RC24588 (W0806-080) June 18, 2008
Computer Science

IBM Research Report

Bootstrapping Coalition MANETs

Mudhakar Srivatsa, Dakshi Agrawal
IBM Research Division
Thomas J. Watson Research Center
P.O. Box 704
Yorktown Heights, NY 10598
USA

Shane Balfe
Information Security Group
Royal Holloway
University of London
UK

Research Division
Almaden - Austin - Beijing - Cambridge - Haifa - India - T. J. Watson - Tokyo - Zurich

Bootstrapping Coalition MANETs*

Mudhakar Srivatsa† Dakshi Agrawal† Shane Balfe‡

† IBM T. J. Watson Research Center, P. O. Box 218, Yorktown Heights, NY 10598

‡ Information Security Group, Royal Holloway, University of London

Abstract

Designing a coalition network in chaotic environments (e.g. responding to a large catastrophe) is challenging because such systems cannot rely on availability of a fixed communication or security infrastructure. In such situations, a coalition may use Mobile Adhoc NETworks (MANETs) to communicate and to extend its operational reach and tempo. In this scenario, bootstrapping security and networking protocols requires that networking protocols cannot assume full existence of operational security protocols and vice-versa. In this report, we outline a realistic bounded resource adversary model and examine bootstrapping problems in the physical & link layer, the routing layer, and identity management with the goal of identifying new research challenges and novel solution methodologies.

In particular, (i) we examine secure link key set up protocols at the physical & link layer that neither use computation intensive PKI mechanisms nor assume pre-configured shared keys between nodes that belong to different coalition partners, (ii) identify new security issues owing to power saving intra-domain routing protocols that use sophisticated packet matching and forwarding; in a coalition setting we also examine inter-domain routing protocols that preserve autonomy and yet permits scalable network monitoring and misbehavior detection, (iii) examine identity management issues in MANETs and propose a novel wireless fingerprinting approach to condone a malicious node from spoofing and forging one or more identities on the network.

1 Introduction

This report explores issues in bootstrapping a coalition mobile ad hoc network (MANET). A coalition MANET comprises of a set of mobile nodes that belong to multiple organizations of a coalition. These nodes, equipped for wireless inter-node communication, work together to establish a communication network capable of providing end-to-end packet delivery service between any two or more participating nodes. The key challenge in bootstrapping a coalition MANET is the establishment a secure and reliable end-to-end packet delivery service starting from a point where nodes belonging to different organizations are put in a field without any pre-configured coordination of either the networking or the security protocols among members of a coalition. In this scenario, bootstrapping security and networking protocols requires that networking protocols cannot assume full existence of operational security protocols and vice-versa.

In this report, we examine how to enable secure communication at the lower layers (physical and data link layer) as well as at the network layer leading to secure end-to-end packet delivery service in a coalition MANET. We start with the challenges in establishing physical layer communication including discovery of other nodes and secure configuration of physical & link layer parameters. We illustrate bootstrapping issues by considering two cases: in the first case, nodes use a wireless communication protocol similar to the family of IEEE 802.11 standards, and in the second case, nodes use a low probability of interception and detection (LPI/LPD) wireless communication protocol from the military grade wideband waveform. Using these considerations, we abstract out security implications for the networking layer.

We then look at the networking (IP) layer, specifically on the routing protocols used to set up end-to-end paths for packet delivery. Unlike fixed networks which use simple IP-address prefix based matching and routing, MANETs use more sophisticated routing protocols such as flexible end point based routing, network coding based cooperative routing, in network semantic aggregation, etc with the goal of minimizing the over all power consumption (and thus, the longevity of the nodes and the network itself). We argue while such novel protocols offer performance benefits, they bring forward new security challenges in key management algorithms, data confidentiality & integrity and denial of service (DoS) mitigation. Further, in a coalition MANET setting, we argue that in most circumstances, the nodes belonging to each organization will organize themselves in one or more routing domains in a coalition MANET. Any communication between two nodes belonging to different organizations will be done through inter-domain routing gateways using BGP like protocol to discover end-to-end path through routing domains. We then focus on some of the security issues such as route authentication, cooperative fraud

*Research was sponsored by the U.S. Army Research Laboratory and the U.K. Ministry of Defense and was accomplished under Agreement Number W911NF-06-3-0001. The views and conclusions contained in this document are those of the author(s) and should not be interpreted as representing the official policies, either expressed or implied, of the U.S. Army Research Laboratory, the U.S. Government, the U.K. Ministry of Defense or the U.K. Government. The U.S. and U.K. Governments are authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation hereon.

detection, etc in inter-domain routing algorithms.

As a result of our analysis, we present a catalogue of different security functions that need to be implemented and enabled for securely bootstrapping coalition MANETs. In future, we plan to consider how these security functions can be enabled simultaneously with networking protocols being researched in TA1.

2 Adversarial Models and Security Metric

2.1 Space-Time Delimited Adversary

In a MANET environment, nodes are susceptible to physical attacks and capture. Furthermore, nodes and links have limited resources which can be exhausted easily. In the prior work on security mechanisms for MANETs, adversarial model have taken traditional adversarial models and enhanced the adversary's abilities by taking several aspects of the MANET environment into account. For example, some of these models assume that a certain fraction of nodes can be physically captured and compromised anywhere in the network; others assume that corrupted nodes may be Byzantine, and yet others assume that the "man-in-the-middle" (MITM) attacks are possible everywhere. These models assume that arbitrary nodes can get corrupted, corrupted nodes are capable of injecting false and misleading information anywhere into the network, and that the corrupted nodes are able to clone other nodes, and collude with one other.

While each of these adversarial models is applicable in some scenarios, it is unlikely that all modes of adversarial operation would be active at once in a network. Without systematically limiting adversarial aspects, it will be hard to derive meaningful conclusions about the design of a trust management system. To that end, we propose to examine *space and time delimited* adversarial models which have not been considered thus far explicitly by the prior work. An adversary which is space delimited can only cause "local" damage, e.g., a corrupted node can only corrupt nodes or information in its immediate vicinity. An adversary which is time delimited can only cause damage "slowly". It is our thesis that such models are more realistic in a MANET environment within a theater of operations, where an adversary has to incur costs and risks for performing each node capture, substitution, etc; and the costs and risks are unlikely to be uniform within a theater of operations. For example, certain portion of the MANET may exist in difficult terrain or a well guarded terrain. Attacks that involve physically capturing a node may be difficult to mount in heavily protected areas whereas these may be easier in areas with less protection.

Even a compromised node has to work in a resource limited environment with limited range wireless links to communicate with other nodes. This put a limit on the "reach in space" of an adversary. Similarly, we assume that an adversary may be able to break into logically or physically weak cryptographic implementations, but it still has to expend resources (energy and time) to do so. A restriction in resource consumption will limit how fast an adversary can compromise more nodes in different parts of the network.

We note that space and time delimited adversarial model does permit multiple points of attack on the network. It is only that even if multiple points of attack are successful, further damage to the security mechanisms will have limits on its propagation both in space and time. A focus on space and time delimited adversary will allow us to examine resiliency and performance of a trust management system for a MANET against a realistic adversary.

2.2 Physical Layer Metrics

In the light of above model, we will now define some new security metrics for MANETs. At the physical layer, the fundamental resource can be considered to have four independent dimensions: space, time, energy, and radio spectrum. The goal of an adversary is to deny the usage of this resource along any of these four dimensions or a combination thereof to a MANET. The efficiency of the attack is measured by the ratio of resources the adversary has to spend to deny a certain amount of resources to the MANET. For example, using a 802.11x protocol, an adversary can send a `deauth` frame causing the handset to disconnect from an access point (AP), wait for a time-out period of about one minute and seek a new channel to reconnect to the AP. Sending a `deauth` frame (by forging the AP's MAC address) takes one unit of time, one unit of energy, and one unit of radio spectrum, and one unit of space. The result is wastage of 16 units of time, 16 units of energy, 16 units of radio spectrum, and one unit of space.

Towards this goal, Xu *et al.* [28] define two metrics to measure the effectiveness of a jammer at the data link layer: (a) Packet Send Ratio (PSR) which is the ratio of packets that are successfully sent out by a legitimate traffic source compare to the number of packets it intends to send out at the data link layer. This metric is geared towards MAC layers that employ some form of carrier-sensing multiple access control before transmission may be performed. Such protocols require that the channel be sensed idle before a node can transmit a packet. A radio interference attack in this case may cause the channel to be sensed as busy causing the legitimate node to wait before it can transmit packets. (b) Packet Delivery Ratio (PDR) which is the ratio of the packets that are successfully delivered to a destination compared to then number of packets that have been sent out by the sender. This captures the scenario when attacks target corruption of packets.

Another interesting set of metrics has been proposed by Law *et al.* where they measure effectiveness of an attack by consider *attrition rate* R_a, the fraction of additional energy a node has to spend in presence of a jamming attack. In addition, they consider the *effort ratio* R_e, defined as the ratio of the attacker's per node energy expenditure to mount an attack to the network node's energy consumption when not under attack. These two numbers are then used to calculate the *lifetime advantage* R_l of a jammer node over a sensor node, that is how long a jammer node can live compared to a sensor node. They then compute lifetime advantage for

various MAC layer protocols.

2.3 Routing Layer Metrics

The effectiveness of routing layer attacks on MANET routing protocols depends on the number of malicious nodes in the network and the rate of benign failures in the network (e.g.: node crash failure, link failure due to interference, mobility, etc). Consequently, routing layer metrics are defined as a function of the fraction of malicious nodes and the rate of benign failures in the network. Routing layer metrics are defined as *multipliers* on performance metrics. For instance, *bit multiplier* denotes the ratio of the number of bits required to send (reliably) a unit size message in the presence of an adversary to that in the absence of the adversary. Similar metrics include *latency multiplier*, *jitter multiplier*, *control data multiplier*, *storage cost multiplier*, *computation cost multiplier*. An adversary may introduce routing black holes, loops, grey holes, sub-optimal routes, etc and adversely affect the latency and jitter of a route. Control data refers to the average amount of computation and communication cost expended by a node on handling control traffic; an adversary may trigger heavy control traffic by inducing heavy network flux, exploiting multicast tree construction and maintenance protocols, etc. Storage cost is measured by the average case size (and the worst case size) of the routing state maintained by each node in the network; the storage cost can be significantly affected by poisoning routing caches in source-based routing protocols. Computation cost is measured by the number of CPU cycles expended by a node on forwarding a packet in the network; MANETs use more complex packet matching and routing protocols (discussed later) and thus incur higher computation costs.

While some of the above metrics equally apply to fixed networks, there are additional security considerations for MANETs. Routing layer in fixed (wired) networks typically rely on simple address prefix based packet header matching and forwarding. This allows efficient hardware based implementation of routers and facilitates the network to reliably sustain large data transfer rates. However, in MANETs, energy and battery life considerations drive routing protocols to implement more sophisticated matching and forwarding algorithms such as flexible end point based routing protocols, network coding based routing protocols, semantic aggregation based routing protocols (discussed in later sections). Essentially all these protocols require additional functionality from the routing nodes (as against simple address based prefix matching and forwarding in IP networks). While this represents an opportunity to improve the performance of the network, these new protocols also carry additional security risk and new challenges.

3 Securing Communication at the Physical and Data Link Layer

The primary challenges in establishing physical layer communication includes discovery of other nodes and secure configuration of physical layer parameters. Before we go into the details, consider the case of a covert communication network where one of the main goals of the network is to hide its very presence from an adversary. The candidate physical layer protocols in such networks will employ a radio modulation scheme that has low probability of interception and detection (LPI/LPD). Such modulation schemes will typically employ frequency hopping and spread spectrum codes to configure their radio links. By definition, nodes that wish to communicate with each other will have to have shared preconfiguration before deployment to the field since the goal after deployment is to exclude discovery by external means.

In contrast consider the case of a detectable network whose presence can be relatively easily deduced (e.g.: 802.11x networks). In this case, the main goal of the network is to ensure performance and availability of the network to provide an end-to-end packet delivery network that may be insecure against eavesdroppers. In this report, we focus on the security issues in the second case since they are more challenging to secure than covert networks.

3.1 Jamming Attacks

There are several key issues involved in establishing secure MANET communication at physical and data link layer of a detectable network. The first issue is that of securing the radio spectrum (wireless medium) against an adversary who may employ jamming techniques. Fortunately, jamming at the physical layer is a highly resource intensive operation for an adversary even when the adversary knows physical layer configuration parameters such as spread spectrum code or frequency hopping patterns. Essentially, jamming at the physical layer is a brute force attack wherein an adversary transmit a large amount of energy in form of "white noise" in a frequency band. Furthermore, such adversaries are often easily detected in practice (e.g. using wideband or channelized radiometers); it may even possible to deduce the physical coordinates of a jamming adversary. For this reason, more realistic adversaries will exploit other vulnerabilities in higher layers of the networking stack to launch attacks. Good thing about brute force jamming is that it can guarantee throughput to zero for a given class of devices. Such a guarantee may be very attractive for certain missions.

A resource constrained adversary may choose strategic locations in a MANET to inject physical layer jamming attacks. Additionally, an adversary may partition the network by jamming the links along a minimal cut in the network. In particular, for a random power-law topology, the size of a min-cut (number of links in the min-cut) is a constant that is independent of the network size. Hence, an adversary would require only constant amount of resources to partition an arbitrary network.

Further, an energy constrained adversary can launch smart jamming attacks by targeting data link layer protocols with the goal of degrading a link's availability and reliability [17, 24, 5]. Here the adversary exploits two facts: first, wireless medium is a shared medium and therefore data link layer will have a medium access control (MAC) protocol that detects when a node can use the wireless medium. Attacks on the MAC protocols can make the channel seem busy for

a long duration, thus preventing the packets from getting transmitted. Other attack involves corrupting the transmission of a packet by creating short bursts of noise that are sufficient to overcome forward error correction codes. Jamming attacks are attractive at the data link layer since they require only protocol specific information, they do not presume the knowledge of any instance specific parameters. Along these lines, Hoesel et. al. [18], categorize MAC layer protocols into three types (S-MAC, A-MAC and L-MAC) and present low power jamming attacks on each of these classes of link layer protocols.

3.2 MAC-Layer Protocol Vulnerabilities

In terms of sophistication, the next category of attacks uses well crafted packets to disrupt efficient operation of a link. This category of attacks can be largely thwarted if a mutual authentication is used between the two end points of the network. *The key ingredient to support a stable link is mutual authentication between the two end points.* The absence of mutual authentication is responsible for several link hijack attacks on 802.11 protocols including: DoS attacks, and MITM attacks (Man in the Middle). 802.11 protocols have no layer-1 (frame level) authentication, thereby allowing an attacker to pretend to be an access point (AP). Hence, an attacker can send management frames (used for connection establishment) such as associate/disassociate frames (to handle client connect, disconnect and roaming), auth/deauth frames (to handle access control on the network), etc.

DoS attacks are typically triggered using disassociation and deauth attacks, wherein an attacker sends a forged disassociate (or a forged deauth) frame to the target with the access point's MAC address. Consequently a well behaved client disconnects itself from the AP. Now, the client attempts to discover a new and stable channel to connect to (this can be exploited in MITM attacks described later). Additionally, DoS attacks may attempt to trip the MIC (message integrity check) as follows: When an access point receives two packets whose MIC check fails in one second, it assumes an active attack and disassociates with the client for one minute before re-associating. Hence, an attacker can spoof a client's MAC address and send packets such that MIC fails. MITM attacks are triggered by forcing a client to switch to a different channel (say, using a deauth attack). Now, the attacker sets up a forged AP on another channel; a disconnected client searching for a new and stable channel may connect to the forged AP. The forged AP reestablishes new channel keys with the client and the actual AP. Now, the forged AP can continue talking to the actual AP on behalf of the client, while being able to listen to all the packets (in plain-text) sent from/to the client.

Supporting mutual authentication in link layer protocols can protect a link from an adversary. *There are two well known approaches to support mutual authentication: PKI based mechanism and pre-configured shared symmetric keys.* Both these approaches are faced with the challenge of having to trade off between the effects of an insider attack (say, a malicious insider or a compromised node) with the overhead of key management. Reusing a link key reduces compromise containment, that is, the compromise of one link key may affect several links in the network. In the worst case, when all nodes in an organization use the same key, an attacker can attack all the links in the network after compromising just one node. Using a PKI based approach requires only one key per node. However, they are computationally very intensive; an attacker can exploit this expensive link key set up protocol to launch DoS attacks (similar to DoS attacks on SSL handshake). The preconfigured shared keys based approach may in the worst case require a node to maintain n keys (a total of n^2 pair-wise keys). Several papers in literature have studied various approaches to improve the efficacy of pair-wise key distribution and management [4]. Further, the assumption that two nodes from different coalition partners share a pre-configured key is questionable.

Yet another alternative is an out-of-band key exchange mechanism, wherein both the nodes send a request to establish a link between themselves to their respective command centers; the command centers securely establish the link key and communicate it both the nodes. In the following sections we will explore in-network key exchange protocols.

3.3 Information Theoretic Secure Key Exchange

In coalition scenarios, neither PKI based mechanisms nor pre-configured shared symmetric keys may work. Here a third approach has promise. This approach essentially exploits the fact that if an intended recipient R and an eavesdropper E are a few wavelength apart, then the fading experienced by R and E from a given transmitter T will be independent. This difference in physical channels can be exploited to achieve perfect information-theoretic secrecy [10, 14, 15, 1, 21]. Along these lines, Koorpaty, Hassan and Chennakeshu [16] have proposed a technique that uses the short-term reciprocity of the radio channels and rapid decorrelation of radio channels in time, space, and frequency domains to provide a means for secret cryptographic key agreement between two users. Their fundamental idea can be further extended to design space-time transmission schemes that exploit MIMO antenna configurations for a secret key agreement [19, 27]. Li, Trappe, and Yates have done further experimental verification of similar techniques [20]. We note that a price paid for secrecy using physical layer approaches is the reduced rate of information transfer between transmitter and legitimate receiver. However, the reduced information rate is not a concern for the initial handshake used to exchange secret keys for subsequent communication as the number of bits transferred during this initial handshake is very small (less than 100 bytes). However, as opposed to PKI based mechanisms or pre-configured shared symmetric key techniques this approach remains relatively unexploited and represents untapped potential.

3.4 Risk Based Key Exchange

In an intra-domain setting, we might have preconfigured link keys between a subset of nodes in one organization. Two nodes that do not have a preconfigured link key may establish

a channel between them as follows: the nodes may estimate the current risk and threat level and decide to exchange the secret in plain-text, or the nodes may establish a link key by communicating over a secure multi-hop network (say (a, b) have no preconfigured keys but (a, c) and (b, c) have preconfigured keys. Then a and b can establish a shared key by communicating via c. In an inter-domain setting we argue in the following section, it is best to route all traffic across organizations through a small set of inter-domain gateways in order to achieve better security, accountability and preserve autonomy. Hence, link keys need to be configured only between the gateway nodes of two organizations.

Instead of securing all the links in the network, an alternate approach that exposes the security characteristics of a link to higher layer networking protocols may offer promise. For instance, a link set up using pre-configured key may be highly trusted. A link (a, b) established using a chain of secure links (say, a, c_1, $\cdots$, c_k, b) may have a trust value that is inversely proportional to k. We note that if any node c_i is compromised then c_i can use MITM attacks (similar to those on 802.11) to hijack the link (a, b). In this case, the trust value of the link (a, b) could be $\prod_{i=1}^{k}(1 - comp(c_i))$, where $comp(c_i)$ denotes the probability that a node c_i is compromised. A link (a, b) established over the open air may have some low but non zero trust value (assuming a space-time delimited adversary model). However, this approach requires novel routing protocols that use link security metrics in addition to link performance metrics (bit rate, latency, etc) to route packets on the MANET.

4 Securing Communication at the Routing Layer

In this section, we describe security issues at the routing layer in MANETs. First, we explore intra-domain routing protocols in MANETs and identify new security challenges in view of sophisticated packet routing and forwarding protocols used in MANETs. Given that the link layer protocols support mutual authentication and facilitate secure exchange of link keys, an adversary can launch routing layer attacks only by compromising one or more nodes in the network. Hence, the routing layer protocols must be designed such that they can tolerate a small fraction of malicious nodes in the network; also network management infrastructure must be capable of detecting compromised nodes and either repair them or expel them from the routing network. As we point out in the next section, expelling a compromised node is a challenging problem in itself. For instance, a malicious node may reappear elsewhere in the network and forge one or more new identities. Hence, security at the routing layer should be implemented as a combination of robust routing protocols and a network management system (NMS) that quickly detects malicious or compromised nodes. For a system to be stable the rate at which NMS detects compromised nodes must be faster than the rate at which an adversary may compromise nodes; this ensures that in steady state, only a small fraction of network nodes are in a compromised state, thereby allowing the routing protocols to operate efficiently.

Second, we argue that routing protocols in a coalition MANET must use inter-domain routing protocols (IDRP). We argue that IDRP offers autonomy for each coalition partner while providing certain routing guarantees (e.g.: throughput, latency, reliability, etc) to the end points. It also allows one to device novel root cause analysis and fraud detection techniques that can detect misbehaving routing domains (and gateways) assuming a threshold number of coalition partners are honest. In the rest of this section, we first examine intra-domain routing issues followed by inter-domain routing issues with the goal of identifying new challenges and unsolved research problems.

4.1 Naive Packet Forwarding Network

In a traditional packet forwarding network, a node S may send packets to a destination D through a path $\langle S, A, B, D\rangle$; here, nodes A and B perform packet forwarding function to deliver packets. Node S requires cooperation from the routing nodes to discover a route to node D (route set up and discovery). A malicious node can create a *black hole* by advertising low cost routes and drop all packets routed to it, destabilize routes, and create routing loops. A detailed survey of routing layer attacks on ad hoc networks is presented in [9, 12].

There is an inherent trade off between the robustness and the communicating cost of packet routing and forwarding protocol. For instance, if each node uses a broadcast (flooding) protocol, it may maximize the probability that a packet from S reaches D; however, its packet forwarding cost is linear in the size of the network. In any event, if an adversary can partition the network (by compromising a *vertex cut*) then it can completely control all communications between the partitions.

Fortunately, in a mobile network the topology changes dynamically and arbitrarily; and thus the vertex cut is not static. Hence, an adversary is forced to invest more resources in attempting to compromise new nodes as the topology changes. On the other hand, the network may invest more resources into increasing the mobility of nodes to defend against network partitioning attack. In the limiting case, if the network had infinite resources for mobility, then it does not have to use multi-hop routing protocols; the communicating parties can move closer to one another and correspond over a direct link. Most papers in literature have failed to explicitly include mobility as a resource (available to both the network and the adversary) while analyzing the security properties of routing protocols.

In addition to naive packet forwarding, MANETs use more sophisticated routing protocols that rely on the routing nodes to perform complex operations. Such routing protocols are designed with the goal of reducing wireless transmission costs. In a typically sensor mote, transmitting one bit expends as much energy as executing 800 instructions [13]. Hence, wireless networks use flexible end point based routing, network coding based cooperative routing, in-network data aggregation to reduce transmission costs. We argue below that these routing protocols pose new challenges in pre-

serving packet data confidentiality and integrity, mitigating resource exhaustion DoS attacks, and require novel key distribution and key management algorithms for scalable access control.

4.2 Flexible End Point Based Routing

First, several routing protocols in MANETs use flexible end point based routing, wherein, the end point is not defined by an identity (such as an IP-address); instead the end point could be based on: (i) fixed attributes of an entity (e.g.: role): deliver this packet to any entity who is authorized to play a role R, (ii) dynamic attributes of an entity (e.g.: geographical routing): deliver this packet to any entity within a geographical bounding box, or to the entity closest to geographical coordinates (lat, lng), (iii) content-based routing (e.g.: publish/subscribe networks): deliver this packet with attributes e (e.g.: $e_1 = \langle mission,\ A\rangle$, $\langle secrecyLevel,\ Secret\rangle$) to all entities who are authorized to listen to a filer f (e.g.: $f_1 = \langle mission,\ =,\ A\rangle$, $\langle secrecyLevel,\ \preceq,\ topSecret\rangle$, $f_2 = \langle mission,\ =,\ A\rangle$, $\langle secrecyLevel,\ \preceq,\ classified\rangle$) such that $match(e, f) =$ `true` (e.g.: $match(e_1,\ f_1) =$ `true`, $match(e_1,\ f_2) =$ `false`). Unlike (i) and (ii) wherein an end point is defined by a predicate over the entity's fixed or dynamic attributes, (iii) defines an end point using a predicate over the packet payload's attributes.

While research in the network security community has explored identity based end point routing, flexible end point routing appears to be largely untapped. First, flexible end point based routing protocols rely on efficient *multicast overlay trees to match and forward packets on the network*. Such routing protocols have not been properly inspected in the presence of compromised routing nodes that attempt to actively subvert the protocol. Improperly constructed routing trees may significantly increase the transmission cost. Further, with flexible end points, the leaves in the routing tree may change dynamically over time. Malicious nodes may artificially increase the churn rate for a routing tree, thereby, significantly increasing the cost of constructing and maintaining routing trees.

Second, flexible end point based routing *requires novel key management algorithms to ensure that the packet payload are intelligible only to authorized recipients*. For example, in geographical routing, a packet intended for a node in a geographical bounding box B must be intelligible to only some node within the box B. However, the key challenge here is that the sender may not a priori know the identity of the recipient. *This precludes the possibility of encrypting the packet either using a symmetric key or using a public key that is bound to the identity of the recipient.* A naive approach is to first identify a node in the box B and use the identity of the node to appropriate encrypt the packet (with a shared symmetric key or a public key). However, this defeats the performance and scalability benefits of geographical routing; also, when the node moves out of the box B, the sender has to redo the task of identifying a new node in box B. One alternative approach is to leverage identity based (attribute based) public key management protocols (ID-PKC), wherein, the sender encrypts the packet using the attributes associated with the bounding box B. In this case, the problem reduces that of key distribution: when a node is in box B, the network must distribute keying material to the node that allows it to generate an appropriate private key; also, the key must be revoked when the node leaves the box B.

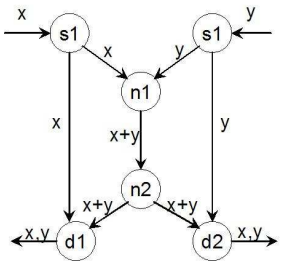

Figure 1: Network Coding based Cooperative Routing Example

4.3 Network Coding based Cooperative Routing

Recent research on reducing transmission power in MANETs has proposed network coding based cooperating routing approach. Figure 1 shows a simple example of network coding. Let us suppose there are two sources s_1 and s_2 each of which generate data streams x_i and y_i at the rate of one bit per second. All wireless channels can carry at most one bit per second. There are two destination nodes d_1 and d_2 both of which need the bit streams x_i and y_i. One can show that no packet routing and forwarding scheme can achieve the goal of delivering both x_i and y_i to both d_1 and d_2. On the other hand, this goal can be met if n_1 uses packet coding and transmits $x_i \oplus y_i$ (see Figure 1).

In addition to packet forwarding and routing attacks, the routing nodes may improperly execute packet coding, thereby, compromising the integrity of a packet. While it may be possible for the receiver to ultimately detect a corrupted packet (and subsequently drop it), the malicious node has succeeded in wasting the transmission power at every node on the route from the sender to the receiver (this problem becomes worse when we use multicast routing trees). In a simple packet forwarding scenario a source S and destination D can protect packet data confidentiality using payload encryption; every intermediary node (including the receiver D) on the routing path can verify the integrity of the packet by checking the sender's signature. In network coding schemes, confidentiality from packet coding and forwarding nodes can be achieved using payload encryption (most network coding schemes operate on the entire payload as if they were bit strings); however, it may not be possible to generate $sig(x_i \oplus y_i)$ from $sig(x_i)$ and $sig(y_i)$[1]. One possible approach is to use a computation intensive Goldwasser-Micali [8] digital signature that is homomorphic on the $\oplus$ operator. However, using expensive computational operations exposes a node to DoS attacks (similar to SSL handshake based DoS attacks that exploit the cost of public key signature gener-

[1]One solution is to attach both $sig(x_i)$ and $sig(y_i)$; however, this increases packet size and consequently the transmission cost

ation and verification). Hence, it is very crucial to couple network coding schemes with cryptographic schemes that allow all intermediary nodes to efficiently verify the integrity of a packet before expending its energy to forward the packet.

4.4 In-Network Aggregation

In a sensor network, the base station may not be interested in collecting all the raw data; but may require only some aggregates on the raw data such as `sum, average, count, variance, min, max, etc`. Hence, sensor nodes may perform in-network packet data aggregation to reduce transmission costs. In addition to packet forwarding and routing attacks, a malicious node may improperly execute the aggregation operator. However, one may exploit the statistical properties of aggregation operators and a data model (for raw data) to limit the extent of damage caused by malicious nodes [6].

In the aggregation schemes, it is hard to maintain both confidentiality and integrity data from forwarding and aggregating nodes. One possible approach is to use homomorphic encryption schemes (Benolah [2] and Paillier [23]); however, there is no known cryptosystem which preserves the ring structure of the plaintexts, i.e. allows both addition and multiplication on a group. In the absence of efficient cryptographic primitives, the network is faced with the challenge of effectively trading off efficiency (in the worst case by turning off in-network aggregation) with the goal of improving its resilience to routing layer attacks.

4.5 Need for IDRP for Coalition MANETs

We have so far described routing layer security issues in intra-domain routing protocols. In this section, we argue that inter-domain routing protocols are more suitable for coalition MANETs wherein each coalition partner forms a small routing domain in the network. We describe security challenges in inter-domain routing protocols in the next section.

Easy Physical/Link Layer Configuration: As indicated in earlier section, to establish physical link, we need to share configuration parameters and if an adversary gets hold of these parameters, they can mount various attacks that affect the availability of the link. So the idea here is to share physical configuration parameters among a set of trusted nodes only, implying that only these nodes can communicate directly with each other. One natural partition would be nodes that belong to the same organization which can have physically preconfigured trust in devices.

Exploit Node Heterogeneity: Inter-domain routing protocols route all communications between two autonomous domains via gateways. During bootstrap, these gateways would need to talk to each other and therefore exchange physical configuration parameters. We observe that older radios (which are nowhere close to their retirement age due to the cost of replacement) are incompatible with each other. On the other hand, the newer JTRS radios are equipped with multiple signaling waveforms. That makes JTRS devices ideal to act as hubs and routers, gateways. As indicated in the previous, this entails some risk that an adversary located in the close proximity can hijack the gateway-to-gateway link. However, we can choose gateways that are in better protected territory, better equipped to exchange physical configuration parameters without compromise (e.g. by exchanging key material through physical contact).

Perimeter Defense: Actually, security may be the most important and the only good reason. Through gateway model, we can implement perimeter defense, where stuff like flooding etc. can be suppressed, firewalls implemented, which may be difficult to implement in each node.

Control Information Flow: Again, however, doctrinal and other issues nix technical possibilities. The UK's FIST studies concluded that interoperability is best achieved at the company level. According to Steve Turner, "There are doctrinal issues to making interoperability possible at lower levels. From a command structure perspective you do not want a section leader doing something with another section leader without going through the chain of command. The company level is where the exchange of information between nations or different companies should take place."

Establish a Trusted Routing Infrastructure: Trust in any system has to be complemented by accountability. In fact, these two form a feedback loop, wherein the results of accounting (say, via audit) are used to update the trust metric; and the accounting metrics and mechanisms are based on the trust metric (say, carefully monitor a poorly trusted system). Physical and link layer protocols operate between two connection peers, making it easy for either peer to monitor the link (say, using channel busy periods, MAC layer collisions, etc) and detect possible misbehavior. In contrast, routing protocols are distributed over all the nodes in the network making it hard to implement accountability. We argue that autonomous routing domains making accounting feasible and provide a good level of accounting granularity by exploring route authentication and route authentication & audit.

Route Authentication: In an inter-domain routing protocol, a gateway B advertises BGP-like path vectors, which suggest best routes from B to a given destination. Let us suppose that B advertises a route ($B \rightarrow C \rightarrow E$ to A. Route authentication refers to binding a destination node e in E to a path vector (say, $B \rightarrow C \rightarrow E$). Using an inter-domain routing protocol allows us to authenticate a route using S-BGP like mechanisms or using more recent work based on OMS (ordered multi-signatures [3]) that produces a compact signature (with respect to a given path length).

Route Accounting and Audit: Let us suppose for a given path vector $A \rightarrow B \rightarrow C \rightarrow E$ each intermediate gateway maintains a simple counter of the number of packets that it believes has been successfully forwarded to its next hop gateway. Let us suppose that C is a misbehaving gateway that drops all packets. When A audits these counters, it realizes that the counters at B and C do not agree with one another. In the absence of a priori beliefs that A has in B and C, A regards both B and C as suspicious; note that B could very well be misbehaving by not forwarding packets to C; and these two cases will be indistinguishable to A. In the absence of a priori beliefs one can use multi-path correlation to

enhance accounting and audit. For instance, using another path $A \rightarrow D \rightarrow C \rightarrow E$, A decides that D or C is suspicious; A can correlate this information with its audit results from path $A \rightarrow B \rightarrow C \rightarrow E$ and deduce that C is more likely to be the misbehaving node. Another approach is for B to collect proofs from C for successful transmissions. One can leverage light weight optimistic fair exchange protocols wherein node B sends a packet to node C in exchange for an irrefutable receipt from node C.

Route Optimization: Intuitively it might appear that having a single routing domain maximizes routing performance. However, this may not be the case. The nodes in different organizations are working towards aligned but not identical goals. Hence, the nodes from different organization may vary significantly along several dimensions: resources (computing, memory, bandwidth, battery life, etc), mobility patterns (fast moving, slow moving, static, etc), etc. As observed in MANET routing literature, resource considerations and mobility patterns significantly affect the efficacy of routing protocols. In a multi-domain setting, we need to cleanly separate these concerns and let a domain B deal with the best routing protocol that fits its profile. Hence, a path vector $B \rightarrow C \rightarrow E$ is an abstract path; the actual path from $B \rightarrow C$ is completely determined by B. For example, B could communicate to C via a satellite link, a one hop link using a powerful antenna, a multi-hop network using several nodes in B, etc. These details may not relevant to A and it may be better to hide these details from A based on the famous "need-to-basis" doctrine for information sharing.

However, B might export a clean interface to A that describes its route properties to C using metrics such as delay, jitter, reliability (packet loss rate, connection drop rate, link/route trust), etc. A can use a simple calculus to aggregate these metrics over a path $B \rightarrow C \rightarrow E$; delay and jitter is additive, reliability is multiplicative, etc. Now A can expand its accounting and audit mechanisms to not just maintain a simple packet counter, but also monitor these complex route metrics. However, unlike a simple packet counter based monitor, it is harder to generate proofs (and receipts) for complex route metrics (such as delay, jitter, reliability, etc). This approach requires research on novel diagnostics techniques to deduce misbehaving nodes discussed in the next section.

Exploit Geographical Clusters: It is reasonable to assume that nodes in the same domain form geographical clusters. Inter-domain routing provides a natural way to exploit these geographical clusters to: (i) minimize the number of inter-domain crossings, and (ii) provide better routes.

4.6 Security Issues with IDRP

This section expands on two important security issues in IDRP: (i) establishing trust in a path vector, and (ii) cooperative monitoring and audit with the goal of detecting misbehaving entities and subsequently updating their trust metrics.

Let us consider a path vector $A \rightarrow B \rightarrow C \rightarrow E$ which transports all communications between the end points $A.a$ and $E.e$. First, the packet is routed from $A.a$ to A's gateway $A.gateway$. Security issues in routing a packet from $A.a$ to $A.gateway$ are identical to that of routing in a single routing domain. Things get more interesting when the packet leaves A's domain. When $A.gateway$ has to route a packet to $E.e$, it has to identify a trusted path to E's gateway. As described in the earlier section, we bind a path vector ($B \rightarrow C \rightarrow E$) with an end point ($E$) and path characteristics (described by delay, jitter, link trust, reliability, etc). Routing layer trust has to be computed and dynamically updated using a trust management system. As described earlier, a route from B to C may involve an internal route in B. Hence, A's routing layer trust in B will not only depend on B's gateway but also on B's internal route to C. Given that A has no visibility into internal routes used by B, it trust B's estimate of its route metrics.

The problem binding an end point to a route has been studied in the context of S-BGP (and its variants), which relies on two fundamental concepts: Address Attestation that binds an entity e to an organization E and Route Attestation that is an authorization created by one a domain (say E) to its neighboring domain (say C) to advertise a route (say, $C \rightarrow E$). More recently, improvements apply sequential multi-signatures and ordered multi-signatures (OMS) to authenticating path vectors. OMS allows which allows signers to attest to a routing advertisement as well as the order (path) in which they signed. In addition to route attestations, we require route characteristics to be aggregated and authenticated. As noted before route characteristics may be aggregated along a route using a simple calculus. The key challenge here is how to authenticate an aggregated route metric in accordance with an ordered path vector and a route performance metrics calculus.

Given authenticated routes with route metrics a trust management system must be capable of cooperatively monitoring the network with the goal of detecting misbehaving nodes. An authenticated route metric is considered as a guarantee made by the nodes on the route. Similar to root cause analysis (RCA) that attempts to find a soft/hard failure in the network, we need monitoring and audit techniques to detect the nodes that cause a measured route metric to violate from the 'promised' route metric. For instance, let us consider a path vector $A \rightarrow B \rightarrow C \rightarrow D$, where only B is in the immediate vicinity of A. Now if packets from A to D are *lost somewhere on the path*, A may work in conjunction with domains B, C and D to deduce misbehaving nodes under the assumption that not more than a threshold number of domains are fraudulent. A uses novel root cause analysis (RCA) algorithms to identify a poorly performing link (soft RCA on delay, jitter, and reliability metrics); in the absence of complete topology data (or fraudulent topology information from a subset of domains) one can use more sophisticated network tomography techniques to pin-point misbehaviors. The key challenge here is develop algorithms that can use outputs from n monitors, such that even if k monitors operate fraudulently (e.g.: Byzantine failure), the system can accurately (low false positives and false negatives) and efficiently (low monitoring overhead) pin-point the fraudulent party.

5 Identity Attacks

One can have, some claim, as many electronic personas as one has time and energy to create.
−Judith S. Donath [7]

Naming service (e.g. domain name service (DNS)) is one of the core services offered by any network. In an open ad hoc network wherein arbitrary nodes can join the network, it is hard to verify the identity and the credentials associated with a new node in the absence of a common certification authority (CA). The worst case scenario manifests itself as a Sybil attack. In a Sybil[2] attack [7], a single malicious entity presents multiple identities and uses them to gain a disproportionately large influence, thereby undermining the outcome of de facto election algorithms, redundancy control algorithms and trust management systems.

Theoretically, in the absence of a trusted authority, an arbitrarily powerful adversary can forge infinitely many identities without being detected by the network. However, in practice, a network's vulnerability to a identity attacks depends on how cheaply identities can be generated, the degree to which the network accepts inputs from entities that do not have a chain of trust linking them to a trusted authority, and whether the network treats all entities identically. There are two prominent approaches used to mitigate Sybil attacks.

In a *Resource Challenge* based approach the amount of resources available to an adversary is challenged. An example of a CPU resource challenge is a cryptographic puzzle [11, 26]. A cryptographic puzzle ensures that if an adversary has ρ times as computationally powerful as the network nodes, then the adversary can spoof no more than ρ identities. Other challenge mechanisms focus on memory size (using matrix inversion test) and the number of radios available at a malicious entity (number of simultaneous conversations) and limit the number of spoofed identities.

In a *RF Localization* based approach, the neighbors of a malicious entity may use RF localization techniques [22] to determine the physical coordinates of a malicious entity. In the event of a Sybil attack, the purported locations of all fake identities reported by a malicious entity would appear geographically clustered (within a small radius). Standard detection theoretic approaches (e.g.: hypothesis testing) can be used to analyze cluster size and cluster radius to detect spoofed identities.

A new and a promising approach to handle identity attacks is *wireless fingerprinting*. The key idea here is to identify a node by its intrinsic hardware properties (such as the physical characteristics of its antenna). Such intrinsic properties must be hard to spoof and forge; in particular, the properties should be chosen such that an adversary should not be able to spoof more than ρ identities. Such an approach solves the *resurrecting duckling* problem [25] wherein a malicious node vanishes and reappears with a new identity elsewhere in the network. For instance, one can bind the reputation of a node to its wireless fingerprint. The network nodes may use a gossip based protocol (or a trust management system) to propagate this information on the network, thereby, curbing the resurrecting duckling problem.

[2]Named after the subject of the book *Sybil*, a case study of a woman with multiple personality disorder

6 Summary

In this report, we have outlined a realistic space and time delimited adversary model for MANETs. The model allows us to quantify security protocols as a function of the amount of resources (e.g.: space, radio spectrum, energy, mobility, etc) available to the network nodes and the adversary. Based on this model we have examined security requirements at two networking layers: physical & link layer and the routing layer; and a cross layer issue: identity management (see Figures 2 and 3).

First, at the physical and link layer, we have argued that traditional key set up protocols (PKI and a priori shared symmetric keys) may not be applicable to coalition MANETs. We have outlined two alternate approaches: information theoretic key exchange and risk based key exchange. In particular, information theoretic key exchange mechanisms offer unconditional (perfect) secrecy albeit a lower bit rate during the handshake protocol.

Second, at the routing layer, we have argued that sophisticated power saving routing protocols used by MANETs opens up security vulnerabilities in the network layer. In particular, we have argued for: novel key management algorithms for flexible end point based routing, new cryptographic schemes to support confidentiality and integrity in network coding based cooperative routing schemes and in-network aggregation schemes, and robust routing protocols to mitigate DoS attacks on multicast routing tree construction and maintenance protocols.

Third, we argued that identity management is a serious problem in coalition MANETs leading to the resurrecting duckling problem that adversely affect any trust management system. We have proposed a wireless fingerprinting approach that attempts to remotely capture intrinsic properties of a transmitter as a signature (identity) for a wireless node.

7 Acknowledgment

This work immensely benefited from many discussions held in various meetings and workshops organized by "International Technology Alliance" and "Collaborative Technology Alliance". In particular, the authors would like to acknowledge discussions held with Virgil Gligor and Pankaj Rohatgi for stressing importance of data-centric models. Pankaj Rohatgi also instigated our focus on space and time delimited adversarial models. Stephen Wolthusen provided us a validation of our thoughts on how trust cab be bootstrapped at the physical layer of a MANET. We also benefitted from discussions with John Clark, Greg Crinicione, Jorge Lobo, Kenny Paterson, John Murdoch, Brian Reviara, Morris Sloman, Benjamin Trevor, and many others in the ITA alliance.

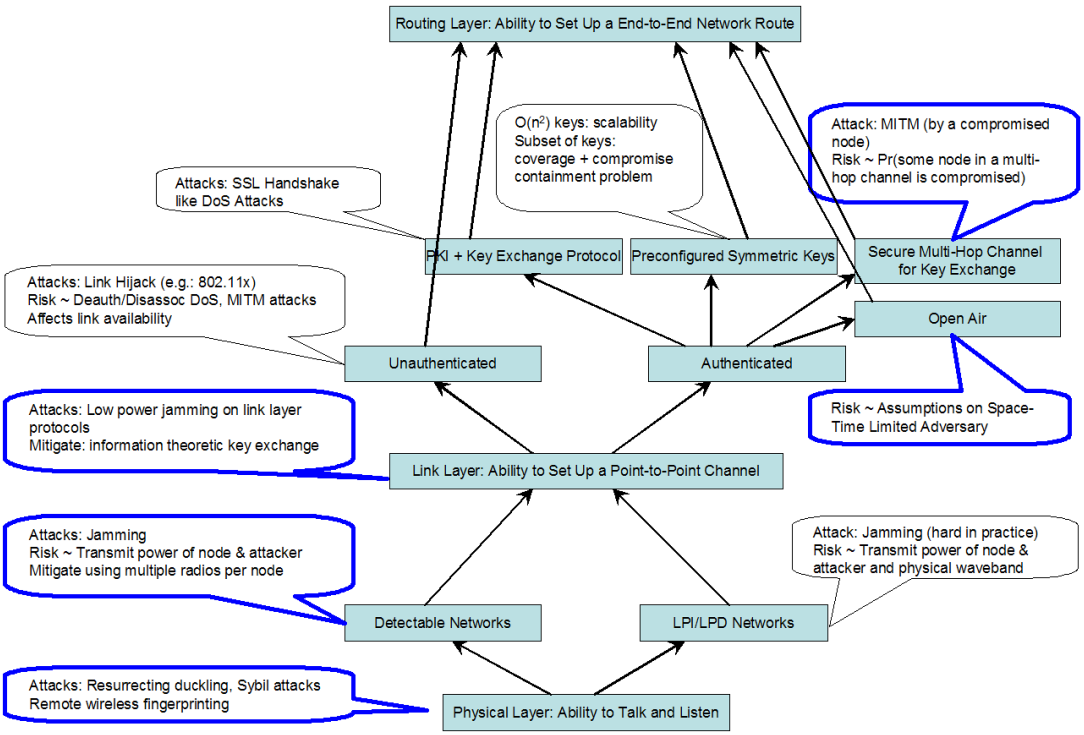

Figure 2: Physical/Link Layer Issues

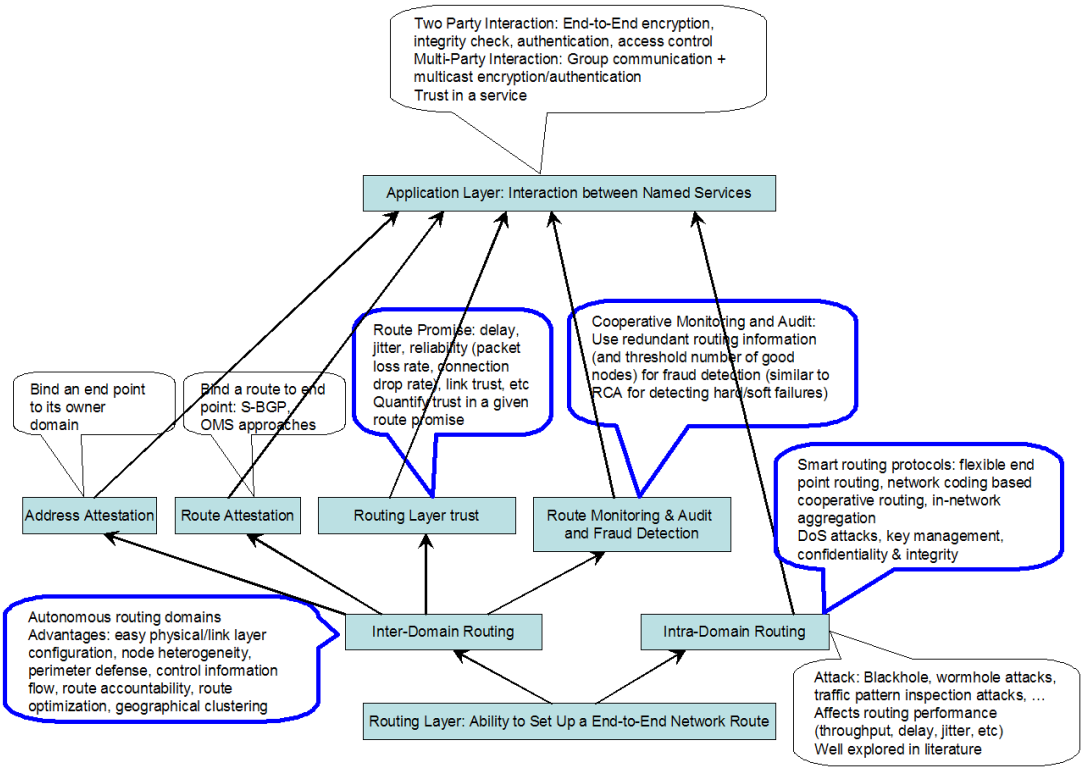

Figure 3: Routing Layer Issues

References

[1] J. Barros and M. R. D. Rodrigues. Secrecy capacity of wireless channels. In *Proceedings of the 2006 IEEE International Symposium on the Information Theory*, pages 356–360, 2006.

[2] J. Benaloh. Dense probabilistic encryption. In *http://research.microsoft.com/crypto/papers/dpe.ps*.

[3] A. Boldyreva, C. Gentry, and A. O'Neill. Ordered multi-signatures and identity-based sequential aggregate signatures with applications to secure routing. In *ACM CCS*, 2007.

[4] S. A. Camtepe and B. Yener. Key distribution mechanisms for wireless sensor networks: Survey. Technical Report TR-05-07, RPI, 2007.

[5] A. Cardenes, S. Radosavac, and J. H. Baras. Detection and prevention of MAC layer misbehavior in ad-hoc networks. In *SASN*, 2005.

[6] H. Chan, A. Perrig, and D. Song. Secure hierarchical in-network aggregation in sensor networks. In *ACM CCS*, 2006.

[7] J. Douceur. The sybil attack. In *2nd IPTPS Workshop*, 2002.

[8] S. Goldwasser and S. Micali. Probabilistic encryption and how to play mental poker keeping secret all partial information. In *14th ACM STOC, pp 365377*, 1982.

[9] Y. C. Hu and A. Perrig. A survey of secure wireless ad hoc routing. In *IEEE Security and Privacy Magazine*, 2004.

[10] A. O. H. III. Secure space-time communication. *IEEE Transactions on Information Theory*, 49(12):3235–3249, 2003.

[11] A. Juels and J. Brainard. Client puzzle: A cryptographic defense against connection depletion attacks. In *NDSS*, 1999.

[12] C. Karlof and D. Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. In *Elsevier's AdHoc Networks Journal, Special Issue on Sensor Network Applications and Protocols*.

[13] C. Karlof and D. Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. In *Elsevier's AdHoc Networks Journal*, 2002.

[14] A. Khisti, A. Tchamkerten, and G. Wornell. Secure broadcasting with multiuser diversity. In *44th Allerton Conference on Communication, Control and Computing*, 2006.

[15] A. Khisti and G. Wornell. The MIMOME channel. In *45th Allerton Conference on Communication, Control and Computing*, 2007.

[16] A. C. S. Koorapaty, H.; Hassan. Secure information transmission for mobile radio. *Communications Letters, IEEE*, 4(2):52–55, Feb 2000.

[17] P. Kyasanur and N. Vaidya. Detection and handling MAC layer misbehavior in wireless networks. In *DSN*, 2003.

[18] Y. W. Law, L. van Hoesel, J. Doumen, P. Hartel, and P. Havinga. Energy-efficient link-layer jamming attacks against wireless sensor network mac protocols. In *SASN '05: Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks*, pages 76–88, New York, NY, USA, 2005. ACM.

[19] X. Li, M. Chen, and E. P. Ratazzi. A randomized space-time transmission scheme for secret-key agreement. In *Proceedings of the 39st Annual Conference on Information Sciences and Systems, CISS 2005, 16-18 March 2005, Johns Hopkins University, Department of Electrical Engineering, Baltimore, MD, USA*.

[20] Z. Li, W. Trappe, and R. Yates. Secret communication via multi-antenna transmission. In *CISS*, pages 905–910. IEEE, 2007.

[21] U. M. Maurer. Secret key agreement by public discussion from common information. *IEEE Transactions on Information Theory*, 39(3):733–742, 1993.

[22] D. Nicelescu and B. Nath. Ad hoc positioning (APS) using AOA. In *Proceedings of IEEE Infocom, pp: 1734-1743*, 2003.

[23] P. Paillier. Public-key cryptosystems based on composite degree residuosity classes. In *EUROCRYPT pp223-238*, 1999.

[24] S. Radosavac, J. H. Baras, and I. Koutsopoulos. A framework for MAC misbehavior detection in wireless networks. In *WiSE*, 2005.

[25] F. Stajano and R. Anderson. The resurrecting duckling: Security issues for ad-hoc wireless networks. In *In Workshop on Security Protocols, LNCS 1796, Springer-Verlag, pp. 172-194*, 1999.

[26] X. Wang and M. K. Reiter. Defending against denial-of-service attacks with puzzle auctions. In *IEEE Symposium on Security and Privacy*, 2003.

[27] E. Xiaohua Li; Juite Hwu; Ratazzi. Array redundancy and diversity for wireless transmissions with low probability of interception. *IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP 2006*, 4:IV–IV, 14-19 May 2006.

[28] W. Xu, W. Trappe, Y. Zhang, and T. Wood. The feasibility of launching and detecting jamming attacks in wireless networks. In P. R. Kumar, A. T. Campbell, and R. Wattenhofer, editors, *MobiHoc*, pages 46–57. ACM, 2005.