Securing Information through Trust Management in Wireless Networks

Mohit Virendra, Shambhu Upadhyaya

Computer Science and Engineering

The State University of New York at Buffalo

Buffalo, NY

Sep 24, 2004

University at Buffalo
The State University of New York

CENTER OF EXCELLENCE IN INFORMATION SYSTEMS ASSURANCE RESEARCH AND EDUCATION

Trust Schemes: Wireless Domain

Wireless Network Classification

1.Independent Ad-hoc

2. Central Authority

Trust-based Security Schemes

a. ***Independently*** Mutual information exchange between the nodes

b. Using a ***Trusted Central Authority***

Overview

Problem Statement:

Defining trust schemes for securing information in WLANs and Ad-hoc networks

Contributions:

- Trust based Admission Control scheme with a *first yes* policy for WLANs
- Trust monitoring through Intent Graphs in wireless domain
- *Actual Condition Review*-based Peer Monitoring Scheme
- Trust based security scheme for ad-hoc networks: *Physical and Logical Security Domains*
- Trust management through *Domain Heads* in ad-hoc networks

CA Assisted Scenario: WLAN model

WLAN Architecture: Two servers on the Distribution System: (a) Admission Controller (AC), (b) Global Monitor (GM)

Trust Based Admission Control
admission time trust establishment

Intent query scheme between AC and the new node

Admission decision depends on "trust value" and "intent" of the new node

Perfunctory check policy for node with unknown trust

Optimistic Approach: Trust everyone until misbehavior detected

"First Yes Policy": Node proves and maintains trust value to be in session. Trust verified while node is in the system

Looks Naïve!
But very effective in selective admission control

WLAN model: Trust Establishment

Nodes use symmetric key pairs for communication with AP, key duration dependent on trust value and "incrementing" trust also

Trust Levels: Used to (dis)allow a node to perform certain operations

Three Trust Levels: **Low, Medium and High**

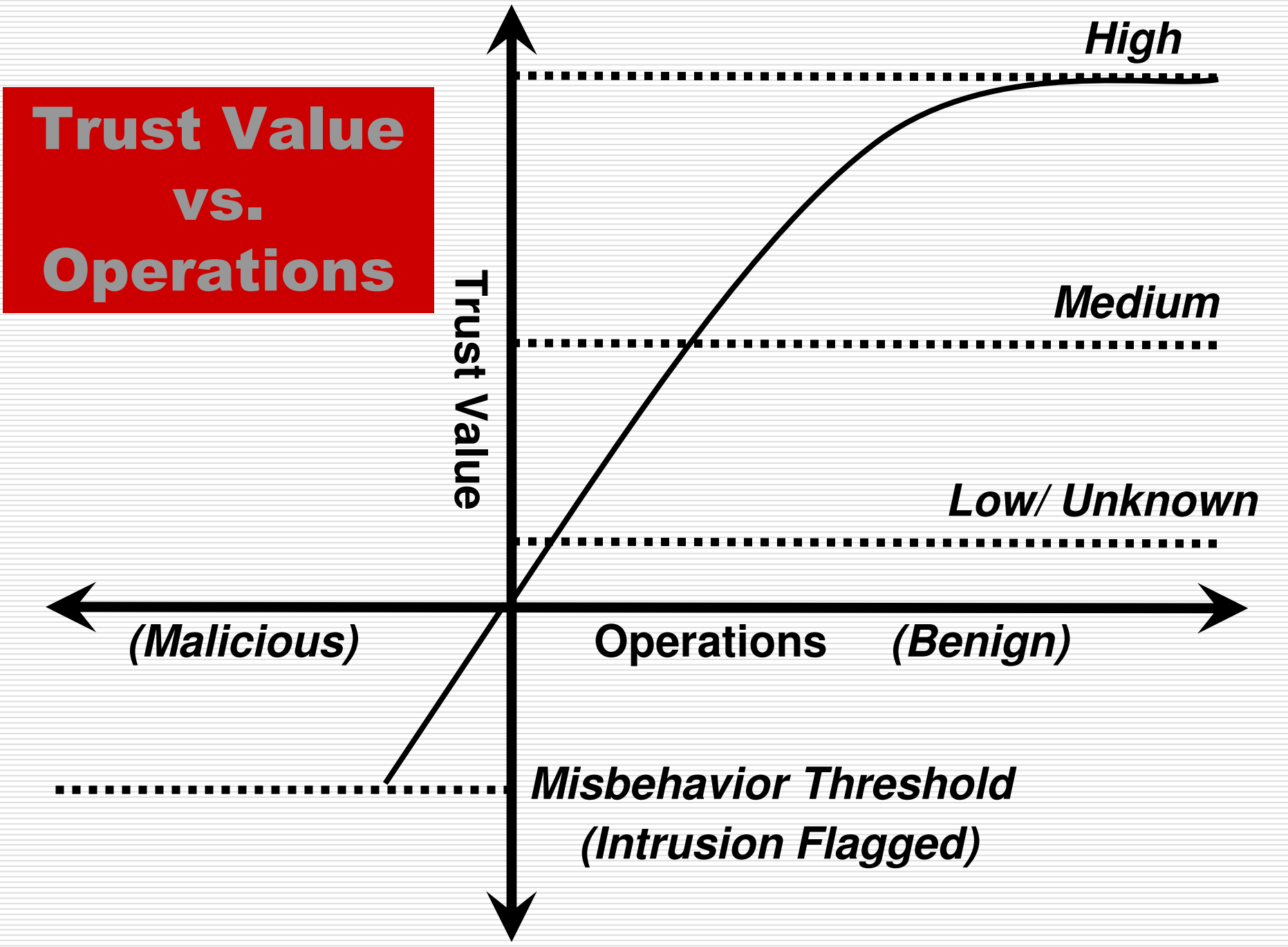
Intent Map (Graph) Generation: models node's intended behavior

FSM based on resources required & steps to be followed

During the operation, AC/GM monitors node using **GHMS** [10], checks against **Intent Map** and builds its **Trust History**

Benign transactions increase node's trust value

Relationship between transactions completed and trust value depicted by graph on next slide


Trust Value vs. Operations
High
Medium
Low/ Unknown
Trust Value
(Malicious)
Operations
(Benign)
Misbehavior Threshold
(Intrusion Flagged)

Intent Graphs and ACR generation

Tolerance in Intent Graphs	Tolerance Level and Misbehavior Threshold

Dealing with excess data rates: calculating threshold as an incremental percentage or probability as a function of data rates [11]

Each deviation => closer to threshold ~ severity of misbehavior	Flagging an intrusion == premature expiration of the session key between node and AP
Trust Values help in Leader Selection	Peer Trust Monitoring: Actual Condition Review (ACR) report generation scheme

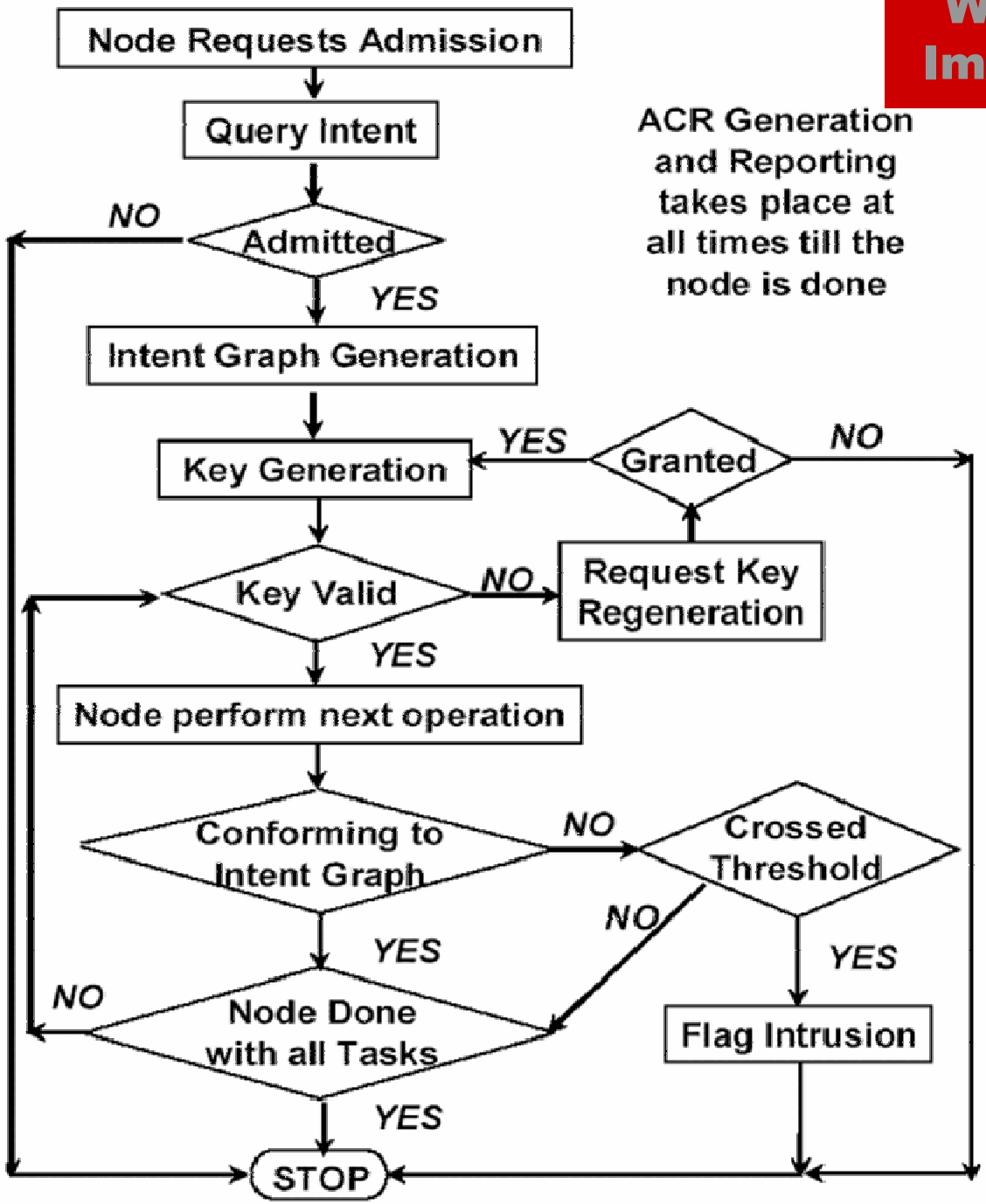
FORWARD MONITORING: APs generate ACRs about nodes

REVERSE MONITORING: Nodes generate ACRs about APs

SELF MONITORING: Nodes forced to submit their own progress report

Result: A self correcting trust monitoring system

WLAN Logical Implementation



Independent Ad-hoc Networks

Mutual Information Exchange Based Trust

Trust Based Domains

Grouping nodes with similar trust parameters and interests

Defining Qualitative Trust Parameters and Quantifying Trust

A ~> B and B ~> C, then A =~> C using B's trust as a verifier

More comprehensive schemes if A and C don't trust a common node

Node may share trust interests with nodes belonging to two or more domains: "Border Nodes"

Membership in a domain a collective decision (e.g. secure polling)

Encryption Schemes proposed by Zhou et al. [17], [18]

Domains

Nodes preloaded with keying material: establish pair-wise symmetric keys on the fly with domain members

Nodes in a Domain share a common

DOMAIN KEY

Domain Heads: Election and Rotation

Domain Heads can establish pair-wise symmetric keys with each other on the fly for trust negotiation

All inter and intra-domain communication uses symmetric pair-wise keys

Physical Trust Domains (PTDs) and Logical Trust Domains (LTDs)

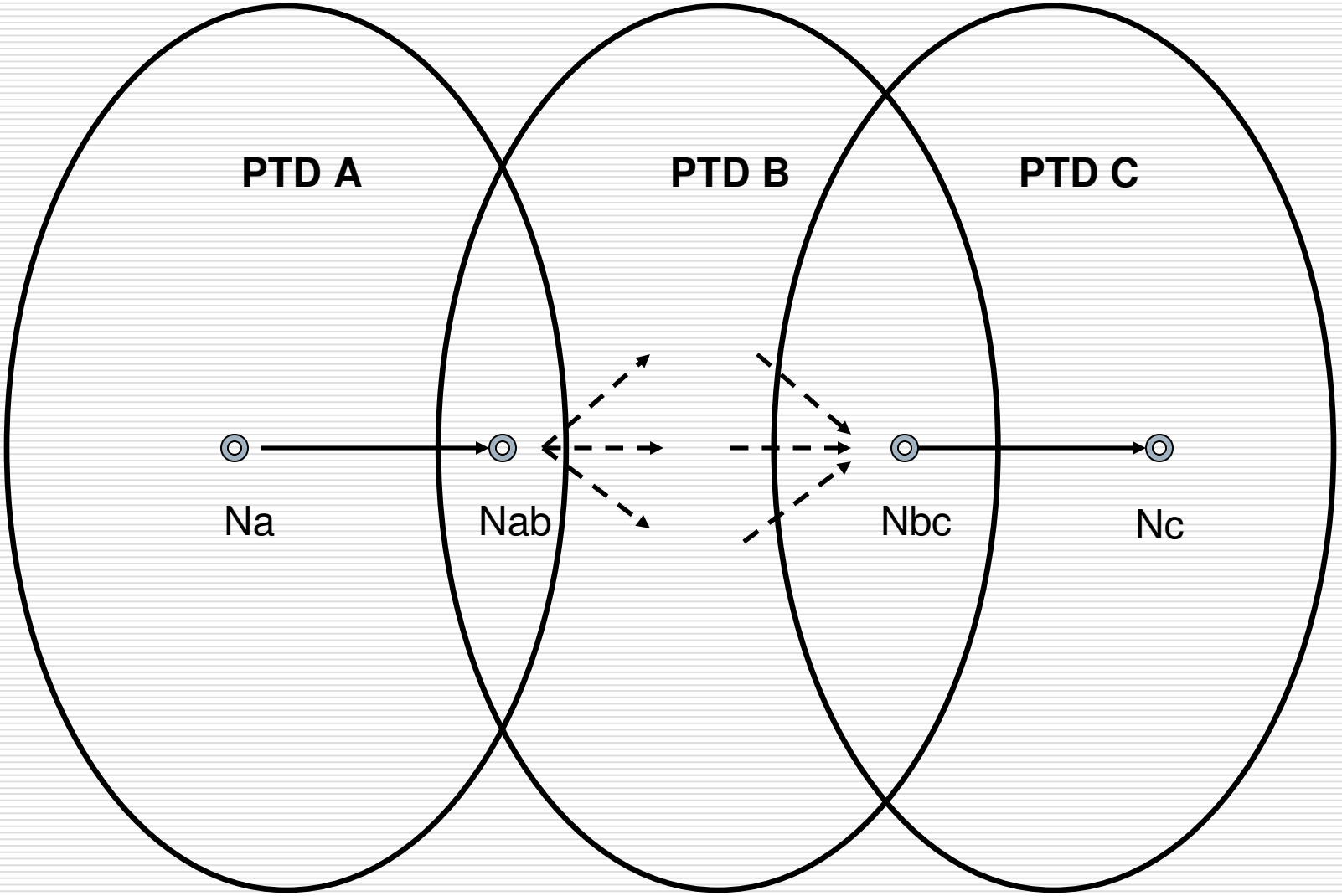
Overlapping PTDs

Non-overlapping PTDs

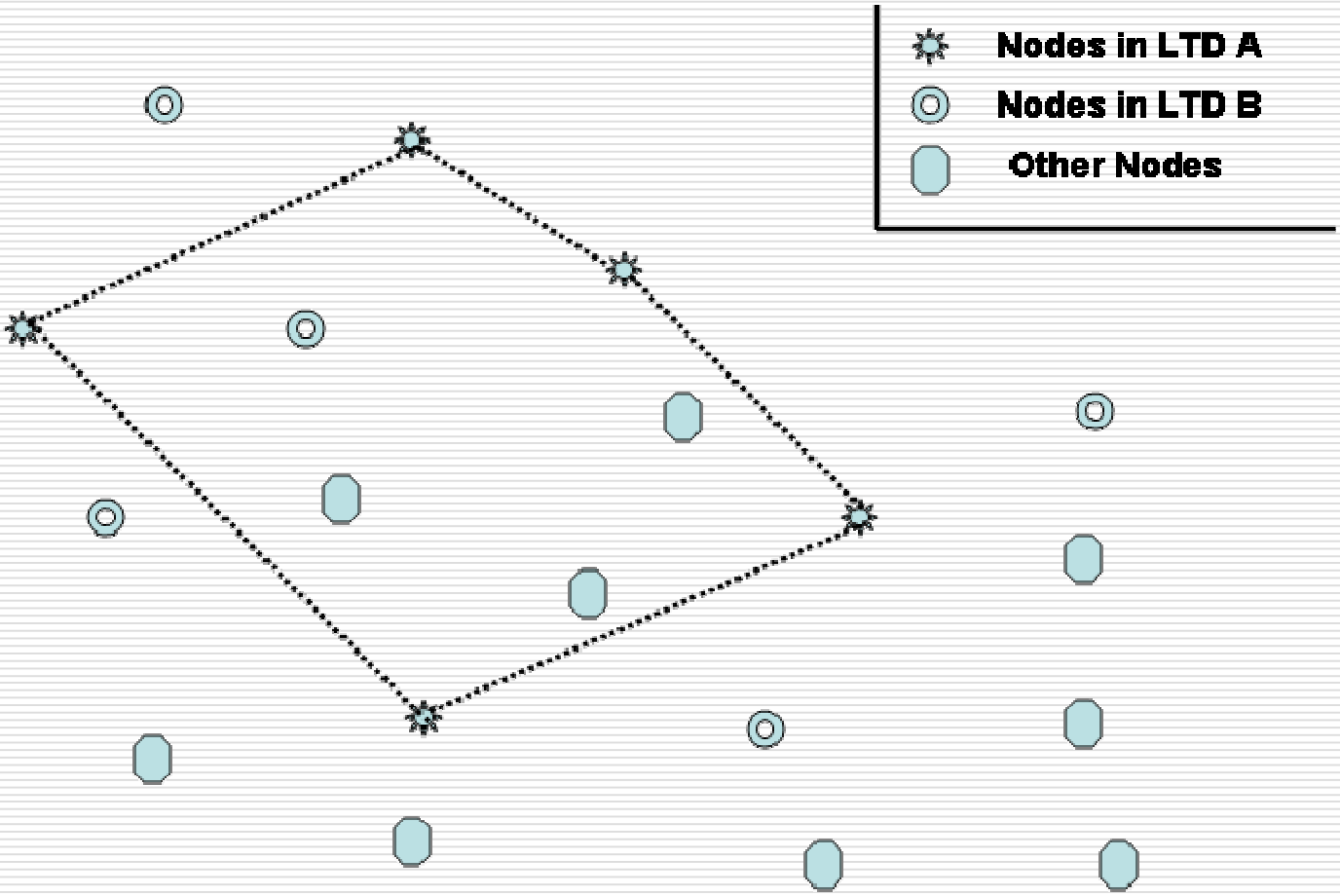
Overlapping LTDs

Non-overlapping LTDs

Overlapping PTDs



Overlapping PTDs



Non Trusted Regions and Hierarchical Trust

Communication between non-trusted regions: End to end tunnels

Tradeoff between:

Information Security and Information Relevance Lifetime

Sending information along multiple routes:

Minimum Trust Value of a route

Hierarchical Trust and Super Domains

Addressing Scalability and Reduce Control Overhead of Head Nodes

Hierarchical Trust :

Would help if a domain head (hence all domain members) are compromised

But, requires extra degree of protection for domain heads and super domain heads against attacks targeted at Central Authority

Conclusion and Discussion

Introduced trust based schemes for wireless networks

Trust based security model for WLANs

Idea of Physical and Logical Trust Domains in ad-hoc networks

Conceptual paper: describes new paradigms and concepts, require deeper investigation

Continuing Research:

Studying control overheads of the schemes introduced by us

Formalizing the "first yes" admission control scheme

Extending the ACR generation scheme to ad-hoc networks

References

1. A.Rahman and S. Hailes, "A Distributed Trust Model", New Security Paradigms Workshop 1997, ACM, 1997.
2. D. Balfanz, D. Smetters, P. Stewart and H. Wong, "Talking to Strangers: Authentication in Ad-hoc Wireless Networks", NDSS, San Diego, 2002.
3. L. Eschenauer, V.Gligor and J. Baras, "On Trust Establishment in Mobile Ad-Hoc Networks", Proc. 10th International Workshop of Security Protocols, Springer Lecture Notes in Computer Science (LNCS), Apr. 2002.
4. J. Kong, H. Luo, K. Xu, D. L. Gu, M. Gerla, and S. Lu, "Adaptive security for multi-layer ad-hoc networks," in Special Issue of Wireless Communications and Mobile Computing. Wiley Interscience Press, Aug. 2002.
5. T. Hughes, J. Denny, P. Muckelbauer, J. Etzl, "Dynamic Trust Applied to Ad Hoc Network Resources", Autonomous Agents & Multi-Agent Systems Conference, Melbourne, Australia, 2003.
6. J. Kong, P. Zerfos, H. Luo, S. Lu and L. Zhang, "Providing Robust and Ubiquitous Security Support for Mobile Ad-hoc Networks", ICNP, Riverside, CA, 2001.
7. L. Zhou and Z. J. Haas, "Securing ad hoc networks," IEEE Network Magazine, vol. 13, no. 6, pp. 24–30, Nov.'99.
8. C. Davis, "A localized trust management scheme for ad-hoc networks", Proc. 3rd International Conference on Networking (ICN'04), Mar. 2004.
9. H. Debar, M.Dacier, A. Wespi and S. Lampart, "An Experimentation Workbench for Intrusion Detection Systems", Research Report, IBM Research Division, Zurich Research Laboratory, Switzerland, 1982.
10. M. Virendra, S. Upadhyaya, X. Wang, " GSWLAN: A New Architecture Model for a Generic and Secure Wireless LAN System", 5th Annual IEEE Information Assurance Workshop, West Point, NY, June 2004.
11. M. Molloy, "Performance analysis using Stochastic Petri Nets", IEEE Trans. On Computers, vol. 39, no 9, pp. 913-917.
12. Y. Huang and W. Lee, "A Cooperative Intrusion Detection System for Ad Hoc Networks", ACM CCS SASN Worskhop, Oct. 2003.
13. Y. Huang, W. Fan, W. Lee, and P. Yu, "Cross-feature analysis for detecting ad-hoc routing anomalies", 23rd International Conference on Distributed Computing Systems, Providence, May 2003.
14. S. Upadhyaya, R. Chinchani, K. Kwiat, "An Analytical Framework for Reasoning about Intrusions", Symposium on Reliable Distributed Systems (SRDS'01), New Orleans, Oct. 2001
15. L. Zhou, F. Schneider, R. van Renesse, "COCA: A secure distributed on-line certification authority", ACM Transactions on Computer Systems 20, Nov. 2002, pp. 329–368.
16. H. Debar, M.Dacier, A. Wespi, S. Lampart, "An Experimentation Workbench for Intrusion Detection Systems", Research Report, IBM Research Division, Zurich Research Laboratory, Switzerland, 1982.
17. S. Zhu, S. Xu, S. Setia and S. Jajodia, "Establishing Pair-wise Keys for Secure Communication in Ad Hoc Networks", 11th IEEE International Conference on Network Protocols (ICNP'03), Atlanta, Nov. 2003.
18. S. Zhu, S. Xu, S. Setia, S. Jajodia and P. Ning, "An Interleaved Hop-by-Hop Authentication Scheme for Filtering of Injected False Data in Sensor Networks", IEEE Symposium on Security and Privacy, Oakland, May 2004
19. Y. Ko , N. Vaidya, "Location-aided routing (LAR) in mobile ad hoc networks", Proc. 4th annual ACM/IEEE international conference on Mobile computing and networking, pp.66-75, Dallas, Oct. 1998

Questions ?

Email: {virendra, shambhu}@cse.buffalo.edu

www.cse.buffalo.edu/~virendra