Security and Privacy-Preserving Communication in Hybrid Ad Hoc Networks

Srdjan Capkun, Jean-Pierre Hubaux and Markus Jakobsson

1

Paper Outline

- Introduction
- System Model
- Privacy Goals and Challenges
- Overview of the Solution
- Privacy Preserving Routing
- Security and Performance
- Related Work / Conclusion

2

Introduction

- Objective is to provide both routing security and privacy preservation for hybrid ad hoc networks

- Hybrid ad hoc network
  - wireless ad hoc network + dual-homed (wireless/ wired) access points
  - Access points provide connection to wired infrastructure (therefore reach & scalability)
  - E.g. multi-hop Wi-Fi or cellular networks

3

Introduction (cont'd)

- Privacy features
  - Anonymity
    - "the state of being not identifiable within a set of subjects called the anonymity set"
  - Location Privacy
    - "ability to prevent other parties from learning one's current and past locations"
- Goal is to keep a node's identifier and location private from other network nodes

4

Introduction (cont'd)

- Approach
  - Use node pseudonyms and change frequently
    - Nodes should avoid being identified by:
      - the locations they visit
      - the type of traffic they generate
  - Enforce user accountability via dynamic, but verifiable, cryptographic keys
    - Same keys that provide confidentiality, integrity, and authentication

5

Introduction (cont'd)

- Contents of the Paper
  - Present an overview of privacy threats
  - Propose a scheme for secure and privacy-preserving communication
  - Present a quantitative analysis of privacy

6

System Model

- Network Model
- Security and Trust

7

Network Model

- System consists of:
  - A set of access points (APs), mutually connected via a high-speed backbone
    - Each AP controls a bounded geographic area called a control area
  - A set of mobile nodes

8

Network Model (cont'd)

- Assumptions
  - All comms between nodes, and between a node and an AP, are wireless
  - APs and mobile nodes have the same power range
  - All links are bi-directional, i.e. any two communicating nodes must be in each others' power range
    - Some nodes will need to user other nodes as relays to reach an AP

9

Network Model (cont'd)

- All communicating nodes access the backbone in a multi-hop fashion
- Source node (S) transmits message (m) to destination node (D) via an access point (BS)
  - S -> BS_S : uplink
  - BS_S -> BS_D: inter-station
  - BS_D -> D : downlink

10

Network Model (cont'd)

- Both uplink and downlink protocols are multi-hop, i.e. they require the participation of nodes on the route
  - These nodes are typically peers of the source and destination nodes
- All nodes in the control area are loosely time synchronized

11

Security and Trust

- Each mobile node has
  - A unique identifier
  - A secret key
- Both are known by the operator(s) of the BSs, but not by the other mobile nodes
- Contractual agreement between nodes and network operator
  - Access points monitor node behavior
  - Misbehavior can lead to service/network exclusion

12

Security and Trust (cont'd)

- Network membership includes:
  - Certificate of membership
    - In order to provide proof of membership to other nodes
  - Ability to uniquely sign a message
    - Other nodes can verify a legitimate node signed it
    - But only the network operator can identify who signed it
- This allows protocols to be secure and anonymous while holding users accountable for their behavior

13

Security and Trust (cont'd)

- However, the users do not need/want to trust each other
  - No mutual contract agreements between nodes
  - Not willing to trust each other with their identities and locations
  - Do not want to trust other nodes to correctly execute networking functions
    - E.g. forwarding packets, providing accurate routing information

14

Privacy Goals and Challenges

- Design Goals
- Privacy Challenges

15

Design Goals

- Enable user-anonymous and location-private communication
- Source (S) and Destination (D) Anonymity
  - Source anonymity means that a message is not linkable to any source, and vice-versa
  - Destination anonymity has similar definition
  - The process of sending/receiving messages does not reveal any additional info about S or D than was already known by an attacker prior to transmission

16

Design Goals (cont'd)

- Strictly a need-to-know basis
  - S needs to know the identity of D, but not its location
  - The BSs need to know who S and D are (to verify membership) and their location (to route messages successfully)
  - Nobody else (incl. the nodes on the route between S/D) should be able to infer identity or location of S/D

17

Design Goals (cont'd)

- Location is compromised if attacker can infer the BS-relative (# of hops) or absolute (physical) location of a node
  - It is assumed that no sophisticated positioning mechanism is used (e.g. GPS)

18

Design Goals (cont'd)

- Anonymity metrics
  - Anonymity set
    - Max. degree of anonymity is proportional to the size of the list of registered nodes
    - Assume a sufficiently large anonymity set
  - Entropy
    - Computed based on probabilities assigned to each identity
    - E.g. the probability that a given user is the message source
  - Both metrics are used in the analysis

19

Privacy Challenges

- Threats
  - Malicious/Compromised Users
    - Proper network operation requires nodes to share identifiers, topology info and/or locations
      - Facilities passive internal (compromised) and external (malicious) collection/analysis attacks
    - Active attacks against routing protocol
      - Periodically asking for routes to other nodes to determine topology
      - Advertising shortest route to BS in order to collect/ analyze traffic

20

Privacy Challenges (cont'd)

- Threats (cont'd)
  - Untrusted network operators
    - Can easily trace users and/or reveal their true identity
  - Unique network/interface addresses & cryptographic keys
    - Use of static/unique addresses (e.g. MAC, IP) or crypto keys/certificates (e.g. Public Key) can facilitate user tracking

21

Privacy Challenges (cont'd)

- Threats (cont'd)
  - Radio fingerprinting
    - Radio transceivers emit signals with unique fingerprints that could be used for tracking
    - Also, static S/N can facilitate pseudonym mapping

22

Overview of the Solution

- Node Pseudonyms
- Dynamic Keys

23

Node Pseudonyms

- Each node shares a secret key with the BS
- Only the central authority (and the node itself) knows this key and the true identity of the node
- Node identity is protected via a pseudonym which changes over time:

$$P_S(t) = HMAC_{K_S}(ID_S, t)$$

Note that t is a time step design parameter, and different than a device timestamp

24

Dynamic Keys

- A privacy-preserving key management scheme is proposed
  - Control area-wide secret key schemes can protect identity but completely fail if a single node is compromised
    - Misbehavior is hard to isolate as well

25

Dynamic Keys

- Dynamic public key scheme
  - Each node holds a set of key pairs …

    $(PK^1_A/PrK^1_A, \ldots, PK^n_A/PrK^n_A)$
  - … and certificates

    $Cert^k_A = [PK^k_A, SIG_{PrK_{Auth}}(PK^k_A)]$
  - Nodes use key pairs to establish symmetric secret keys with neighbors.
  - Each time node changes pseudonym, it changes key pairs and symmetric keys.

26

Dynamic Keys

- Update frequency
  - Frequency of pseudonym and key changes is a design parameter (arbitrary)
  - Can be temporal or event-driven (e.g. start of new session)
  - Other factors that determine degree of privacy include node mobility and attacker strength
  - Authors conclude that 1/min is sufficient for their scenario

27

Privacy Preserving Routing

- Protocol Overview
- Uplink
- Downlink
- Inter-station Protocol
- Book-keeping

28

Protocol Overview

- Four sub-protocols are described
  - Uplink
    - Routing from S to BS_S
  - Downlink
    - Routing from BS_D to D
  - Inter-station Protocol
    - Routing between BSs
  - Book-keeping
    - Used by BSs to track node locations, pseudonyms, and network topology

29

Uplink

- S does not know all of the pseudonyms of the nodes on the path to BS_S - only neighbor nodes
  - Nor are routing tables relevant due to frequent pseudonym changes and mobility of nodes
- Therefore a distance vector protocol is used
  - Nodes know (depending on age of latest update) their distance from BS_S as well as neighbor node closest to BS_S

30

Uplink (cont'd)

$$
\begin{aligned}
S :&\quad MHead = [P_S(t), P_A(t), t_S, Up, BS_S] \\
:&\quad E_S = E_{K_S}(D, m) \\
:&\quad M_{SA} = MAC_{K_{SA}}(MHead, E_S) \\
S \rightarrow A :&\quad [\underline{P_S(t)}, \underline{P_A(t)}, Up, \underline{t_S}, BS_S] \mid \underline{E_S} \mid \underline{M_{SA}} \\
\\
A :&\quad \text{check the validity of } M_{SA} \\
:&\quad MHead = [P_A(t), P_B(t), t_A, up, BS_S] \\
:&\quad E_A = E_{K_A}(P_S(t), E_S) \\
:&\quad M_{AB} = MAC_{K_{AB}}(MHead, E_A) \\
A \rightarrow B :&\quad [\underline{P_A(t)}, \underline{P_B(t)}, Up, \underline{t_A}, BS_S] \mid \underline{E_A} \mid \underline{M_{AB}} \\
\\
B :&\quad \text{check the validity of } M_{AB} \\
:&\quad MHead = [P_B(t), BS_S, t_B, Up, BS_S] \\
:&\quad E_B = E_{K_B}(P_A(t), E_A) \\
:&\quad M_B = MAC_{K_B}(MHead, E_B) \\
B \rightarrow BS_S :&\quad [\underline{P_B(t)}, \underline{BS_S}, Up, \underline{t_B}, BS_S] \mid \underline{E_B} \mid \underline{M_B} \\
\\
BS_S :&\quad \text{decrypt } E_B,\ E_A, \text{ and } E_S, \text{ check} \\
&\quad \text{the validity of } M_B; \\
:&\quad \text{update the distances of } S,\ A \\
&\quad \text{and } B \text{ in the distance database}
\end{aligned}
$$

31

Uplink (cont'd)

- S's identity and location is only revealed to the BS_S. Neighbors only see S as a neighbor routing traffic.
- Encryption of m & D by S guarantees that no one but BS_S can infer identity of D
- Per-hop re-encryption of m
  - allows the BS to verify the hop count and identities of the nodes along the route
  - guarantees that m cannot be tracked by an attacker
    - m is effectively altered with each hop

32

Downlink

- BS_D knows the optimal route to D hence a source routing protocol is used
- BS_D performs the following:
  - computes the current pseudonyms of the nodes on the route
  - includes them in the packet
  - sends the packet to the first node on the route

33

Downlink (cont'd)

$$
\begin{aligned}
BS_D :&\quad MHead = [BS_R, P_C(t), t_{BS}, Down, BS_D] \\
:&\quad E_{BS} = E_{K_C}(P_E(t), E_{K_E}(P_D(t), E_{K_D}(S,m))) \\
:&\quad M_{BS} = MAC_{K_C}(E_{BS}, MHead) \\
BS_D \rightarrow C :&\quad [\underline{BS_R}, \underline{P_C(t)}, \underline{t_{BS}}, Down, BS_D] \mid \underline{E_{BS}} \mid \underline{M_{BS}} \\
\\
C :&\quad \text{check the validity of } M_{BS}, \text{ decrypt } E_{K_C} \\
:&\quad MHead = [P_C(t), P_E(t), t_C, Down, BS_D] \\
:&\quad E_C = E_{K_E}(P_D(t), E_{K_D}(S,m)) \\
:&\quad M_{CE} = MAC_{K_{CE}}(E_C, MHead) \\
C \rightarrow E :&\quad [\underline{P_C(t)}, \underline{P_E(t)}, \underline{t_C}, Down, BS_D] \mid \underline{E_C} \mid \underline{M_{CE}} \\
\\
E :&\quad \text{check the validity of } M_{CE}, \text{ decrypt } E_{K_E} \\
:&\quad MHead = [P_E(t), P_D(t), t_E, Down, BS_D] \\
:&\quad E_E = E_{K_D}(S,m) \\
:&\quad M_{ED} = MAC_{K_{ED}}(E_E, MHead) \\
E \rightarrow D :&\quad [\underline{P_E(t)}, \underline{P_D(t)}, \underline{t_E}, Down, BS_D] \mid \underline{E_E} \mid \underline{M_{ED}} \\
\\
D :&\quad \text{check the validity of } MAC_{K_{DE}}, \text{ decrypt } E_E
\end{aligned}
$$

34

Downlink (cont'd)

- Similar to Uplink
  - D's identity and location is not revealed. Neighbors only see D as a neighbor routing traffic.
  - Encryption of S & m by BS_D guarantees that no one but D can infer identity of S
  - Per-hop packet content changes guarantees that m cannot be tracked by an attacker
- If the route is broken and delivery fails, it is reported to the BS – which updates route info and re-sends

35

Inter-station Protocol

- If BS_S and BS_D are owned by same authority and S and D trusts them respectively, the process is straightforward
  - Uplink packet is forwarded to BS_D where MACs are verified, message decrypted, and downlink packet created and sent.
- If S/D does not trust BS_S/BS_D, they will use their home networks, HN_S and HN_D respectively, to protect their identities

36

Inter-station Protocol (cont'd)

- If D does not trust BS_D
  - S's message will be first sent to HN_D (by BS_S ?)
  - HN_D computes D's pseudonym and sends packet to the appropriate, but untrusted, BS_D
  - BS_D than creates and routes the downlink packet to D, using D's pseudonym as the destination address

37

Inter-station Protocol (cont'd)

- If S does not trust BS_S
  - Issue: How does S prove to BS_S and neighbor nodes that it is a legitimate node without revealing it's true identity ?
    - S uses existing dynamic public keys that are certified by HN_S
    - HN_S's public key needs to be certified by the untrusted network, NU
    - Since NU trusts HN_S (at least for charging purposes), S can be considered a legitimate node without revealing its identity
    - Alternatively, NU can issue a short-term cert to S

38

Book-keeping

- BSs keep records of the time, distances, identities, and pseudonyms of the nodes in their control areas

- Associated key topics:
  - Secure and Private Topology Discovery
  - Topology Update
  - Secure Time Synchronization

39

Book-keeping (cont'd)

- Secure and Private Topology Discovery
  - Topology discovery is initiated by the BS via a discovery request

$$BS \rightarrow * : TREQ, rid, BS, t \mid SIG_{PrK_{BS}}(TREQ, BS, t)$$

  - Each receiving node forwards it to its neighbors if it has not seen the same request previously

40

Book-keeping (cont'd)

- Secure and Private Topology Discovery (cont'd)
  - Receiving nodes then perform:
    - neighborhood discovery/update
    - neighbor authentication and key establishment
    - generates an encrypted neighbor list (pseudos, PKs) and sends it back to the node that forwarded the request
  - Intermediate nodes merge the received information with their own and pass it on

41

Book-keeping (cont'd)

- Secure and Private Topology Discovery (cont'd)
  - BSs then perform the following:
    - Verify the signatures of the nodes
    - Match the PKs to users' real identities
    - Reconstruct network topology
  - Note that only BS can decrypt neighbor lists successfully. Therefore intermediate notes can not observe or modify the topology information
  - Compromised node attacks must be mitigated by the BSs detecting topology inconsistencies

42

Book-keeping (cont'd)

- Topology Update
  - Maintenance
    - Nodes determine their distances from BS by collecting distance information from neighbors
      - Protected by timestamps and shared secret keys
  - Uplink
    - When BSs receive uplink packets, it will note the route taken and can update topology accordingly.
  - Downlink
    - When nodes receive downlink packets, they can update their topology if the BS piggy-backs believed distances for the nodes on the route.

43

Book-keeping (cont'd)

- Secure Time Synchronization
  - The protocols assume only loose time synchronization
    - Reference time is provided by BSs
  - When a node is in range of a BS, it can perform clock synchronization
    - Node sends challenge encrypted with shared key
    - BS provides response which includes challenge and current/processing time, all encrypted with shared key
    - Node updates its clock using BS time values and ½ round-trip time of the challenge/response

44

Book-keeping (cont'd)

- Secure Time Synchronization
  - Nodes can use neighbors to update clock as well
    - Node sends similar challenge to all of its neighbors
    - False time info can be detected unless majority of neighbors are compromised
    - Node can complain about other nodes providing false time info to BS
  - Since pseudos and PKs do not need to be changed very frequently, node clock differences can be as high as several seconds

45

Security and Performance

- Now to analyze the privacy-preserving scheme for performance and resistance to various attacks
- Topics include:
  - Attacker Model
  - Anonymity
  - Location Privacy
  - Security of Routing
  - Performance Analysis

46

Attacker Model

- Malicious node
  - node controlled by a malicious adversary and cannot authenticate to a BS (& other nodes ?)
- Compromised node
  - Node controlled by a malicious adversary and can authenticate to a BS
  - Undistinguishable from an honest node until misbehavior is detected
- Notation: Attacker-C-M

47

Attacker Model (cont'd)

- Attacker-0-1 (single malicious node) can:
  - observe if nodes (pseudonyms) in its neighborhood sends/receives messages
  - observe which nodes (pseudonyms) in its neighborhood are neighbors to each other
  - observe signal-to-noise (S/N) ratios of the devices in its neighborhood and try to link each S/N ratio with a given node pseudonym
  - detect signal watermarks of the devices in its neighborhood and link them with node pseudonyms

48

Attacker Model (cont'd)

- Attacker-0-1 can also:
  - estimate how distant nodes in its neighborhood are from the access point (in term of number of hops), based on its physical distance to the access point.
- Attacker-1-0 (compromised) can also:
  - observe accurate pseudonym distances to the access point of the nodes (pseudonyms) in its neighborhood
  - modify network traffic or generate traffic to infer nodes' locations or real identities.

49

Attacker Model (cont'd)

- Attacker-c-m can also:
  - observe/generate intelligence-gathering traffic on a wider network area
    - would further facilitate inference of users' real identities and locations
  - May be able to send a message to D and track the message to find D's location
    - However if $BS_S <> BS_D$ this is pretty hard

50

Anonymity

- Analyze the level of source and destination anonymity achieved by the scheme based on entropy

$$H(X) = -\sum_{i=1}^{N} p_i \log_2 p_i$$

H(x) = the entropy of the system after attack

p_i = Pr(X=i), X is a discrete random variable

i = an element of the anonymity set (a node)

N = size of the node set

51

Anonymity (cont'd)

- Maximum system entropy

$$H_{max} = \log_2 N$$

- Degree of anonymity provided by system
  - Quantifies the amount of information the system is leaking

$$d = \frac{H(X)}{H_{max}}$$

52

Anonymity (cont'd)

- Recall S/D anonymity as the property that a particular message is not linkable to any S/D, and vice-versa
- Two important aspects to be analyzed
  - Anonymity of node pseudonyms
    - linkability of messages to pseudonyms and their PKs
  - Mutual linkability of node pseudonyms
    - ability for an attacker to link two or more pseudonyms to a particular node

53

Anonymity (cont'd)

- Anonymity of node pseudonyms
  - Attacker-0-1 can observe behavior of a transmitting neighbor node, $P_A(t)$ -> $P_B(t)$, and determine:
    - $P_A(t)$ is either the source or just a forwarding node
    - $P_B(t)$ is not the source
    - Other neighbor nodes are probably not the source

54

Anonymity (cont'd)

- Denoting $p(X=P_A(t)) = p_A$, an attacker could assign source probabilities as follows:
  - $p_A = 1/s$, $s <= N$, N = the # of possible sources
  - $p_B = 0$
  - $p_1 = \ldots = p_{k-1} = 0$, k = # of attacker's neighbors
  - $p_i = (1-p_A) / (N-k-1)$

55

Anonymity (cont'd)

- If $P_A(t)$ is located close to BS, almost any node in the control area could be source
- If $P_A(t)$ is located on the edge, only a few nodes could be source
- For Attacker-0-1,

$$H(X) = \frac{1}{s}\log_2(s) + (1 - \frac{1}{s})\log_2 \frac{s(N-k-1)}{s-1}$$

56

Anonymity (cont'd)

- For Attacker-0-M (M malicious nodes),

$$H(X) = \frac{1}{s'}\log_2(s') + (1 - \frac{1}{s'})\log_2 \frac{s'(N - M' - 1)}{s' - 1}$$

  - where M' = # of neighbors of M (M' = M x k) and s' <= s, s' being # of possible sources that are not neighbors of M

- For Attacker-C-0 (C compromised nodes),

$$H(X) = \frac{1}{s'}\log_2(s') + (1 - \frac{1}{s'})\log_2 \frac{s'(N - C' - C - 1)}{s' - 1}$$

  - where C' = # of neighbors of C (C' = C x k)

57

Anonymity (cont'd)

- Note that the maximum entropy for Attacker-0-M and Attacker-C-0 differs
  - The size of the anonymity set for the former is N, and N-C for the latter
  - Attacker-0-M, $H_{max}(X) = \log_2(N)$
  - Attacker-C-0, $H_{max}(X) = \log_2(N\text{-}C)$

58

Anonymity (cont'd)

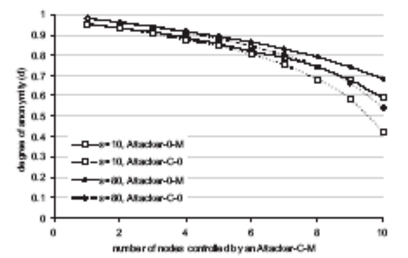


Figure 4: Pseudonym anonymity degree with Attacker-0-M and Attacker-C-0, for a control area with 80 nodes and for two sizes of the set of possible sources ($s = 10$ and $s = 80$).

- Note that as the set of possible sources (s) gets smaller and C/M increases, d decreases

59

Anonymity (cont'd)

- Also note that d does not decrease significantly with a smaller s
  - Even if the attacker knows the size of the set, it does not know which pseudos belong
    - thus any pseudo has an equal chance of being in the set
  - Anonymity only decreases with increased M/C
  - This demonstrates the scheme's effectiveness

60

Anonymity (cont'd)

- Mutual linkability of node pseudonyms
  - Observing S/N of devices
    - Attacker detects the same S/N for two (or more) pseudonyms
      - Concludes the two pseudos are used by same node
    - Assuming that the node does not move during observation
  - Signal watermarking (fingerprinting)
    - Attacker detects the same fingerprint from a node that has changed pseudonyms
      - Concludes the pseudos are linked to the same node
    - In this case, node mobility is not a mitigator

61

Location Privacy

- Both S/N and fingerprinting can also be used to track node locations
  - Once attackers can map node movements to pseudonyms
  - Signal watermark randomization can mitigate fingerprinting
- By installing a large # of nodes across the control area, the attacker can track pseudos and correlate them by location

62

Location Privacy (cont'd)

- Mix zones
  - A connected spatial region of a maximum size in which none of the nodes are in the power range of any of the nodes controlled by the attacker
- For each pseudo pair $P_X(t_1)$ and $P_Y(t_2)$, the probability X = Y is:

  $Pr(P_X(t_1), P_Y(t_2) : X = Y) = 1/MixSize$
- If the attacker can divide control area into smaller mix zones, the entropy drops and it is easier to correlate pseudonyms

63

Location Privacy (cont'd)

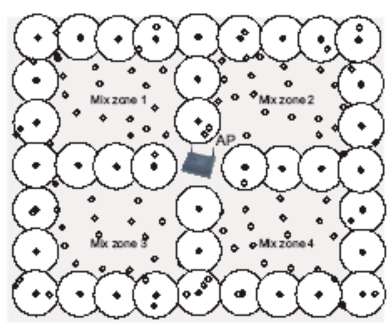
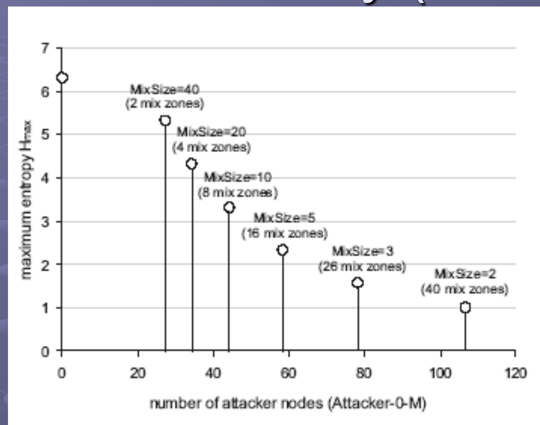


Figure 5: An example of a scenario in which the attacker divides the access point control area into four mix zones of equal size.

- In this case, the attacker divides the control area into four mix zones, lowering the entropy

64

Location Privacy (cont'd)



- Maximum entropy decreases with the number of attacker nodes and size/number of mix zones

65

Location Privacy (cont'd)

- Attacker can create a tracking matrix M[i,j]
  - Records frequencies with which nodes go from zone i to zone j through a mix zone z.
    - zones i and j are controlled by the attacker
  - Used to compute the probabilities that the pseudonyms belong to the same node, thus reducing entropy
- Pseudonym correlation success
  - Depends more on the # of nodes controlled by the attacker
  - Less on the frequency of pseudonym change

66

Location Privacy (cont'd)

- Frequency of pseudonym change
  - Needs to be only 2x higher than the average frequency a node moves from an attacker-controlled zone to a mix zone
  - Estimated to be 1/t(r)
    - where t(r) is the average time that it takes a node to cross the distance equivalent to the power range.

67

Security of Routing

- How resistant is the protocols to various attacks ?
- False distance information dissemination
  - Attacker claims it is closer to or further from BS than it really is
  - Cannot be performed by Attacker-0-M
  - Attacker-1-M will be easily detected as non-neighbor nodes will report different distances
  - Attacker-C-M could be successful if C is sufficiently large to fake the whole topology without being detected by the BS

68

Security of Routing (cont'd)

- Black Hole attack
  - Attacker advertises close proximity to BS, then gathers/drops packets
  - Can be detected similarly to false distance
  - Can also be mitigated by nodes randomizing their choice of next uplink hop
  - Black hole can't paralyze an entire hybrid network as it can for MANETs
    - Only a fraction of its neighboring nodes in its control area

69

Security of Routing (cont'd)

- Wormhole attack
  - Attacker tunnels and retransmits packets in a remote part of the network
  - Similar to Black Hole, this attack can be mitigated by:
    - Topology control by BS
    - Temporal packet leashes
- Power drain attack
  - Attacker-1-M inserts random packets into network in order to drain node batteries
  - BS controls all traffic, hence can mitigate

70

Performance Analysis

- Analyze the cryptographic and communication costs associated with the scheme
- Cryptographic cost
  - Routing is secured by symmetric key (SK)
  - Dynamic key establishment is by public key (PK)
  - SK establishment between 2 nodes
    - 1 PK signature & 1 PK signature verification per node
    - 1 PK signature verification of authority's certificate
  - SK updates are of minimal impact
    - Fixed cost, seldom performed (1/min or less)

71

Performance Analysis (cont'd)

- Cryptographic cost (cont'd)
  - Forwarded packet
    - 3 SK operations
      - Verify MAC, Re-encrypt message, Create new MAC
  - It would be possible to replace PK operations with SK-based TESLA keys (future work)

72

Performance Analysis (cont'd)

- Communication cost
  - Dynamic Key Update cost
    - PK update cost depends on frequency
      - Low, for this scheme
      - BS sends one certificate to each node at the same frequency at which keys/pseudos are updated
  - Secure and Private Routing cost
    - Low, a single MAC is added to each message on its way to and from BS

73

Related Work

- Existing research efforts related to:
  - Hybrid ad hoc networks
  - Secure Routing
  - Anonymity and Location Privacy
  - Anonymous Credentials
- See paper for details

74

Conclusion

- Proposed a scheme to secure and protect the privacy of communication in hybrid ad hoc networks
  - Both security and privacy preservation can be integrated in the same protocol
  - Privacy preservation provided by the use of pseudonyms and dynamic key renewal
  - Detailed description of the Privacy Preserving Routing protocol and associated overhead/ robustness

75

Discussion

- Performance analysis is high-level and theoretical.
  - Simulation would provide harder data
- No discussion of how nodes determine destination node identity (D)
  - Perhaps a service database is available that uses pseudos instead of true identity

76

Discussion (cont'd)

- All message traffic must go through BSs
  - No trust mechanism is provided between S & D
- S & D do not need to share a key
  - All trust is provided via BS/HN

77

Questions ? Comments ?

78