA.COM)

ABSTRACT

MANET networks are transitory, poorly regulated and essentially local in nature. Such environments have need for Information Assurance (IA) services, but the lack of regulation, the limited reach-back connectivity, and the ad hoc nature of the networks make supplying these services difficult. MANET IA services should supply subscriber confidentiality, data integrity and peer authentication, while being 1) independent of access to the larger network infrastructure, 2) resilient to a variety of attacks unique to wireless ad hoc environment, and 3) based on established industry protocols when possible. This paper proposes an approach to securing MANET networks by leveraging standard IP based security protocols such as PKIX, IKEv2 and IPSEC, and the new generation of cryptographic protocol standards e.g., MQV, AES, SHA-384 and ECDSA that supplies the required IA services within the MANET environment.

1. INFORMATION ASSURANCE PROCESS

Networks have come a long way since the early days of ARPAnet [1]. Thousands of businesses and billions of users depend on the Internet access; and greater dependency and access results in increased risk. This is especially true in mobile ad hoc networks (MANET) where access is virtually unlimited and network nodes are extremely vulnerable to attacks. Without proper protections against attacks, software definable radios (SDR) MANET networks are likely to fail to realize their potential.

Though MANET networks may be ad hoc, developing appropriate protection mechanisms must not. Protections must be developed methodically or, as history has shown, protection coverage will be left with huge holes. A methodological approach to developing appropriate security coverage usually includes:

- **Assets Identification** - resources of value that need protection.

- **Vulnerability and Threat Assessment** - Identifying what resources need protection and how those resources are threatened.
- **Risk Assessment** - Identifying the degree of risk associated with a threat and needed security services; the mechanisms and countermeasure needed to supply a sufficient level of asset protect.
- **Security Policy Development** – Developing a comprehensive set of rules for the use of security services that supply the level of protection required.

Considering the complexity and the importance of such an analysis, a sample of such a process would greatly help future developers of software definable radios (SDR) that operate in MANET environments. The following sections provide an example, examining each of these areas listed, and offering high level views of MANET assets, vulnerabilities, threats, risk assessments and related security policy features.

2. UNDERSTANDING PROTECTION NEEDS

Wireless networks are growing at a frantic pace. From cellular phone services to wireless web access, wireless services have been integrated in our lives. Nevertheless, many technical constraints still remain. Visibility is required of a user node before it can be granted access to network services. At times, direct node visibility may not be practical, but indirect access through neighbor nodes may be possible, if user nodes cooperate. At times, access to distant points may not be achievable, even through neighbors, but the cascading effect of nodes working together, helping each other transmit information from source to destination, may form a larger local area network that is of value. This cooperative behavior is the motivation behind Mobile Ad Hoc Networks (MANETs).

Integrating MANET routing capabilities into end nodes has the potential of providing users with robust and efficient wireless networks without the need for classical (wired or wireless) infrastructure. These networks are dynamic, often

rapidly-changing, random, multi-hop topologies composed of relatively bandwidth-constrained links [2]. The following sections provide an overview of the MANET environment from the perspective of information assurance.

2.1 MANET Environment

Figure 1 depicts the typical elements found in MANET. Depending on the context, user nodes can be packet-enabled cellular phones, personal digital assistants, personal computers, etc. Nodes may be static (e.g. network access nodes) or highly dynamic, rapidly moving or appearing and disappearing, depending on their on-off state, battery condition and proximity.

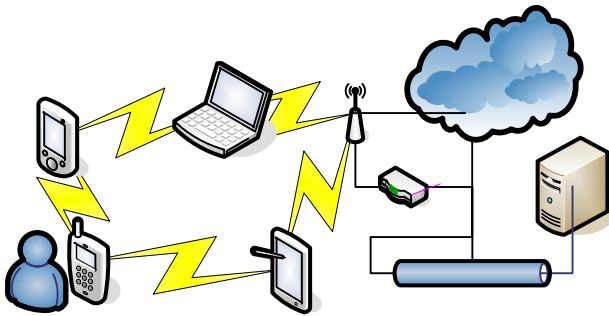


Figure 1 Sample MANET Network

2.1.1 MANET Characteristics

MANET networks have characteristics that differentiate themselves from classic wired and cellular networks. They include:

- **Network Topology:** MANET networks are highly dynamic, multi-hop and random. They may contain both unidirectional and bidirectional links, depending on user nodes conditions.
- **Bandwidth Constraints:** A MANET environment consists of multiple wireless user nodes sharing the same physical level medium; RF and medium access level phenomenon (noise, fading, interference, congestion), contribute to throughput limitation [3].
- **Energy Constraints:** User nodes are often battery operated, limiting their operational capabilities and impacting the sharing of bandwidth (e.g. to preserve resources, low power nodes may not want to route other nodes' information.)
- **IA Constraints:** Conventional wired systems possess physical access controls (building security) that are not available in wireless networks. The cooperative nature of MANETs produces a system more susceptible to attacks exploiting this cooperation, (e.g., eavesdropping, spoofing and denial-of-service.)

The preminent feature of MANET networks is that user nodes supply routing services. As such, a node is not

only a source or a destination for information but also a router for neighbors. The four most popular MANET routing protocols are topology-based, dynamically forming routing functions with neighboring node's link information. There are also position-based MANET protocols (e.g. LAR [4]). They take advantage of knowledge of position and speed of neighboring nodes when performing their routing functions. They require a positioning system (e.g. GPS) and knowledge of neighbor node positions. (These are especially advantageous in inter-vehicular communication applications [5]).

From an information assurance perspective, the philosophy of MANET networking is fundamentally different than conventional IP networks who rely on well established and relatively stable hierarchy. Given the dynamic topologies of MANET nodes, such networks cannot rely on a well established and stable hierarchy. At best, a few nodes may be elected for higher level functions (e.g. MPR nodes from OLSR protocol) but the election is short lived. While hierarchy is the keyword in conventional IP networks, cooperation is the key for MANETs and thus, trusting neighbors is essential.

2.2 MANET Asset Analysis

Traditional networks simply transported user information from point A to point B; the focus was on performance, and performance was measured in terms of technical parameters such as: packet-loss ratio, latency and jitter. Owners and operators of infrastructure were distinct from users.

MANET networks do not distinguish between users and infrastructure; the distinction between operator (control) information and user information (bearer) blurs. Cooperative aspects of MANET networks imply the possibility for anyone to access information as needed. This dual use, owner/user, aspect of the MANET networks implies access to user information should be denied to those without need.

2.2.1 Owner Information

MANET nodes are usually tied to individual owners. MANETs networks that rely on and transmit precise geographical data are also transmitting precise geographical positioning data on the owner. MANET networks not utilizing geographical data may still reveal physical position of a user/owner. As an example, consider the MAC addresses in 802.11 or Bluetooth products. The address is usually factory installed, unique, frequently broadcasted and rarely changed. Given RF characteristics of routing protocols, a MAC can be easily tracked, even from hundreds of meters away, enabling a hostile agent to track owner movements and location. By carrying a MANET wireless device (e.g. cell phone) owners can potentially be

tracked to their homes and have their shopping and other outside activities monitored. Most would find such surreptitious monitoring a violation of their privacy.

Ad Hoc networks are not anarchistic. Cooperation requires each node agreeing to and carrying out responsibilities. It is likely that waveforms will have built in monitoring systems to detect and respond to nodes that either fail to carryout their responsibilities or perform their responsibilities incorrectly. Nodes with bad reputations are likely to have service by others reduced or be excluded from the network, thus reputations have valued.

2.2.2 Traffic

Owner information is also found in the payload of user data packets. Payloads may contain proprietary and sensitive information. Once information has been launched in the network, this information becomes part of the network traffic.

2.2.3 MANET Resources

Network traffic also contains network control information. Corruption of network control information may have extreme consequences and disrupt routing.

Individual MANETs nodes are (usually) battery operated. Energy and processing resources are limited and must be used sparingly. Useless operations consume both computational resources and battery life. Routing protocol resources are also finite. False information not only corrupts the network, it may cause buffer overflow.

It may be desirable to provide various bandwidth capacity allocations depending on the MANET context or applications traffic. Prioritizing bandwidth capacity allocations must be fair.

MANET technology may be used to provide network visibility to nodes that are not a neighbor to network gateways. Access to the network gateway must not be impaired.

Table 1 MANET Assets to be protected

Owner Information	Traffic	MANET Resources
User Identity	Information Payload	Energy
Physical Position Information		Computing Resources
Reputation	Network Control	Bandwidth Capacity Allocation
Information Payload	Payload	Gateway Access

Table 1 presents a summary of the identified MANET Assets that need to be protected from an information assurance perspective.

3. VULNERABILITY ASSESSMENT

By definition, assets have value and value is usually subject to compromise. In the case of information, access to and use of an asset need not be denied to the owner to create a compromise. Table 2 summarizes SDR MANET asset vulnerability.

3.1 MANET Asset Vulnerability Analysis

Not all MANET assets are subject to the same set of compromises. By their very nature MANET routing information is not strictly private. They must be shared between peers. Such is not true for transported user data. Users expect a certain level of privacy when transmitting data across a network. The effect of a compromise of an asset's attribute(s) has on the assets and asset owner must be analyzed and evaluated.

3.2 Device, User Identity and Location

The device's identity and location is often directly associated with the owner. This coupling subjects a SDRs identity and location to the following vulnerabilities:

Privacy Violations: The SDR identity may be coupled with a specific user or class of users. Tracking the activity and location of an SDR leads to tracking the activity and location of the SDR's owner. Such tracking may subject the owner to personal harm.

Harm to Reputation: Misattribution of harmful or disreputable acts to the owner of the device harms the owner of that device.

Theft of Authority: It is likely that SDRs have service agreements allowing them access to networks and resources. That authority is usually device/owner specific. Use of that authority by others is a form of theft.

3.3 Transport Services (Traffic)

MANET networks forward traffic from a source to the designated destination through intermediaries. Intermediaries carrying traffic create vulnerabilities including: interception, misattributed source, privacy violations integrity violation, and denial of service.

Interception: Traffic is normally intended for specific destinations. Intermediaries may misdirect traffic.

Misattributed Source: Recipients value knowing the source of received traffic based. Data passed through intermediaries may not come from the purported source.

Privacy Violations: Intermediaries may read traffic while in transit, violating the privacy associated with the traffic.

Integrity: Recipients of traffic expect to get the traffic as sent. Intermediaries that modify the traffic while in transit violate the integrity of the traffic.

Denial of Service: MANET peers are expected to act as routers forwarding packets destined for others.

3.4 MANET Resources

MANET networks are cooperative efforts depending on accurate routing information and fair sharing of the mutual burdens by carrying traffic for others. MANET cooperation results in the following vulnerabilities.

Network Control: Transport efficient and fair networking services are supplied through collaboration between devices. Such collaboration is dependent on the exchange of fair and accurate routing information, but such information is subject to compromises that may undermine the cooperative effort.

Platform Resources: Transport services require each platform dedicate a share of its resources to cooperative use for the network. Resources shared include bandwidth, memory, CPU, power, routing information and gateway access. Table 2 summarizes SDR MANET asset vulnerability.

Table 2 Asset Vulnerability in a MANET Network

SDR Asset	Value	Vulnerability of Resources
Device and User Identity and Location	Privacy	Disclosure
	Reputation	Misattribution of actions
	Authority	Misuse of Authority
Transport services (Traffic)	Intended recipient	Interception
	Reliable source	Misattribution of source
	Privacy	Disclosure
	Integrity	Compromised
	Reliable Delivery	Denial of Service
MANET Resources	Network Control	Biased, unfair, crooked routing
	Platform Resources	Excessive, destructive expenditure of resources

4. ATTACKS, THREATS AND RISK ASSESSMENT

“... a power of estimating the adversary, of controlling the forces of victory, and of shrewdly calculating difficulties, dangers and distances, constitutes the test of a great general.” - Sun Tzu

To understand the risks a system faces, threats to the system must be considered; and threats cannot be understood without understanding the possible attacks.

4.1 MANET Specific Attacks

The unique characteristics of MANET routing algorithms result in new sets of wireless computing attacks. The majority of these attacks are directed at the algorithmic capabilities; the means of communicating routing information and the transporting of data. A partial listing of MANET specific attacks follows:

Altering Radio Route Tables – Hack the radio and modifying routing tables and the propagation of these alterations. [6]

Black Listing – Trick a network/system into believing a good node is behaving maliciously. [7]

Black Hole – Complete refusal to participate in a network, can be sudden.

Gray Hole – Selectively dropping packet causing network disruption - can be difficult to detect.

Jamming – Selectively jamming routing messages that define the network. Jamming a central node can break down a network. Timed jamming at intervals can cause the appearance of messages being lost, route loss.

JellyFish – Active insertion of jitter/delay into packet routing harms QoS and can deny timely packet delivery. [8]

Man in the Middle – A class of attacks where an intermediary node maliciously manipulates routing messages creating loops, wormholes, and biasing the network to route packets thought malicious nodes. [8]

Masquerading Data – Message injection without response: Loop forming, spoofing.

Masquerading Peer – Presenting self with multiple identities or presenting self as neighbors taking on neighbor functions and roles. MAC spoofing, also know as Sybil attack.

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 Man in the Middle attack, classified as an unauthenticated node having inserted itself into the network function. [9]

Rushing – An attack where a node “rushes” a corrupt packet identified to match the real packet. The receiving node first accepts the corrupt packet, dropping it and then, on receipt of the good packet matches the packet identity to that of the prior, and drops it. [10]

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

Sink Hole – Taking on more routing than needed, forcing data thought self; becoming an overly critical network node [11].

Traffic Analysis – Patterns of routing messaging and resultant message storms can divulge network topology. Some nodes might be in a silent mode. Hostile route requests can cause “silent” nodes to chat. Behavior of nodes for given algorithms can lend insight to node type

4.2 Attack Categorization by Threats

Many of the attacks share common vectors that allow them to achieve their ends. Understanding how these attacks function allow for better placement of defensive mechanisms.

Table 3 Threat Vulnerability in a MANET Network

Threats	3GPP Wireless Threats [12, 13]	MANET Specific Threats	MANET Specific Attacks
Masquerade	Peer Masquerade	Peer Masquerade	Sybil Attack / Impersonation Man In The Middle
Disclosure Sensitive Information	Traffic Analysis	Traffic Analysis	Predictive behavior, easier classification. Routing causes “silent” nodes to chat.
	Eavesdrop	Not MANET specific	
Unauthorized Modification	Traffic and Data Manipulate	Route disruption	Alter Radio Routes Replay Route altering
		Refusal to Participate	Black and Gray hole
Denial of Service	Physical Intervention	Jamming	Routing message jamming Central node jam
	Protocol Intervention	Denial of Service	Selective Drop / Gray Hole Rushing JellyFish Flooding – Greeting / Storm
	Data Masquerade	Data Masquerade	Loop forming Spoofing Black Listing
Unauthorized Use of Services	User Masquerade	Not MANET specific	
Repudiation Certainty	Charging Traffic Origin and Delivery	Not MANET specific	

Of the attacks listed, a few are passive in nature. Traffic Analysis only requires the attacker to view and sort on energy. For Refusal to Participate (Black Hole, Gray Hole) attacks, the attacker minimizes or reduces its participation; The selfish node also attacks by passive means, by not actively assisting in routing.

In 2001, the 3GPP security working group published a threat analysis applicable to wireless communication. These threats provide a structure to map available attacks. By their nature, MANETs have a subset of the 3GPP threats. They also have threats that are specific to the MANET routing algorithms. The first column of Table 3 contains the 3GPP general category of threat. Column 2 contains the 3GPP working group sub category. Columns 4 and 5 further distill this information classifying MANET specific attacks and MANET specific threats.

4.3 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. Table 4 gives an abbreviated sample risk assessment.

Table 4 Mapping of Assets at Risk from Threats

Assets	Peer Masquerade	Traffic Analysis	Route Disruption	Refusal to Participate	DoS and Jamming	Data Masquerade
Energy	Y		Y	Y	Y	Y
Computational Resources	Y		Y	Y	Y	Y
Bandwidth	Y		Y	Y	Y	Y
Gateway Access	Y		Y		Y	
Payload Data					Y	
Routing Data	Y		Y		Y	
User Identity		Y				
Location Info		Y				
Repudiation	Y					Y

The level of threat to the assets is a function of the specific deployment; it is a study that should be done for each design. Such a level assessment allows for proper placement of Information Assurance means.

5. INFORMATION ASSURANCE

The National Security Agency defines Information Assurance as the set of “measures intended to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality,

and non-repudiation”.[14] These five features, availability, integrity, authentication, confidentiality, and non-repudiation are the backbone of protecting information resources.

Confidentiality: Mechanisms restricting the disclosure of information to those who are authorized. Confidentiality mechanisms may be provided through symmetric cryptographic means, where the intended recipient holds of a secret, such as a key, that together with a designated encryption algorithm can decrypt the data.

Integrity: Mechanisms validating information has not been modified since transmittal; there are two broad methods of providing integrity: keyed hashes and digital signatures.

Keyed Hashing: both sides share a secret. The sending party creates a one-way hash mechanism that includes the data and the shared secret; it sends this hash to the intended recipient. The recipient performs the same action with the data and compares the result with what was received. If the two match, the recipient has assurances that the data has not been modified since transmission.

Digital Signatures: Digital signatures rely on asymmetric cryptographic methods. The sending party performs a one-way hash on the data, “signs” the result with his private key then sends both the protected hash and the data to the recipient. The recipient, using the sender’s public key, decrypts the hash and compares result to his own hash of the received data. If the two match, the recipient has assurances that the data has not been modified since “signing”.

Authentication: Mechanisms confirming the purported source of information was the actual source. Authentication is usually provided using the same mechanisms for integrity (keyed one-way hashes or digital signature).

Identity Trust through Third Parties: Mechanisms allowing a trusted third party to attest to a claim made by a second party; the most commonly used method is a digital certificate. A digital certificate is a binding of a public key to an individual through the digital signature by the trusted third party. The binding may also include attributes, identifying possible key usage, e.g. key encryption, digital signatures, and non-repudiation.

Third Party Authorization: Mechanisms indicating permissions granted by an authority. The mechanism most applicable to a MANET environment is a variation of a digital certificate called an attribute certificate. An attribute certificate binds not only an entity to a public key but also

includes attributes, identifying the authorities that have been granted to the holder by the issuer.

Non-Repudiation Security Services: Mechanism preventing an entity from denying having attested to a particular action related to data. The most common method of non-repudiation is through digital signatures that have been bound to individuals through public certificates.

5.2 Additional Support

Intrusion Prevention: Provides a means of actively detecting malicious node behavior, be it internal or external, and then acting accordingly. The nature of MANET routing, where traffic flows are available to multiple nodes, lends itself well to detecting attacks since the attacks or their behaviors are propagated throughout the network.

Audit Logs: Proper recoding of security related actions, actions beyond those related to data/traffic.

Waveform Selection: Waveforms have differing characteristics and the differing characteristics affect their susceptibility to attack. Low Probability of Interception, Low Probability of Exploitation, Low Probability of Detection, Low Probability of Jam, are examples of mechanisms that protect against attacks. The IA benefits of a waveform must be considered when choosing a waveform for MANET network deployment.

Routing Algorithmic Robustness: MANET networks are cooperative in nature. Each node is expected to obey the rules of the routing protocol and perform functions in accordance with those. To protect the network from rogue nodes, the protocol must have built in techniques that monitor for bad or deficient behavior and respond when such behavior is detected.

6. MANET INFORMATION ASSURANCE SECURITY POLICY

Section 5 discussed current technology that supplies counter-measures and mechanisms that can be used to address various classes of threats. Specific classes of mechanisms counter specific classes of threats. The selection of specific mechanisms used to counter specific classes of threats comes under the heading of MANET network security policy and specific to the environment.

The MANET network security policy outlines the rules for SDR access to a MANET network, determines how the rules are enforced, and lays out some of the basic architecture of the MANET security environment. In essence, MANET security policy dictates proper operations of an SDR device in a MANET environment. The policy dictates the specific IA mechanisms that should be used to

supply protection to the MANET resources that the threat analysis determined needed protection.

6.1 MANET Asset Protection Analysis

The analysis done in sections 3 and 4 showed the device and user identity and location, transport services and MANET resources were vulnerable assets and subject to attacks.

6.1.1 Protection for Device and User Identity and Location

As discussed in section 3, the attributes of identity and location assets are: privacy, reputation and authority.

Protection of Privacy: Privacy is generally protected through confidentiality mechanisms. Identity and location information is disclosed on a need to know basis and never sent over the network in the clear. Those who need to know must share a secret with the peer, one that may be used to generate a cryptographic key shared only by the two.

Reputation: Surprisingly, reputations are protected by non-repudiations services. An individual is protected from others claiming to be them and committing harmful or disreputable acts under that claim because the imposter cannot forge the individual’s digital signature.

Authority: Authority is protected through digital signatures and attributes certificates. Given a signed request and an attribute certificate from a trusted third party, a recipient of the request is guaranteed that the signer issued the request

6.1.2 Protection for Transport Services

Intended recipient: Currently, there are no technical solutions that guarantee that a packet is not misdirected to an unintended recipient: but if confidentiality services are used, the received information is rendered nearly useless to the unintended recipient.

Reliable source: Authentication services guarantee that the data originated form the sender. Keyed hash mechanisms are particularly efficient in the MANET environment.

Privacy; Privacy is generally protected through confidentiality mechanisms. As long as the transmitting receiving peers share a secret that is not held by others and use proper cryptographic services, the traffic is protected form disclosure to unintended third parties.

Integrity: Integrity of data in transit is protected by integrity mechanisms. As with reliable source, keyed hash mechanisms are particularly efficient in the MANET environment.

Waveform IA: Waveforms come with their own built in IA mechanisms, some better than others. These mechanism protect the reliability of physical and link layers.

Routing Protocol Rule Enforcement: Routing protocols have their own mechanism for detecting, responding and eliminating rogue nodes.

6.1.3 Protection for MANET Resources

Network Control: Authentication and integrity mechanisms assure peers that the information exchanged between them has not been modified in transit by a malicious intermediary. Other methods must be used when a member of a network goes rogue.

Platform Resources: As with network control, authentication and integrity, mechanisms assure that transported information comes from and goes to peers. But a peer can turn rogue. Methods other than cryptographic must be used to counter rogue network nodes. At a minimum, policy should limit the amount of resources that is dedicated to shared MANET activity.

Table 5 summarizes the attributes and associated protection mechanisms.

Table 5 Asset Attribute Protection Mechanism

SDR Asset/Resource	Value	Protection Mechanisms
Device and User Identity and Location	Privacy	Confidentiality
	Reputation	Non-repudiation
	Authority	Digital Signatures and Attribute Certificates
Transport services (Traffic)	Intended Recipient	Confidentiality
	Reliable Source	Authentication
	Privacy	Confidentiality
	Integrity	Integrity
	Reliable Delivery	Waveform IA features Routing Protocol Rouge Node Detection and Response
MANET Resources	Network Control	Integrity, Authentication, Intrusion Detection and response
	Platform Resources	Intrusion Detection and Response Policy

6.2 MANET Security Policy Development

In general security policies dictate: the IA mechanisms that must be used to protect assets, how they are applied and the

required quality of those mechanisms. The MANET security policy specifies defense in depth including: information assurance protocols cryptographic algorithms, key lengths, key generation support functions such as random number generators, acceptable certificate authorities, intrusion detection and response, mandatory waveform IA features, mandatory MANET protocol rouge element detection and response features, auditable events, access control, and the level assurance – the quality of the protection mechanisms.

6.3 MANET Security Policy Requirements

The completed analyses should produce a set of security policy requirements that weave required IA mechanisms and assurance levels into a context that supplies protection in depth, e.g., the required specific IA mechanisms and countermeasures to supply protection in depth. These requirements guide both developers and evaluators and can be scrutinized for weaknesses and deficiencies before development begins. They also give third parties a measure of confidence that the resulting platform has sufficient IA features to protect users and user data.

7. CONFLICTING INFORMATION ASSURANCE NEEDS IN MANET ENVIRONMENTS

The analysis needed to develop a quality security policy is complex. SDR operate in a resource limited environment. Tradeoffs must be made between costs and quality of protection.

7.1 Effectiveness vs. Overhead

SDR bandwidth, battery life, computational resources and memory are limited. These limits should be reflected in the selection of IA mechanism and counter measures. The chosen protection mechanisms must be reasoned and justified. Placing excessive resource demands on the platform or bandwidth to satisfy security is not practical.

7.2 Ad hoc and trusted third party

Developers of security policy may need to make assumptions about environmental support. A true ad hoc network may have no connection to the wider world nor may it have any assumed infrastructure support such as certifying authorities. Without such support, the conditions for some security mechanisms are not satisfied and the security policy must not be dependent up their availability.

Other MANET environments may have access to the wider internet or may come preconfigured with needed support features such as trust anchors for certificate validation. It is a reasonable choice to restrict the operations of an SDR to those MANET environments that support a basic level of infrastructure support.

7.3 Costs vs. Assurance Levels

Assurance levels dictate the quality of the IA mechanism and counter measures, but quality is not free. Assurance levels of implementation must not be so burdensome that costs associated with obtaining the assurance level becomes prohibitive.

As a rule of thumb, the cost of security should never exceed the value of the assets being protected.

8. INFORMATION ASSURANCE NEGOTIATION

Section 7 discussed a few of the tradeoffs that must be made when developing a security policy. It is highly unlikely that all developers of SDR security policies will arrive at the same security policy. A one size security policy does not fit all MANET devices. By necessity, MANET peers are required to negotiate common security policy for the MANET network, i.e., IA mechanisms, to supply a level of protection acceptable to all.

To permit reaching a common agreement on the security policy that governs the MANET network, SDR security policy must permit a level of flexibility as to acceptable MANET IA mechanism. Different SDRs may have digital certificates issued by a certifying authority but may be willing to accept certificates offered by a different authority. Multiple cryptographic algorithms and security protocols may need to be supported. Security policy developers must consider and balance flexibility, complexity of implementation, and required level of security.

Negotiating a common security policy is tricky even in the best of circumstances. MANET networks have a transitive attribute that affect negotiations. The security policy A negotiates with B may restrict the policy B may negotiate with others. A may agree to carry traffic generated by B but may not agree to forward the traffic B is forwarding for others. A may insist on a level of assurance that B can meet but in meeting that level of assurance B is prevented from forming a common security policy with C. A thorough analysis of acceptable negotiation protocols can prevent unpleasant but foreseeable consequences.

9. USE OF ESTABLISHED STANDARDS

Any discussion of information assurance in a MANET environment would be remiss if it neglected some discussion of standards. Standards supply the means for negotiation and establish a basis for a reasonable level of assurance.

9.1 Standards and Negotiation

As previously outlined, there is a need to negotiate security policy that is acceptable to all in the MANET network. Such negotiations cannot take place without a basis for agreement

upon particular IA protocols and cryptographic algorithms, e.g., defined through standards. Mutually supported standards do not guarantee all parties will reach mutual agreement, but the lack of protocols supported by both virtually guarantees parties cannot negotiate, putting a common security policy beyond reach.

9.2 Standards and Assurance Levels

Poorly architected security harms more than helps, giving system users a false sense of security. Building security protocols and cryptographic algorithms from scratch requires particular expertise and considerable experience. Public vetting is required before a protocol or algorithm is accepted by the IA community. Claims of keeping a protocol or algorithm confidential for security reasons are usually met with suspicion. Usually, a protocol or a cryptographic algorithm becomes a standard only after such a review has taken place.

9.3 IA Standards for an SDR MANET Environment

An SDR developer wishing to implement security policy requirements through standards will be faced with a plethora of choices as many standard bodies have and are developing security standards; developers need guidance.

Fortunately, the very characteristics of MANET networks help reduce the number of potential candidates. Security protocols that need access to central servers for authentication services must be excluded. Access to the wider Internet is not assured and IA techniques that depend on access are inappropriate for the MANET environment. Commercial waveforms may come with built-in IA features but the history of security in commercial waveforms is lacking. Applications, and related application level security protocols are too specific and not all platforms will support all or even any one common application.

9.3.1 IP Based Security Protocols

This paper assumes that all future SDR platforms will support either IPv4 or IPv6 protocols. Industry direction supports this assumption. [15] If all platforms support IP, then IP based security protocols form a strong basis for mutually supported security protocols. IPSEC [16 – 21] defines standard formatting for encrypting, authenticating IP packets between peers and encapsulating the result. IKE [22, 23] defines a policy negotiation and key agreement protocol between peers. Both are IETF examples of some of the IETF standard for IP based security. Selection of IPSEC and IKE brings additional advantages and can be used to protect both user traffic and MANET control information.

9.3.2 Suite B Cryptographic Protocols

The IPSEC standards support a range of cryptographic algorithms. Since most platform implementers will want to

minimize implementation efforts, if all SDRs are to support one set of cryptographic algorithms then that set should be viewed as strong by the cryptographic community. Fortunately there exists such a set commonly called Suite-B [26]. Suite B includes an encryption algorithm (AES [27]) a digital signature algorithm (ECDSA [28]), a key agreement algorithm (EC Diffie-Hellman or Elliptic Curve MQV [29]) and a one-way hash function (SHA 256 and SHA 384 [30])

9.3.3 X.509 Certificates

Mutual authentication of peers without access to the wider Internet requires that each node carry credentials that others can use to authenticate the node. The credentials must be:

- Provided by a trusted third party. Who qualifies as a trusted third party is an operational issue.
- Validated without contact with the issuer.
- Readable by the other.

Certificates fit these criteria. It is signed by a CA so the holders of the CA's public key can verify the signature. Only the holder of the corresponding private key can use the certificate, and certificate standards have a well defined format and syntax. The most commonly used certificate format is the X.509 standard [30].

10. SUMMARY

As the above analysis shows, developing a suitable protection profile for SDRs operating in MANET environments is both complex and critical. Care should be given analyzing what is of value, what needs protection, from whom and how. The how must not be done in a vacuum. Cooperation is the key to MANET network; this cooperation extends to security policy development. Standards are a key to successful cooperative agreement on common security profile for ad hoc networks.

Fortunately for the industry, existing standards of IPSEC, IKE, Suite B cryptographic algorithms and X.509 certificates go a long way to providing much of the needed IA protocols, cryptographic algorithms and third party credentials needed to secure MANET environments.

12. REFERENCES

- [1] D. Hart, "A Brief History of NSF and Internet," *National Science Foundation*, August 2003, http://www.nsf.gov/od/lpa/news/03/fsnsf_internet.htm
- [2] S. Corson, and J. Macker, "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations," *IETF RFC 2501*, January 1999
- [3] E. Thibodeau, M. Youssef, and A. Houle, "Investigating MANET Performance in a VoIP Context." *IEEE 2006 Canadian Conference on Electrical and Computer Engineering*, May 2006
- [4] Y.B. Ko, and N.H. Vaida, "Locations-Aided Routing (LAR) in Mobile Ad Hoc Networks," *Wireless Networks*, vol.6, no 4, pp.307-321, 2000

- [5] P. Beckman, S. Verma, and R. Rao, "Use of Mesh Networks for Inter-Vehicular Communication," *IEEE Vehicular Technology Conference*, vol.4, pp.2712-2715, 2003
- [6] 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
- [7] 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
- [8] I. Aad, J. Hubaux, and E. Knightly. "Denial of Service Resilience in Ad Hoc Networks," *ACM MobiCom*, September 2004
- [9] M. Brumster, and T. Le. "Optimistic Tracing in MANET," Florida State University, Department of Computer Science, March 2006
- [10] 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
- [11] A. Burg. "Ad hoc Network Specific Attacks," *Ad hoc networking: Concepts, Applications and Security Seminar*, Technische Universität München, 2003
- [12] 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
- [13] D. Murotake, and A. Martin. "System Threat Analysis for High Assurance Software Defined Radios," *SDR Forum*, November 2004
- [14] FAQ 1 Information Assurance Recently Asked Questions. National Security Agency Central Security Service <http://www.nsa.gov/ia/iaFAQ.cfm>
- [15] Evolution of 3GPP System; 3GPP TR 21.902 V6.0.0 (2003-09)
- [16] RFC 4302 IP Authentication Header. S. Kent. December 2005
- [17] RFC 4303 IP Encapsulating Security Payload (ESP). S. Kent. December 2005.
- [18] RFC 4304 Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP). S. Kent. December 2005
- [19] RFC 4305 Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH). D. Eastlake 3rd. December 2005.
- [20] RFC 4308 Cryptographic Suites for IPsec. P. Hoffman. December 2005.
- [21] RFC 4309 Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP). R. Housley. December 2005.
- [22] RFC 4306 Internet Key Exchange (IKEv2) Protocol. C. Kaufman, Ed. December 2005.
- [23] RFC 4307 Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2). J. Schiller. December 2005
- [24] RFC 4306 Internet Key Exchange (IKEv2) Protocol. C. Kaufman, Ed. December 2005.
- [25] RFC 4307 Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2). J. Schiller. December 2005
- [26] Fact Sheet NSA Suite B Cryptography. National Security Agency Central Security Service http://www.nsa.gov/ia/industry/crypto_suite_b.cfm
- [27] Advanced Encryption Standard (AES) Federal Information Processing Standards Publication 197 November 26, 2001
- [28] Digital Signature Standard (DSS) Federal Information Processing Standards Publication 186-2 January 27 2000
- [29] Recommendation On Key Establishment Schemes NIST Draft 2.0 Special Publication 800-56 January 2003
- [30] Secure Hash Standard Federal Information Processing Standards Publication 180-2 August 1 2002
- [31] ITU-T Recommendation X.509 (1997 E): Information Technology – Open Systems Interconnection – The Directory: Authentication Framework, June 1997