

Threat Modelling for Mobile Ad Hoc and Sensor Networks

John A. Clark, John Murdoch, John A. McDermid, Sevil Sen, Howard R. Chivers, Olwen Worthington and Pankaj Rohatgi

Abstract— A threat model for sensor networks and mobile ad hoc networks (MANETs) is introduced. Components that can be used to form an *adversary model* are developed. Threat categories, modes of use, and a variety of threats to system assets are identified, including threats to communications, infrastructure services, individual nodes and human users. Example envisaged applications of the threat model are discussed, covering threats to secure information flows, to threshold and identity based cryptography and to risk and trust management.

Index Terms—threat modelling, MANET security, sensor network security

I. INTRODUCTION

AD HOC NETWORKS promise benefits in many types of application. Sensor networks can provide useful and cost-effective monitoring in many domains, e.g. environmental pollution, wildlife behaviour, circumstances of vulnerable people, and the state of at-risk (e.g. on fire) buildings. Mobile ad hoc computing is becoming increasingly important, including next-generation mobile phone systems, urban wireless networks, and support of dynamic coalitions of international military and humanitarian task forces.

It is expected that various types of agency and mission will depend significantly on the appropriate operation of ad hoc networks in demanding security threat environments. We need to understand the security issues involved and develop technologies to facilitate the engineering of practical systems with demonstrably sufficient security. Security risks have to be considered in the context of operational benefits. Resources are inevitably limited and we must deploy security

J. A. Clark is with the Department of Computer Science, University of York, York YO10 5DD UK (corresponding author: 44-190-443-3379; e-mail: jac@cs.york.ac.uk).

J. Murdoch is with the Department of Computer Science, University of York, York YO10 5DD UK (e-mail: murdoch@cs.york.ac.uk).

J. A. McDermid, is with the Department of Computer Science, University of York, York YO10 5DD UK (e-mail: jam@cs.york.ac.uk)

S. Sen is with the Department of Computer Science, University of York, York YO10 5DD UK (e-mail: ssen@cs.york.ac.uk).

H. R. Chivers is with Cranfield University, UK (e-mail: hrchivers@iee.org).

O. Worthington is with DSTL, MOD, Malvern UK (e-mail: olworthington@dstl.org.uk).

P. Rohatgi is with IBM T.J. Watson Research Center, Yorktown Heights, NY (e-mail: rohatgi@us.ibm.com).

measures in a manner that enables mission accomplishment with tolerable risk. Operational requirements for flexibility mean that we must choose security measures in a way that appropriately reflects the contexts in which the system will be deployed.

Threat modelling has emerged in recent years as an essential component of achieving cost-effective security. Many papers have been published on the topic together with a popular book [26]. A threat model identifies assets and threats to them, and considers how such threats may be realized. In this paper, we provide a threat model applicable to two types of ad hoc network: mobile ad hoc networks (MANETs) and sensor networks. In practice, we envisage many deployments of ad hoc networks involving governmental agencies to mix these types of network.

II. THREAT MODELLING

A variety of domain specific threat models have been developed: e-voting systems [4] [5] [6], high performance cluster (HPC) platforms [10], smart cards [34], software defined radio [7], insider threats [8], mobile phones [15], and secure data storage [9] [11] [12]. Traditional threats, such as those arising from data remanence, have also been addressed [13] [14]. Let us first consider the state of threat modelling with respect to the networks of interest.

A. Sensor Networks

Many applications are envisaged for sensor networks, in civilian and military domains. The number of applications will grow as sensor technology becomes cheaper and more sophisticated. The extent to which sensors can be protected (or can protect themselves) against compromise is limited. Sensors, once deployed *in the wild*, are vulnerable to capture and compromise.

Some useful threat work has appeared in the literature. Anand *et al* [20] indicate relevant properties of sensor networks: tree-structured routing; data aggregation; tolerable failures; in-network filtering and computation; sensors as routers; and phased transmission periods. All these features give rise to threats and challenges. Anand *et al.*'s attack model is based on adversary goals, categorized as eavesdropping, disruption and hijacking. Karlof *et al* [21]

provide an extensive set of attacks on current sensor routing together with countermeasures, identifying and describing various network level attacks: spoofed, altered, or replayed routing information; selective forwarding; sinkhole attacks; Sybil attacks; wormholes, HELLO flood attacks; and acknowledgement spoofing. They also identify attacks on specific protocols: TinyOS beaconing; directed diffusion; geographic routing; minimum cost forwarding; low-energy adaptive clustering hierarchy; rumor routing; and energy conserving topology maintenance (GAF, SPAN). The adoption encrypted communications affects greatly the applicability of attacks described. For deployment of governmental agency networks we might assume some degree of protection.

Captured sensors may be deconstructed and examined or else compromised by less sophisticated methods such as RF pulsing to cause circuitry to be disabled or destroyed. The time needed to compromise a mote by sophisticated means may be too great. An interesting account of the current feasibility of physical compromise can be found in [22].

There is a fair amount of work around on threat models for sensor networks, but it is distributed across various papers.

B. MANET Threat Modelling

There would appear to be less literature around on threat modelling for MANETs. Spiewak et al [25] have produced a MANET threat model targeting confidentiality, integrity, availability and anonymity (CIA). The CIA part is fairly traditional in threat models, but the paper reminds the reader of the importance of anonymity in many MANET deployments. The paper places some stress on the adversary model (a theme which we pick up and significantly extend below).

C. What Matters in Ad hoc Networks

There are a great many possible threats to MANETs and sensor networks. However, some of features of MANETs may reduce risks of successful attack. For example, the sensitivity of information may decay rapidly due to the fast changing nature of MANET node deployments. The practical feasibility of realizing some identified threats is unclear. Such issues are clearly important from a rational risk perspective and impact on the development and configuration of *ad hoc* systems and accreditation policy regarding them. These issues are outside the cope of this general paper. The specific risks taken depend very much on the specific adversary model chosen.

D. General Observations

Many papers address threat modelling *in some way*. A few papers have introduced elements of methodological rigour, most typically in the form of lifecycles, either operational lifecycles or data usage lifecycles. It is also clear that real threat analysis for many systems requires skills outside the traditional computer systems based evaluator's experience. For example, knowledge of physics is required for meaningful

arguments about data remanence; physical compromise of sensor motes requires engineering/physics knowledge; analysis of certain aspects of software-defined radio will likewise require specific expertise; and so on.

III. AD HOC NETWORK THREAT MODELLING

Threat models reported in the literature provide broad structuring mechanisms that are often driven (rightly) by convenience; the aim is to chunk information in a way that is deemed useful to the analyst. We too have adopted pragmatic partitioning conventions. Our aim is to provide an intellectual framework in which to carry out threat modelling.

There is a clear distinction between a threat and a mechanism by which it is realized. Examples of how threats may be effected are provided, to illustrate that identified threats are really of concern. We structure our presentation as follows:

Threat types: This identifies the basic types of damage that can be wrought on network assets.

Modes: These characterise major aspects of context, entailing different operational security regimes.

Adversary Models: The capabilities of the adversary significantly affect the threats that may be manifested.

Finer Partitioning of Threats: A network comprises a set of nodes and users together with communications between those nodes. Services of various forms may be provided. We partition consideration of threats as follows:

Network Communications Threats: Threats arising from manipulation of network communications; mostly packet stream monitoring and manipulation here. As noted earlier, access to the (broadcast) medium is trivial.

Service Provision Threats: This includes threats arising from application-specific service provision and from general infra-structural services. Infrastructural services may be common across many MANETs, and include reconfiguration services, or various security-related services such as audit. Services may be end-to-end, or effected in a distributed collaborative way.

Node Compromise: Threats arising from node compromise. This covers what happens when the assumptions relating to node operation are compromised in some way, e.g. by physical compromise.

Human Factors Threats: These are threats involving people in some immediate way, ranging from malicious insider actions through to overloading of well-intentioned but stressed operational staff. People are involved throughout the lifecycle of an ad hoc network and threats may arise at any point.

Our structure aims to be *useful* and to convey some confidence in completeness. We expect threat models for specific systems to augment what is presented here; the model below is a good place for analysts (and ad hoc network security researchers) to start.

IV. TYPES OF THREAT

Researchers have generally considered threats under categories such as: confidentiality; integrity; authentication; availability; and anonymity.

Confidentiality of information has received historically the greatest attention in the literature. Ad hoc networks can be expected to create and maintain significant amounts of sensitive information. Its sensitivity will often be more time-dependent than in other systems; sensitivity of information in MANETS may decay much more rapidly than in other types of systems. (Information on yesterday's troop locations will typically be less sensitive than information on today's.) This is an important and repeatedly occurring feature in MANETS due to the general mobility of system elements. System operations may also involve a variety of aggregating services that further impact on sensitivity of maintained data. Although real-time attribution of accurate sensitivity may require careful consideration, at this point we simply observe that threats to the confidentiality of assets are as important in ad hoc networks as elsewhere. Threats arise also from the pervasive wireless operation of such networks. Eavesdropping, for example, is clearly facilitated by the broadcast nature of the system.

Integrity is a complex property and there have been very many definitions capturing various aspects of it. Integrity addresses issues such as: Has data been accidentally or deliberately corrupted? Does the digital data model reflect important aspects of the real-world appropriately? Has the data been computed by trusted sources? Is its quality sufficient? Is the model 'stale'?

Mechanisms used to provide integrity guarantees vary in sophistication. Good CRCs often suffice for accidental corruption of data. Cryptographic checksums can be used to counter deliberate modification. Other aspects might require that suitably authorized agents modify data using only trusted routes. (For example, an ATM allows you to manipulate your bank account details and balances, but you will not be allowed direct access to disks!) Various levels of data have to be considered including, for example, low-level apparent data and metadata, capturing information on the properties and history of the low-level data. Provenance of data will be crucial in ad hoc network decision making. We will often be faced with making decisions on the basis of incomplete data from sources of limited trustworthiness. Effective decision making requires us to be aware of aspects of the quality of received information. Protocols for ensuring provenance will play an important part in ad hoc network operation.

Authentication in general is about the verification of properties concerning the origin and subsequent handling of messages or data. These can refer to users (where authentication mechanisms link claimed identity to real world users), to messages and data, e.g. to message source (data origin authentication), to a peer process, or to claims about provenance (an historical account of information and the

operations performed on it). Almost all authentication protocols invoke the use of cryptographic algorithms in some way. Authentication presents a particular threat in ad hoc networks since we will generally be without many traditional authentication and trust infrastructures. We may have to accept reduced confidence in claims made simply because the consequences of rejecting them may be operationally damaging.

Availability is more straightforward. Inability of legitimate users to access services is a clear problem. Denial of Service (DoS) attacks have become one of the most worrying problems for network managers. In a military environment, a successful denial of service attack is extremely dangerous, and the engineering of such attacks is a valid modern war-goal. In military networks, time criticality of response means availability is a major requirement. The interval over which availability is compromised may vary. In some cases the goal of an attacker will be to deny service for as long as possible. In other cases, a more sophisticated timely and short-term interruption may be the goal. Disruption of a few seconds or less may render near-range anti-missile systems useless.

Anonymity is important in some military applications, though its interpretation requires a little subtlety. There are degrees of anonymity. The most desirable may be to operate without being detected. (Radio silence of naval operations is a classic example of attempting to achieve this.) Failing that, preventing knowledge of one's specific operation is desirable. Being identified as a critical node is a serious breach of anonymity – command nodes may be attacked, sensor network base stations may be subject to jamming, and so on. Although anonymity is something of a Cinderella property in much security research, it has real significance for military ad hoc networks.

Work within the ITA has identified effective *accountability* as a significant requirement. The availability of suitable accountability mechanisms have been identified as a significant enabler of flexible risk management. It deserves to be considered as a target of threats in its own right.

Conformance: Almost all threat modelling work starts with the fairly traditional categories such as those above. These are interpreted (reasonably) in fairly conventional ways. It is not too difficult to interpret what a breach of confidentiality is. However, the categories are really particular forms of damage that can be wrought on assets we care about. In a sense, an *agreement* between coalition partners is something whose integrity we want to hold. As coalition partners we agree to behave in certain ways and expect members to keep to agreements, even when there is no obvious or direct damage resulting from breaking elements of that agreement.

Such agreements are of such fundamental importance that threats to their integrity deserve to be identified in their own right. *Threats to conformance* will often prove a useful threat category.

V. MODES

Effective structuring of threat modelling is essential for complex systems analysis. Contextual differences or ‘modes’, where different security regimes may apply, provide one such partition. Typical military MANET modes are:

- Peace-time
- Transition to war
- Wartime

In each mode different guidelines apply regarding risk decision making. The modes effectively allow more focussed and context specific analyses to be carried out, acting as a high-level partitioning device for analysis. (Modes form a major part of many safety analyses: analysis of the safety of an airliner may consider: taxi-ing, path to point of no-return, flight after point of no return, ascent, descent, landing etc.) The analyst is free to invent further modes as convenient.

VI. ADVERSARY MODEL

We are interested in identifying possible threats and determining the corresponding risks. The risks to a system depend on the capabilities of the adversary. Assumptions of different capability will lead to different decisions being made by procurers, developers and operational personnel. In this section we identify factors regarding the adversary that we need to take into account when performing analysis; we significantly extend previous adversarial models for ad hoc networks.

Siewviak has suggested the following categories (for MANETs):

Passive/active: This is a traditional analysis partitioning device, used by many threat modelling researchers. Nodes may, for example, eavesdrop on traffic to collect information; no attempt is made to interfere with the host network’s operation. An active adversary may choose to interfere in some way, e.g. by modulating packet forwarding, injecting or replaying packets, by deliberately effecting MAC layer collisions, and so on. We distinguish active/passive *capability* from active/passive *attack strategy*. A passive strategy (e.g. gathering information for network mapping) may often be a pre-cursor to an active one (e.g. seeking maximally efficient disruption of the network).

Insider/outsider: This is a major discriminating characteristic. The ‘insider problem’ exists in all security application domains, and presents a particularly invidious problem. There is often a step change in potential damage that an adversary can cause with insider capability. Researchers have typically addressed this problem by adopting threshold protocols (e.g. m-out-of-n voting protocols) for secret sharing and aggregating application protocols. Analysis and system development is greatly simplified if we can rule out insiders but this seems improbable for dynamic coalitions.

Static/adaptive: In a pedantic sense the distinction is

somewhat arbitrary; a ‘learning’ algorithm in a node may be regarded as static. From a practical viewpoint, the ability of a network to learn in response to its environment will give a significant increase in adversary power. One may, for example, make an informed choice as to which node to compromise next to effect a particularly efficient attack.

Computational power: Computational power clearly affects the ability of an attacker to compromise a network. Such power need not be localised to the attacked network - eavesdropped traffic can be relayed back to high performance super-computing networks for analysis.

We believe that the adversarial model characteristics identified above can be usefully augmented:

Communications capability:

Communications may generally take place:

- via a network, according to the protocol
- via out-of-network-channel communications, or
- via both.

For eavesdropped information there needs to be a channel back home. Fast links between collaborating adversarial nodes may facilitate ‘wormhole’ attacks.

Deployment capability:

Single/multiple locations: Adversary distribution may range from a single node to a pervasive carpet of smart counter-dust, with a consequent variation in attack capabilities. This sort of distinction may affect the ability to eavesdrop, to jam a network effectively, and to escape destruction (e.g. a single powerful jammer can easily be taken out, distributed local jamming is harder to extinguish).

Location control: The location of adversary nodes may have a clear impact on what the adversary can do. An adversary may be restricted to placing attack nodes at the geographical boundary of an enemy network (but may otherwise choose the precise locations), may plant specific nodes (e.g. nodes left behind in territory about to be vacated), or may have the ability *post facto* to create a pervasive carpet of counter smart dust (where arbitrary degrees of pervasiveness may be achieved).

Mobility: This is a variation on the static/adaptive theme. Mobility generally brings an increase in power. (A mobile node can always remain stationary.) For example, an adversary with traffic rate monitoring ability may be able to move and ‘home in’ on a base station in a sensor network. The impact on detection is more complex, depending on the consequences of mobility. A fast-moving tank may soon be some distance away from the position of its last located RF broadcast but a vibration sensing capability may allow its movements to be tracked.

Ante/post facto deployment: For some ad hoc networks it may matter a great deal whether an adversary can pre-empt deployment of the network. In sensor networks there may be an initial self-configuration (e.g. involving topology determination and key establishment). These may take place freely in the absence of adversary action. A pre-distributed

counter network may render these important initial operations attackable.

Loci of malfeasance: Over what parts of the network can the adversary exert passive or active operation?

Ability to avoid detection: As noted above, a single powerful RF jamming node may be readily identified; passive monitoring with very occasional reporting back to base is harder to detect. Also, there are issues regarding sophistication with which nodes may evade sweeping attacks.

Perceived granularity of inference and influence: This is linked to the factors above. Highly restricted deployment may make inference much harder, and constrain availability attacks to specific areas.

Degree of physical access (including node capture ability, ability to carry out physical deconstruction and similar).

Given the agile nature of MANETs predicting an accurate adversary model is difficult. However, systems can be evaluated against a range of representative threat models.

VII. NETWORK COMMUNICATIONS THREATS

Here we are largely concerned about the analysis or manipulation of packets streams.

A. Threats to Confidentiality and Anonymity

Confidentiality and anonymity are related properties. Confidentiality typically is concerned with keeping data secret, whereas anonymity is often concerned with constraining access to contextual attributes, such as existence, identity, role and physical location. The distinction is somewhat a matter of taste.

Confidentiality of communications is subject to the same threats in MANETS as it is in networks in general, but physical access is no longer necessary with almost all communications being wireless. Traditional means of compromising confidentiality include:

Weak or compromised cryptography: The cryptographic algorithm used to protect inter-hop communications may be breakable. Communications may provide too much information, e.g. too much plaintext-ciphertext pairs can be inferred. A key may have been obtained by a malicious attacker.

Unencrypted communications: This may arise from willful disregard of procedures or else as a rational action taken in difficult operational circumstances. Broadcasting in the clear is straightforward leakage.

Inappropriate use of cryptography: Encryption must be used in an appropriate mode – the strength of crypto needs to be evaluated in the context of the particular communications protocols it is used to protect. Thus, use of sequence numbers as initialisation vectors in Cipher Block Chaining mode operation may provide an adversary with an arbitrary encryption oracle in various circumstances.

Disclosure due to side-channel usage: Encrypted traffic may still leak information. Thus, a malicious node may use

encrypted packet properties to encode information (e.g. length, destination, or timing of packet issue.)

Traffic analysis is well established in military circles. Traffic analysis in ad hoc networks may reveal:

- The existence and location of nodes
- The *communications* network topology
- The roles played by nodes
- Current sources and destinations of communications
- The current location of specific individuals or functions. If a commander issues a daily briefing at 10.a.m. traffic analysis may reveal a source geographic location
- Aspects of infrastructure operation, e.g. how the network copes with a node going down
- Aspects of computational and communications performance of a network and its nodes
- The intent and state of the organisation, e.g. that planning or negotiations are taking place, or that an attack is imminent
- Patterns of operational strategy or doctrine, e.g. as evidenced in peacetime practice manoeuvres. Traffic analysis of peacetime activities can be a source of very useful information too

Traffic analysis is not necessarily an entirely passive activity. It is perfectly feasible to engage in protocols, or seek to *provoke* communication between nodes.

We concentrate on the threats arising from traffic analysis, rather than the specific mechanisms used. The means may vary according to adversary sophistication. Techniques may include RF direction-finding capability; traffic rate analysis (e.g. in an aggregating sensor network with a shortest path (tree) routing to a base station); differences in traffic between nodes can readily reveal the topology (and by implication identify the base station); and time-correlation monitoring (where propagation of events through the network can be determined).

B. Threats to Integrity

Threats to the integrity of communications include:

- Environmental corruption of messages. This may be due to the natural environment, or else to specific actions taken by an adversary, or by interference by collaborating materiel.
- Malicious modification, replay or insertion of packets. This is the traditional integrity attack.
- Threats arising due to software errors in the communications stack.

C. Threats to Availability

Networks are by nature heavily dependent on protocols of one form or another, and consequently integrity and availability compromise of such communications is major threat. Threats include:

Selective packet forwarding: Nodes may act as a sink, forwarding no received packets, or else be more sophisticated, targeting specific sources, destinations or even particular packet types. At the extreme, complete packet dropping gives complete denial of service. A considerable number of related attacks work on current service protocols (e.g. routing) (but rely on unprotected communications and so we omit details here).

Impaired QoS: Denial of Service (DoS) attacks have proved to be a major problem for network managers in recent years. However, denial of service is the extreme end of a spectrum. In fact, denial of service may, in some circumstances, be a technique to achieve another goal. For example, sophisticated disruption of communications in a smart dust network during its topology discovery and configuration phase may produce a highly inefficient network communications structure.

Jamming attacks: A straightforward consequence of wireless communication, RF jamming presents an obvious and highly powerful form of denial of service. Forms of spread spectrum communications present the most popular defense approach together with jamming detection and reconfiguration where possible.

Medium hogging: An insider node can request bandwidth at a rate that denies a fair chance of access to the medium by other nodes. A malfunctioning node may do so similarly.

D. Threats to accountability

Manipulation of the packet stream destined for an audit service would seriously compromise accountability. Straightforward packet dropping could lead to no record of specific actions taken. Any ability to spoof, or replay audit packets could also interfere with accountability.

Accountability for communicated messages might be compromised if assumptions about underlying cryptographic mechanisms break down (e.g. by the release of private keys).

VIII. INFRASTRUCTURE AND SERVICE PROVISION THREATS

Secure operation of a MANET may rely on basic underlying services:

A. Threats to Confidentiality and Anonymity

Service provision may leak information in a variety of ways:

Direct and covert communication: Malicious or compromised applications may choose to leak sensitive information via accepted protocols. One way in which this can be achieved is by the use of steganographic channels. An interesting aspect here is that leakage could very well be effected even in the presence of overt checking for good behaviour.

Side channel leakage: Side-channels (e.g. response times) may be used by clients to infer aspects of the servers' loading. Servers may also gain knowledge as to the intentions of a node by the services they request.

B. Threats to Integrity

Attacks on the integrity of a time service: Many security protocols and mechanisms rely on the integrity of a time service. Typical examples include key distribution.

Attacks on security related services: A variety of security related services will need to be implemented in ad hoc networks. Reputation-based approaches to trust attribution form an important part of many commercial systems, e.g. eBay and SlashDot. Reputation calculation by reference to direct experience and to secondary referrals offers one possible workable interpretation of *trust*. However reputation-based approaches provide opportunities for attack including:

- Exploiting start-up reputations.
- Collusion by a set of nodes to isolate a target.
- Collusion by a set of nodes to enhance each other's reputations.
- Building up a reputation by good behaviour and then striking for a specific purpose.

Environmental Manipulation: MANET nodes will combine to provide various services. A common service will involve distributed sensing and data fusion. Modulating the sensed information to prompt the derivation of a misleading inference poses a significant effect.

Aggregation Service Collusion Threats: If nodes are compromised in some way then information communicated by nodes may be misleading. This may apply to services involving sensing (as described above) but also may be much more pervasive.

C. Threats to Availability

Denial of Service Attacks: Services located at a node may be subject to a variety of DoS attacks.

Resilience services: MANETs will often be dynamically reconfigurable. As networks partition, services may be dynamically relocated and services sought at other locations. Every resilience mechanism is an opportunity to bring about denial of services. By clever manipulation of communications for example, we could cause a system to repeatedly reconfigure, leading to a form of *resilience thrashing*.

Low request rate attacks: It may seem counter-intuitive but DoS attacks do not require bombardment of a service with requests. Consider a service with a request buffer. If new requests are received at the rate at which requests are serviced then the buffer may be maintained at its limit. A DoS attacker simply needs to send appropriately timed requests to deny service availability to legitimate users. Buffers at many layers may be subject to attack.

Compute intensive service requests: Other low volume attacks may be envisaged, e.g. service requests that are highly computationally intensive.

Security Service Attacks: Security services themselves present opportunities for attack. Increased security (i.e. more constraints) may be invoked in response to the detection of seemingly suspicious behaviour. This essentially acts as

partial restriction (denial) of service.

D. Threats to Accountability

Attacks on audit servers provide one avenue of compromise. Selective packet manipulation could also provide the same effect. One interesting aspect here is that threats to accountability may very well arise from insiders (e.g. to escape recriminations for reckless actions).

IX. PHYSICAL NODE COMPROMISE

Nodes may be compromised in a variety of ways. Equipment may simply be *taken* or otherwise fall into the hands of the enemy. This problem exists outside dynamic ad hoc networks and the countermeasures taken to prevent consequences vary. In some cases, equipment may be blown up to prevent useful information being revealed.

A. General Threat Considerations

Direct access to stored information: The most dangerous physical compromises are when the adversary is able to access secret information on the node or else is able to reprogram elements (or all) of it. This is a common worry in current mote implementations. This type of threat (to the integrity of the configuration of a node) can effectively compromise all asset properties (and so we extract this aspect before presenting threat specific issues).

B. Threats to Confidentiality

Confidentiality may be brought about by node compromise in various ways:

Environmental monitoring: Even when the node is adequately protected against invasive attacks (e.g. allowing memory or bus lines to be directly accessed) passive monitoring of the interaction of the security critical components with their environment may leak information. Thus, power supply trace data can be used to infer the internal computations of a chip and thus reveal sensitive information. Techniques such as simple and differential power analysis have show how specific secret information (e.g. secret keys) may be leaked in this way

Environmental manipulation: Nodes typically behave well within defined environmental envelopes. Forcing an out-of-specification environment may have unpredictable effects. Thus, the effect of power glitches, or low current supply, may be unpredictable. Even when nodes are protected to some degree against invasive attacks, there may be unusual environment-related actions that can facilitate compromise. For example, it is generally thought and taught that typical RAM loses its contents when power is removed. This may not be the case. It has been reported that lowering the temperature of the chip (e.g. to -30°C) may cause information stored to be maintained. On power up a register may assume the previously stored state. There are also issues of specific data becoming *burned* into the silicon.

The actual risks posed by the above will vary enormously.

Also, some attacks may prove possible but not practically feasible. If a MANET or sensor network is to be deployed with an expectation that it will be operational for a day, attacks using (for example) electron force microscopy in a laboratory will most likely pose little real risk. (Or rather, real immediate operational risk – the longer term risks may be more important).

C. Threats to Availability

There are many ways nodes can be physically compromised affecting availability. These include:

Physical destruction: Motes or small-scale materiel may simply be smashed or forcibly disabled.

Environmental attacks:

- Equipment may be highly susceptible to powerful *RF attacks*. At one extreme, a nuclear electromagnetic pulse may destroy or severely affect elements of unprotected electronic circuitry. But similar local effects can be achieved with fairly primitive equipment. We note in passing that localised ionising radiation attacks may compromise the integrity of the node. The consequences of such compromise will likely be unpredictable.
- *Power source attacks:* The rise of pervasive computing has seen some entertaining attacks occur on low resource systems. Sleep deprivation attacks occur when the environment (adversary) repeatedly engages with a node so that its response consumes batter power until it is wholly depleted.
- *Heat:* This may seem an unusual heading for an attack but we know that computing equipment is sensitive to its environment. Subjecting a node to temperatures outside its environmental specification may have unpredictable effects.

D. Threats to Node Anonymity

Physical node compromise may also pose threats to anonymity:

- There may be data referring to personnel stored at the node. This is a traditional interpretation of anonymity.
- The software (programs and data) loaded on the system may reveal aspects of system capability.

X. THREATS CONCERNING PEOPLE

We can regard people simply as system elements that provide particular ‘services’. The service provided may encompass the roles executed at all points in the chain of operation command and through all stages in the lifecycle of a MANET. In the context of ITA work, although considerable effort is being expended to arrange for decision making to be automated to as great an extent as is practical, inevitably some decisions will have to be propagated up and require

human interaction.

Two forms of human oriented threat may be identified:

- Threats to personnel
- Threats to non-personnel assets.

We can require particular behavioural properties of personnel, or ‘users’: confidentiality (of general information about who they are); integrity (is the user performing the role correctly?); availability (is the user able to carry out the required tasks?); authenticity (is the person performing the role who it should be); and accountability (can the user be held accountable for his actions?).

A. Threats to Confidentiality and Anonymity

Choices made by personnel may compromise confidentiality:

- Breaking with current policy (e.g. to resume wireless communications when radio silence is expected) or use of unprotected communications for sensitive exchanges.
- Carelessness with cryptographic keys;
- Harmful leakage of sensitive information to other people.

B. Threats to Availability

In safety critical systems, overloading the operator is a known problem, e.g. in the Three Mile Island incident there were over 100 alarms raised in under a minute. In security terms this may be regarded as a flooding attack on the human element. An adversary who knows the policy for requiring human intervention can seek to engineer behaviours that cause it to be requested.

As the Three Mile Island incident shows, a human decision making bottleneck may arise without malicious action.

We should not rule out individual parties choosing to deliberately (if temporarily) disengage - a form of self-imposed lack of availability.

C. Threats to Integrity

We may interpret issues of human integrity with some flexibility.

Personnel Compromise: The obvious threat to human integrity is when a user has been compromised and acts as an inside agent.

Poor Risk Decisions: Poor decision-making made in good faith is another interpretation. Quality of decision-making will depend on training, current context (stress etc.), and the way in which information is presented to the user. As research progresses, agreement should emerge about how security risk decision-making is best facilitated by a system.

Poor Management: The integrity of the system may be compromised under conditions of poor maintenance or management.

D. Threats to Accountability

Accountability is a well-established security requirement.

In a military situation significant responsibilities will be given to personnel. It is important that they discharge such duties in good faith, making appropriate risk decisions. Accountability is crucial to encouraging and ensuring acceptable behaviours. In many cases there will be no alternative to allowing decision-making flexibility on the ground, and post-operation review may be appropriate.

However, accountability relies on the availability of trail information to bind actions to people. Obvious attacks are to:

- Prevent accountability information being recorded in the first place.
- Seeking to destroy accountability information.
- We should not rule out the threat of modification of accountability information, e.g. to shift blame for reckless actions onto another party.

XI. FURTHER THREAT MODEL DEVELOPMENT

In this work we have largely identified threats to deployed or operational MANETs. In other work we have developed the concept of a *lifecycle* for a dynamic collaboration. This lifecycle covers the development of a coalition from identification of a common need to collaborate through to decommissioning. We propose to systematically visit each stage of the lifecycle to ascertain the threats throughout the lifecycle.

The lifecycle is useful as a means of partitioning analysis and interesting issues have already emerged from its preliminary use. General MANET literature emphasises parties coming together and then separating (and protocols have been developed to facilitate this). However, little thought has been given to what happens to residual information after a break-up. Threats may arise from how such information is handled by a partner post-coalition.

Party A may choose to collaborate now with party B but will have limited (if any) control over whom B collaborates with next.

XII. APPLICATIONS

In this section we outline some of the security related project work underway as part of the ITA Task 2. This work will expand and use the threat model presented here to assess the general suitability of techniques and approaches proposed.

A. Threat Analysis for Secure Information Flows

The secure information flows project is considering the flow of information from sources to consumers via a set of information transforms. It has been proposed to support risk-based security decisions by means of security metadata bound to data and data-transforms. The semantics of this security metadata will capture security properties such as confidentiality, integrity and provenance of data, including its time-sensitivity, as well as the information needs and requisite authorizations of users. Such an approach has been demonstrated for data flows in static and physically- and

logically-secured systems, where a Trusted Computing Base can perform the binding of data with metadata and maintain the metadata for information transforms. Significant effort is required to adapt this approach to MANETs, due to a very different threat and enforcement environment.

In a MANET environment, the integrity of the binding of metadata to data and to transforms cannot be assumed, due to the threat from physical and logical attacks that can corrupt both the data and the metadata. Such corruption can result in violation of confidentiality, integrity and availability requirements.

For data such as sensor data, which may be subject to tampering by an attacker, one will have to resort to circumstantial evidence from indirect and subjective observations, e.g., by others or by corroborating information from as diverse sources as possible. Realistic assumptions about the limitations of adversaries could be made. For example, even though adversaries can be expected to have advanced technical know-how and have to be considered Byzantine, they will be limited in resources and therefore limited in space and time. Therefore, one can assume a certain degree of locality in adversary activity and assume that the adversary may not be able to compromise a variety of information sources in a short amount of time over a large geographical distance.

Some of the techniques being considered for enabling secure information flows, include usage of cryptographic mechanisms, time-stamping and notarization services, and the usage of trust and reputation metrics to assess the veracity of information from different sources. Therefore, this application also requires careful analysis of threats against these cryptographic systems and implementations, including the timing based services and reputation and trust calculation techniques.

B. Threshold Cryptography

Threshold cryptography refers to a set of tools that are typically used to ensure confidentiality and availability in the presence of node compromise and unavailable nodes. Roughly, in a t out of n threshold scheme, secret information that is needed for some task is split among n nodes, in such a way that *any* t or more of them have enough information to perform this task, but any set *less than* t nodes does not have enough information. This is useful in ensuring confidentiality against compromise of *less than* t nodes, as well as availability as long as *at least* t co-operating nodes can be mustered.

In the context of sensor networks, there may also be an opportunity to use threshold techniques to improve the accuracy or truthfulness of data. This is because it may be more reasonable to rely on a measurement if we know that *at least* t nodes agree with it, than to base decisions on a measurement submitted by just a single node.

The challenge here is to adapt t out of n schemes to be

useful in a MANET environment. For example, many of these schemes rely on static membership and a reliable broadcast channel among the *t or more* co-operating nodes. While such network characteristics can be realized using a wired, static network, it is very easy to see that this model does not fit the wireless and dynamic nature of MANETs. For the most part, existing threshold cryptosystems assume a fixed set of authorized parties as well as a static set of parties running the protocol. In a MANET, parties may join and leave frequently (e.g. owing to mobility or emanation control requirements), and it may be desirable to be able to change the set of authorized parties or the threshold in response network events or mission requirements. Research efforts are underway to address some of these challenges. The threat model described in this paper will be expanded and used to assess the utility and security of threshold schemes under various adversarial capability assumptions.

C. Identity Based Cryptography

Identity-based cryptography can ensure confidentiality and authentication in environments with only limited synchronization and coordination between nodes. Whereas traditional public-key tools require that nodes know each other's public key, typically identity-based cryptography only requires that they know each other's "name" (or some other common information). For example, in some cases it may be possible to send an encrypted message to "the unit that occupies position X at time T" (using X and T as the unit name), even without exchanging any key material with that unit ahead of time. Thus identity based cryptography has the potential to facilitate coalitions that are formed on the fly. The challenges in identity based cryptography when applied to mobile ad hoc and sensor network include the development of mechanisms to distribute trust authority (since nodes may become disabled, or be compromised), enable inter-operability among multiple trust authorities (mobile networks may be formed by the nodes that belong to different administrative domains), and the design of identities and namespaces. Once again, our threat model will be further developed to determine benefits from and risks to identity based cryptography under various adversarial assumptions.

D. Risk and Trust Based Management

The notion of risk is inherent in traditional security mechanisms, e.g., an MLS policy can be viewed as specifying a fixed tradeoff between the risk of leaking sensitive information versus the operational need of providing such information. Most security policies encode static risk-benefit tradeoffs made during the time of policy authoring. These statically determined tradeoffs may be quite sub-optimal in highly dynamic, operational settings and some recent proposals for security management [33] tackle these challenges by proposing methods for explicit risk calculations, risk-benefit analysis and selection of appropriate risk mitigation measures during policy evaluation time based

on current conditions. Such mechanisms and models therefore appear quite suitable for highly dynamic missions and MANET and sensor networks environments. However, care is needed to incorporate dynamic risk management policy models in high threat MANET environments since such mechanisms themselves could be subject to attack.

The core threats to the risk management mechanisms are threats to integrity and to accountability. The information used for risk calculations could be subject to unauthorized modification resulting in false estimates. Such information may include provenance of data, the security labels or metadata associated with data, the impact of the action, the information about the state of the current infrastructure and current operating environment and state of the mission, the static rights of the actors as well their dynamically computed reputation or trust. The integrity of the risk calculation itself needs to be protected. In addition, accountability is extremely important when risk based decisions are permitted, and addressing threats to accountability will be very important for this approach.

Another direction in this space is to explicitly take into account *trust* in entities. Trust is a subjective matter, it is context- and agent-specific, and it involves expectations of future outcome. In other words, trust is the expectation or likelihood of an agent behaving in a specific manner in a given context. Clearly, trust and risk are inter-related concepts – more trust in an agent implies a reduced risk of security compromise. Furthermore, trust in an agent is typically based on multiple evidence or testimonials provided by other agents, based on their direct or indirect observation of the agent. In this sense, mechanisms based on trust provide similar protection as the mechanisms based on threshold cryptography, that is, the compromise or misbehaviour of a single (or a few) node or device is not sufficient to derail security mechanisms. However, it also suffers from similar drawbacks, e.g. agents may collude, to increase or decrease trust values. Research efforts are underway to detect such collusion among agents and to distinguish between cases when an agent is less trustworthy due to degraded capabilities versus when it has been compromised.

ACKNOWLEDGMENT

We would like to thank Dakshi Agrawal and Michael Steiner, IBM TJ Watson Research Center, for their helpful review comments.

REFERENCES

- [1] Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS and Other Systems. Paul Kocher. Proceedings of Eurocrypt 1996.
- [2] Differential Power Analysis. Paul Kocher, J. Jaffe and B. Jun. Proceedings of Eurocrypt 1999.
- [3] Analytical Assessment of Bluetooth Security Mechanisms. Technical report. FORWARD Deliverable D4, www.nextwave-interface.org.uk/centres/City_Buildings/deliverables/D11.pdf
- [4] Analysis of an Electronic Voting System. Response to Diebold's Technical Analysis. Kohno et al. <http://avirubin.com/vote/response.html>
- [5] Privacy Issues in an Electronic Voting Machine. Arthus M. Keller, David Mertz, Joseph Lorenzo Hall and Arnold Urken. WPES '04: Proceedings of the 2004 ACM workshop on Privacy in the electronic society.
- [6] Position Paper on Voting System Threat Modeling. Stanley A Klein. <http://vote.nist.gov/threats/papers/threat-modeling.pdf>
- [7] Threat Analysis of GNU Software Radio. Raquel Hill, Suvda Myagumar and Roy Campbell. http://srg.cs.uiuc.edu/swradio/threat_wwc05.pdf
- [8] Voltaire: Insider Threat Modeling. Stephen Laird and John Rickard. https://analysis.mitre.org/proceedings/Final_Papers_Files/99_Camera_Ready_Paper.pdf
- [9] Towards a Threat Model for Storage Systems. Hassan et al. www.suvda.com/files/toward_storages05.pdf
- [10] Defining a Comprehensive Threat Model for High Performance Computational Clusters. Mogilevsky et al. 2005. <http://arxiv.org/abs/cs.CR/0510046>
- [11] Securing Data in Storage: A Review of Current Research. Paul Stanton. Dept of Computer Science University of Illinois. <http://arxiv.org/abs/cs.OS/0409034/>
- [12] Protecting Multimedia in Storage: A Survey of Techniques Emphasising Encryption. Paul Stanton, William Yurkic and Larry Brumbaugh.
- [13] Remembrance of Data Past: A Study of Disk Sanitisation Practices. IEEE Security and Privacy Magazine Jan-Feb 2003.
- [14] Data Remanence in Semiconductor Devices. Peter Guttman.
- [15] Exploiting MMS Vulnerabilities to Stealthily Exhaust Mobile Phone's Battery. Radmilo Racic, Denys Ma and Hao Chen.
- [16] GSM-Security: a Survey and Evaluation of the Current Situation by Paul Yousef LiTH-ISY-EX-3559-2004
- [17] Attacks and Counter Measures in 2.5G and 3G Cellular IP Networks. Ollie Whitehouse and Graham Murphy. Research Report March 2004.
- [18] Anderson, R., 2001. Security Engineering: A Guide to Building Dependable Distributed Systems. John Wiley & Sons, Inc. ISBN 0-471-38922-6.
- [19] Analysis of an Electronic Voting System. Tadayoshi Kohno, Adam Stubblefield, Aviel D Rubin, and Dan S Wallach.
- [20] Sensor Network Security: More Interesting Than You Think. Madhukar Anand, Eric Cronin, Micah Sherr, Matt Blaze, Zachary Ives and Insup Lee. www.cis.upenn.edu/~zives/research/sensors-hotsec.pdf
- [21] Secure routing in wireless sensor networks: attacks and countermeasures. Chris Karlof and David Wagner. Ad Hoc Networks 1(2003) pp 293-315.
- [22] Tampering with Motes: Real-World Physical Attacks on Wireless Sensor Networks. Becher et al. In proceedings Security of Pervasive Computing 2006..
- [23] OCTAVE Threat Profiles. Christopher Alberts and Audrey Dorofee. Software Engineering Institute. Carnegie Mellon. <http://www.cert.org/archive/pdf/OCTAVETHREATProfiles.pdf>
- [24] Why Phishing Works. Rachna Dhamija, J. D. Tygar, Marti Hearst. 2006. http://people.deas.harvard.edu/~rachna/papers/why_phishing_works.pdf
- [25] Unmasking Threats in Mobile Ad-Hoc Network Settings. Dagmara Spiewak, Thomas Engel and Volker Fusenig. WSEAS Transactions on Communications, Issue 1, Volume 6 (pp 104–110). Jan 2007.
- [26] Threat Modelling. Swiderski and Snyder. Microsoft Press 2004.
- [27] Basic concepts and taxonomy of dependable and secure computing. Avizienis et al., IEEE Trans. Dependable and Secure Computing, 2004. 1(1): p. 11-33.
- [28] The right type of trust for distributed systems. A Jøsang. In New Security Paradigms Workshop. 1996, ACM.
- [29] *End-user functionality of MANETs*, Cirincione, G. ARL, 12th October 2006.
- [30] On trust establishment in mobile ad-hoc networks. Eschenauer, L., V.D. Gligor, and J. Baras. In *Security Protocols 2002*, B. Christianson, Editor. 2004, Springer-Verlag,
- [31] Dynamic decentralized trust computation. D Agrawal in *ITA TA2 Project Workshop*. 2006: New York.
- [32] A logic for uncertain probabilities. A. Jøsang, Int Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 2001. 9(3): p. 279-311.
- [33] MITRE, *Horizontal integration: broader access models for realizing information dominance*, JSR-04-132, 2004, JASON Program Office
- [34] Breaking Up Is Hard to Do: Modeling Security Threats for Smart Cards. Bruce Scheier and Adam Shostak. *USENIX Workshop on Smartcard Technology* Chicago, Illinois, USA, May 10–11, 1999.