5th ACM Workshop on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks (PE-WASUN)

A Security Management Scheme Using a Novel Computational Reputation Model for Wireless and Mobile Ad hoc Networks

Azzedine Boukerche and Yonglin Ren
School of Information Technology and Engineering (*SITE*)
University of Ottawa
Ottawa, Ontario, Canada

Vancouver, BC, Canada October 27th, 2008

Outline

- Introduction
- Background
- Related Work
- Community Management
- Generalized Reputation Evaluation Model (*GRE*)
- Simulation and Evaluation
- Conclusion

Introduction

- Mobile Ad hoc Networks (MANETs) are emerging as a new form of wireless network, security support is indispensable for the potential applications of MANETs

- However, traditional security mechanisms in wired network are not suitable for MANETs, for example: firewall, access control, etc.
  - The lack of pre-deployed infrastructure
  - The low processing capability
  - The mobility of nodes
  - The short range of transmission

Introduction

- In the realm of network security, trust-based reputation appears as a new technique that is attracting more and more attention

- The traditional notion of reputation only indicates a belief or feeling regarding the behaviors of peers; whereas, the current notion of trust refers to the outcome of the observations of an expected action [1]

- In our research, we define the concept of trust as follows: it represents the degree to which a node should be trustworthy, secure, or reliable during any interaction with the node

Background

- Trust Relationship

  - *Object* and *Subject*

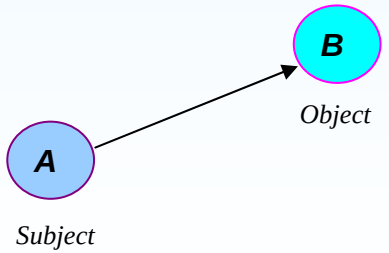
  one node, called the *object*, can forward packets for another node, called the *subject*

  - Let us assume a communication between nodes *A* and *B*, in which *A* is the *subject* and *B* is the *object*, then

  - The notation $Trust_{(Subject, Object)}$ indicates the mutual relationship established between node *subject* and node *object*

  - The trust of *A* to *B* is $Trust_{(B, A)}$

  - The trust of *B* to *A* is $Trust_{(A, B)}$



Subject and object

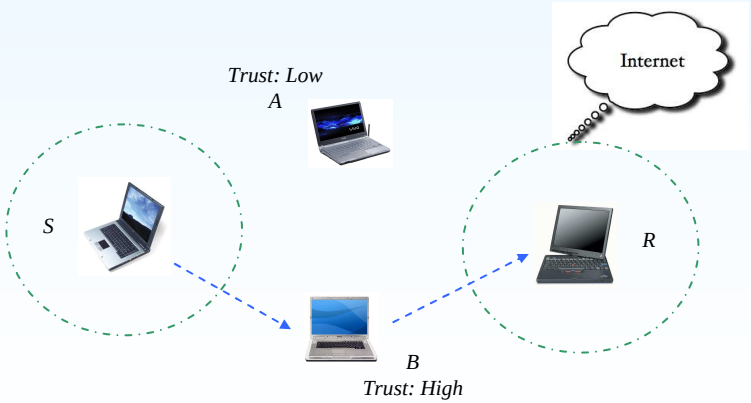
Background

- Thus, reputation can be used to evaluate other nodes' ability to execute an expected action, and a node can take advantage of this reputation information to make decisions

- If the nodes' behaviors have been faithful to the reputation evaluation system, then trust will increase between these entities. For instance, if node *A* successfully forwards a packet for *B*, then *B* thus increases its trust value $Trust_{(B, A)}$ for *A*'s collaborative behavior; *vice versa*

Background

- In a wireless and mobile environment, when *object* is trustworthy enough for *subject* can the *object* participate in the communication initiated by that *subject*
- Additionally, if the *subject* trusts the *object* to perform the intended operation, the trust relationship between these two nodes is considered to be reliable from the communicating initiator's point of view



An example of trust-based communication

Related Work

- The trust and reputation techniques are widely applied in distributed systems, for example

  - Mitra *et al.* [2] focus on the issue of managing trust and incentives in a very large-scale environment

  - Klusch [3] proposes an agent-based technology to evaluate the users' records to form their reputations

  - Selcuk *et al.* [1] design a reputation-based trust management protocol for peer-to-peer networks, which uses the ratings about users' reliability as the criteria of trust evaluation

Related Work

- Reputation is also used in the process of data transmission and routing protocols in wireless and mobile networks

  - Brahim *et al.* [4] present a formal model for cooperative mobility that involves the cooperation models for reputation management

  - Kane and Browne [5] incorporate uncertainty into their reputation computation, such that uncertainty indicates that the local opinion of the node has not been sufficiently well-informed

  - Santi *et al.* [6] propose a framework to encourage selfish nodes to work for members of a network when the network is established

Community Management

- We introduce the concept of a distributed community: for a node that is a central node, we define this node and all of its one-hop neighboring nodes as a community

  - The central node is identical to other nodes in the network and owns the same processing capabilities

  - Due to the mobility of nodes in MANETs, every one-hop community has free memberships for mobile nodes

  - When a node, called the initiator, would like to communicate with another node, called the central node, it has to send a message to establish a link between them, which is equal to joining the central node's community

Community Management

- In our reputation evaluation system each node has its own community centered at itself

  - In the meantime, the initiator will include its public key in the joining message for the later authentication and key distribution

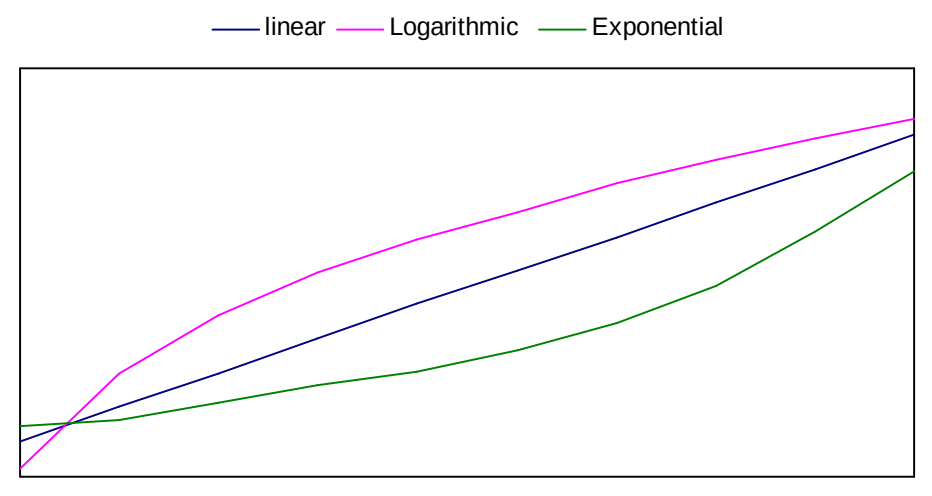
  - The central node then assigns a secret key to this newly joined node that only used for their communication

  - In order to distribute the secret key securely, the central node will encrypt it using the public key of the intended neighboring node before sending it

  - Thus, the central node generates different secret keys for different members

Generalized Reputation Evaluation Model (GRE)

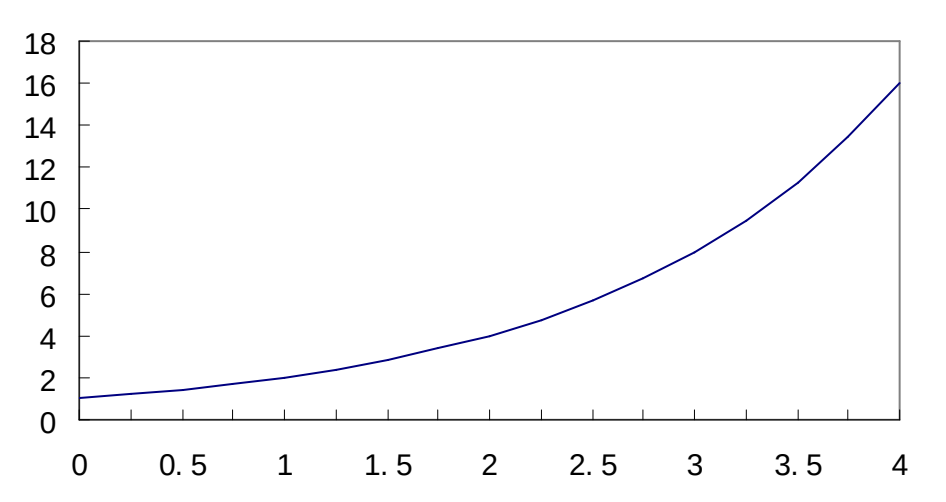
- We propose a trust-based reputation model that will update the trust value based on different increase-shapes



The trust increase shapes based on our reputation model

Generalized Reputation Evaluation Model (GRE)

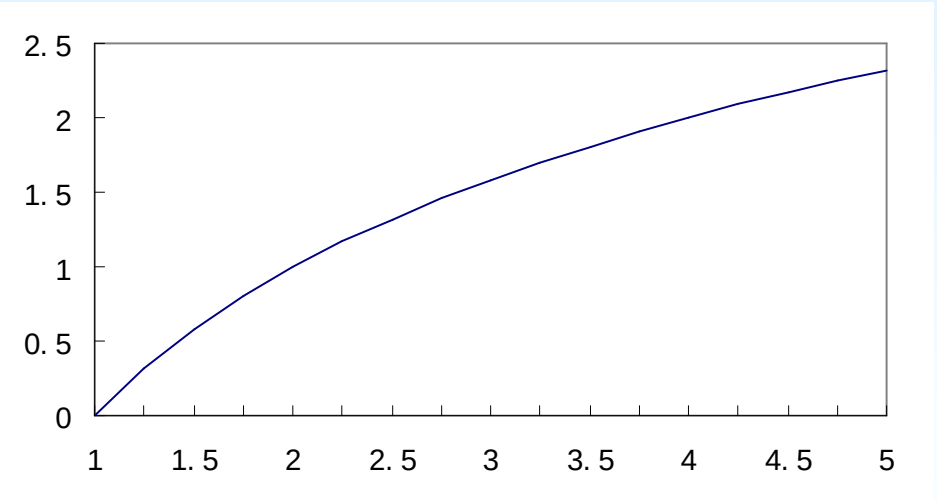
- We use exponential function to describe the reputation increases of different nodes



An example of exponential function

Generalized Reputation Evaluation Model (GRE)

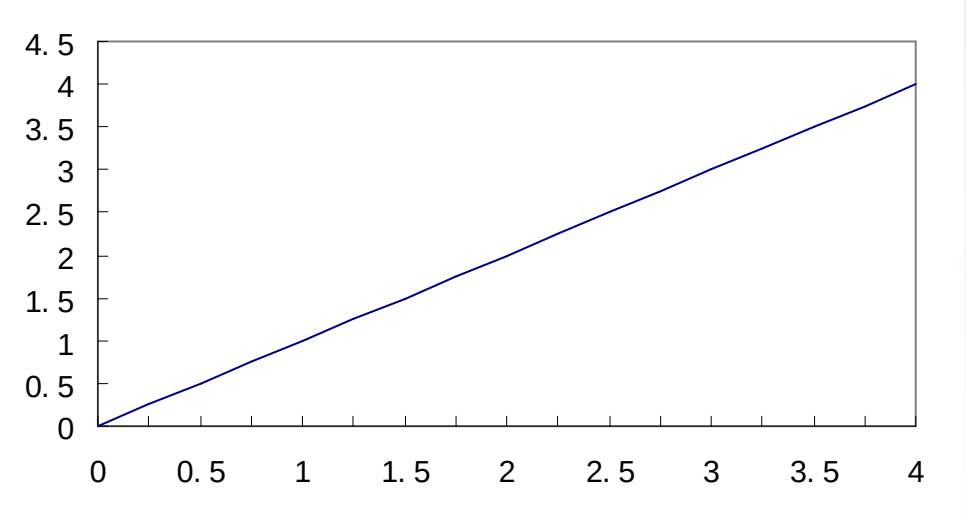
- We also use logarithmic function to describe the reputation increases of different nodes



An example of logarithmic function

Generalized Reputation Evaluation Model (GRE)

- Finally, we use linear function to describe the reputation increases of different nodes as well



An example of linear function

Generalized Reputation Evaluation Model (GRE)

- We propose a reputation evaluation theory that will evaluate the trust value of the node *n* based on different increase-shapes

  - If the node *n* has a good trust record in the past, then its current trust will increase more quickly

  - If the node *n* has fewer trust credits due to less contributions, its current trust will increase slowly

  - If the node *n* has a medium trust record, its current trust will increase moderately as well

Generalized Reputation Evaluation Model (GRE)

- A factor “recent trust (*rt*)” is introduced to record the past behaviors of *n*, since “recent trust (*rt*)” will increase if node *n* contributes more, or decreases with a lesser contribution

$$\omega = \alpha \times rt$$

- This will yield a value very close to 1 for nodes with a moderate recent trust (*rt* = 0.5), a value below 1 for nodes that have lower recent trust (*rt* < 0.5), and a value above 1 for nodes that have a higher recent trust (*rt* > 0.5)

Generalized Reputation Evaluation Model (GRE)

- Another factor “recent activities (*ra*)” is introduced, which indicates a successful forwarding, etc.

$$\beta = \kappa^{T} \times ra$$

- T measures the time that the node *n* stays in the community

- κ is a discount factor between 0 and 1

Generalized Reputation Evaluation Model (GRE)

- Finally, trust is evaluated as follows:

$$Trust = \lambda \times \frac{1-\omega^{(1+\beta)}}{1-\omega}$$

- λ is a scaling factor to keep the *Trust* at a value between 0 and 1

- Thus, the evaluation of trust is defined as a function that depends on both the time that a node has stayed in the community and the past trust that this node has achieved in recent periods

Generalized Reputation Evaluation Model (GRE)

- As for the maintenance of the community, our scheme employs a method similar to that used by the AODV routing protocol [7], which will broadcast HELLO messages periodically from the central node

- The central node updates the trust value each time based on the HELLO messages, and updates other variables in the aforementioned trust computation model as well

- Through introducing our reputation model, which is not complicated but remains efficient, GRE can be suitable for mobile environments

Simulation and Evaluation

- We evaluate our GRE model based on a set of extensive simulation experiments using the Network Simulator *ns-2* within a wireless and mobile network

- Our experiments have two purposes:

  - Verify if the established reputation model works as we predict in the simulation

  - Examine the overhead spent on reputation evaluation and the packet numbers of our scheme, based on a comparison

Simulation and Evaluation

- We compare GRE with the already accepted reputation evaluation method [8], which mainly uses the group-based mechanism to manage nodes and a linear trust computation approach to evaluate the reputation of each node in a wireless context

- We refer to this model as group-based model

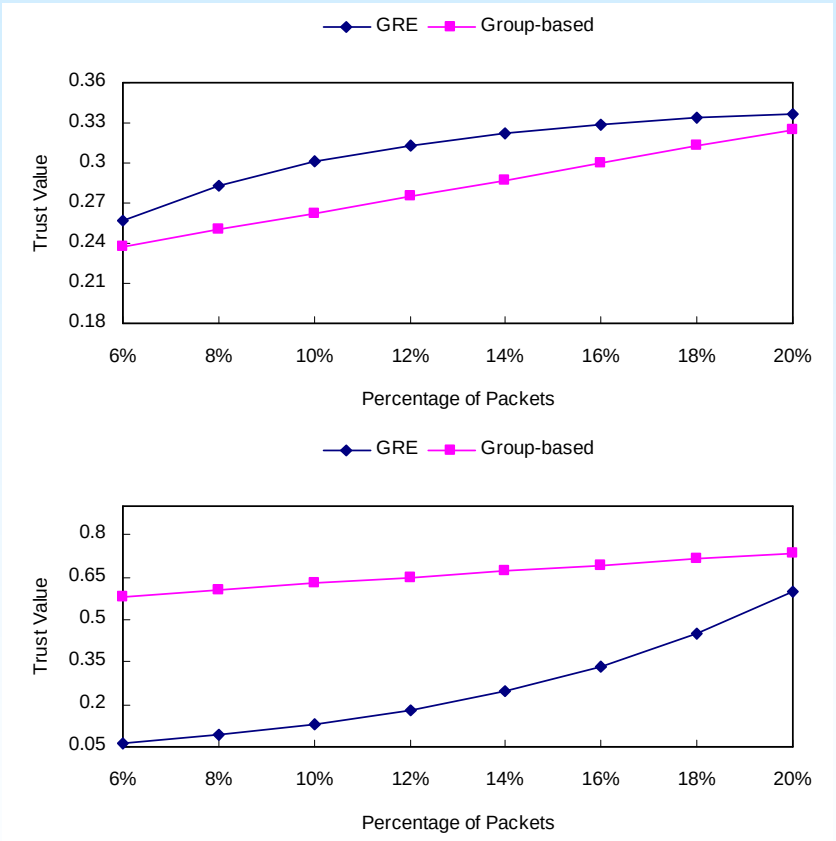
- In this model, nodes are grouped into *High*, *Medium* and *Low* trust groups and their trust changes will be evaluated based on a linear function, which can realistically reflect the basic reputation schemes according to most of these systems

Simulation and Evaluation

- The average change tendencies of reputation evaluation based on different types of nodes

  - Our GRE model has a slower increase in reputation evaluation for the nodes with low initial trust values

  - Similarly, for the nodes with high initial trust values, they will have a quick increase in reputation evaluation based on our GRE model

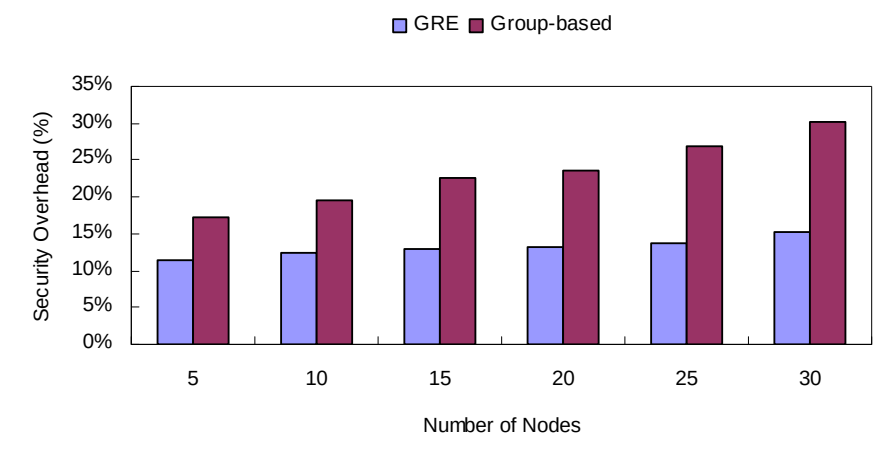


Average reputation changes of GRE vs. the group-based system

Simulation and Evaluation

- A comparison between the group-based model and GRE

  - GRE has a lower security overhead used for the community management than that of the group-based trust system



Security overhead of GRE vs. group-based system

Conclusion

- We introduce the concept of community which uses a distributed way to manage nodes in MANETs dynamically
- We also introduce a novel computational model of trust-based reputation evaluation that can calculate efficiently the trustworthiness of wireless and mobile devices
- We evaluate the performance of our scheme based on an extensive set of simulation experiments and demonstrate that our GRE system has a better performance when compared to other traditional schemes
- In the future work, we will explore the applications of our reputation model in different aspects of mobile security

Reference

[1] A. A. Selcuk, E. Uzun, and M. R. Pariente, “A reputation-based trust management system for P2P networks”, *Proceedings of International Symposium on Cluster Computing and the Grid*, 2004, pp. 251–258.

[2] A. Mitra, R. Udupa, and M. Maheswaran, “A secured hierarchical trust management framework for public computing utilities”, *Proceedings of the conference of the Centre for Advanced Studies on Collaborative research*, 2005, pp. 185–199.

[3] M. Klusch, “Information agent technology for the Internet: A survey”, *Data and Knowledge Engineering*, Vol. 36, 2001, pp. 337–372.

[4] G. B.Brahim, A.-f. Ala, D. Kountanis, and B. Khan, “A new fuzzy-based cooperative movement model in support of QoS in wireless ad-hoc network”, *Proceedings of International Conference on wireless communications and mobile computing*, 2007, pp. 158–163.

[5] K. Kane, and J. C. Browne, “Using uncertainty in reputation methods to enforce cooperation in ad-hoc networks”, *Proceedings of the 5th ACM workshop on wireless security*, 2006, pp. 105–113.

[6] P. Santi, S. Eidenbenz, and G. Resta, “A framework for incentive compatible topology control in non-cooperative wireless multi-hop networks”, *Proceedings of the workshop on dependability issues in wireless ad hoc networks and sensor networks*, 2006, pp. 9–18.

[7] C. E. Perkins and M. E. Royer, “Ad hoc on demand distance vector (AODV) routing”, IETF Internet Draft, www.ietf.org, 1997.

[8] J. Liu, D. Sacchetti, F. Sailhan, and V. Issarny, “Group management for mobile Ad Hoc networks: design, implementation and experiment”, *Proceedings of the 6th conference on Mobile Data Management*, 2005, pp. 47–54.

Thank you!