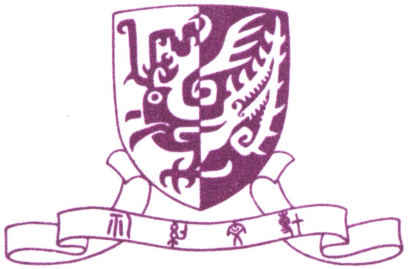
Achieving Secure and Cooperative Wireless Networks with Trust Modeling and Game Theory



PhD Oral Defense

Name: Li Xiaoqi, CSE, CUHK

Supervisor: Michael R. Lyu

Date: May 29th, 2009

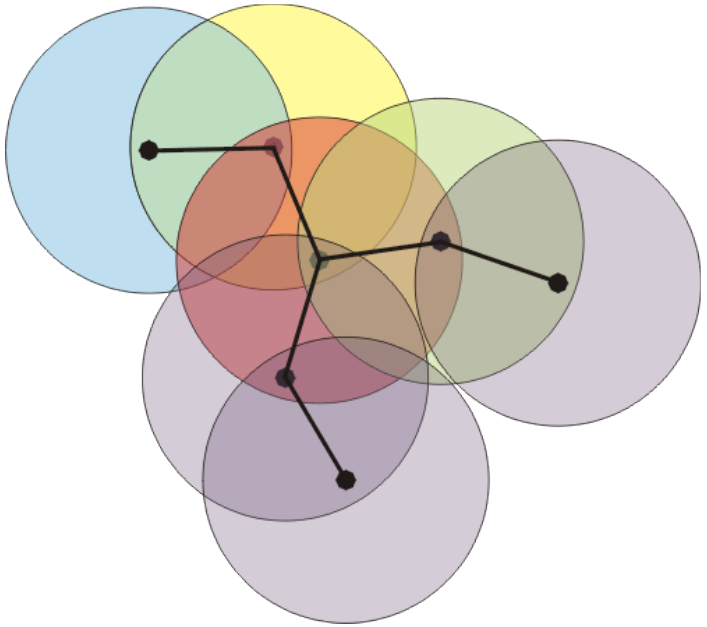
Venue: SHB 1027

Outline

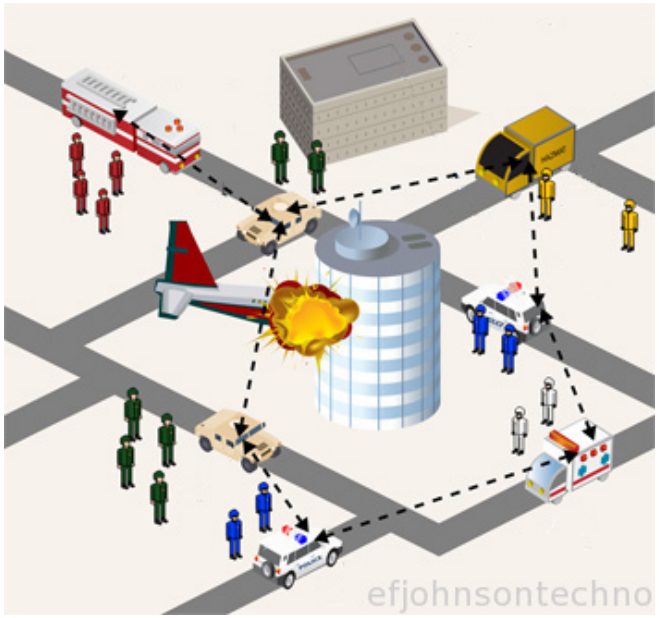
- Background of Mobile Ad Hoc Networks
- Thesis part I
  - A Trusted Routing Protocol for Security Issues of Mobile Ad Hoc Networks
- Thesis part II
  - A Coalitional Game Model for Security Issues of Wireless Networks
- Thesis part III
  - A Coalitional Game Model for Selfishness Issues of Wireless Networks

Mobile Ad Hoc Network (MANET)

- MANET is a collection of mobile nodes which communicates over wireless media.
- Characteristics
  - Decentralization
  - Self-organization
  - Cooperation
  - Openness
  - Uncertainty



Applications of MANET



Disaster Relief

Battlefield Communication

Outdoor Meeting

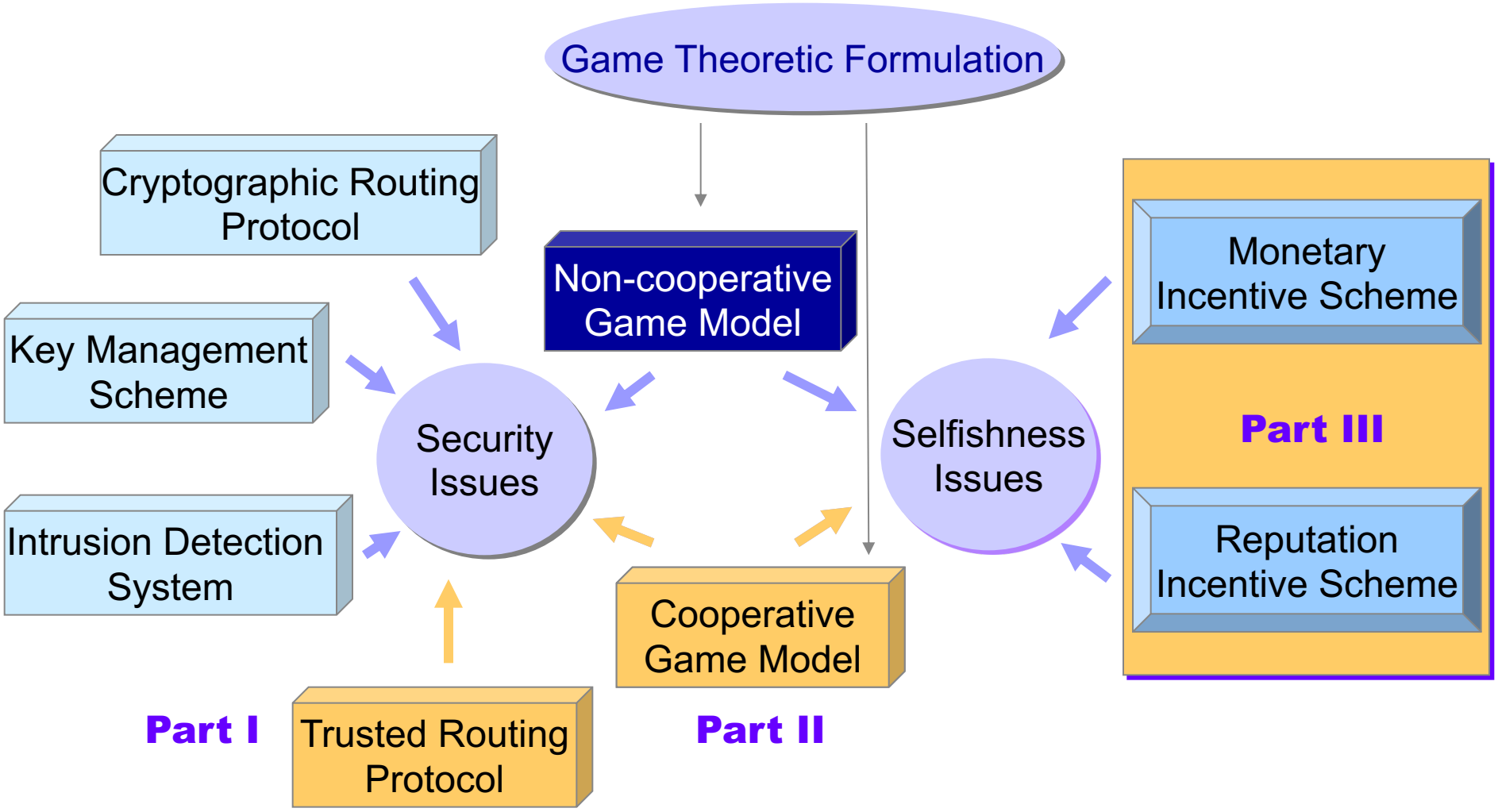
Ubiquitous Peer-to-peer Market

Multi-person Game Through Bluetooth

Limitations of MANET

- Security Issues
  - Self-organization, decentralization and openness introduce insecurity.
  - Nodes lack sufficient information about each other.
  - Malicious nodes can join the network freely.
  - The routing protocol has no security considerations.
- Selfishness Issues
  - Being cooperative is the design goal of MANET.
  - Nodes belong to different self-interested entities.
  - The mobile devices have limited resources.

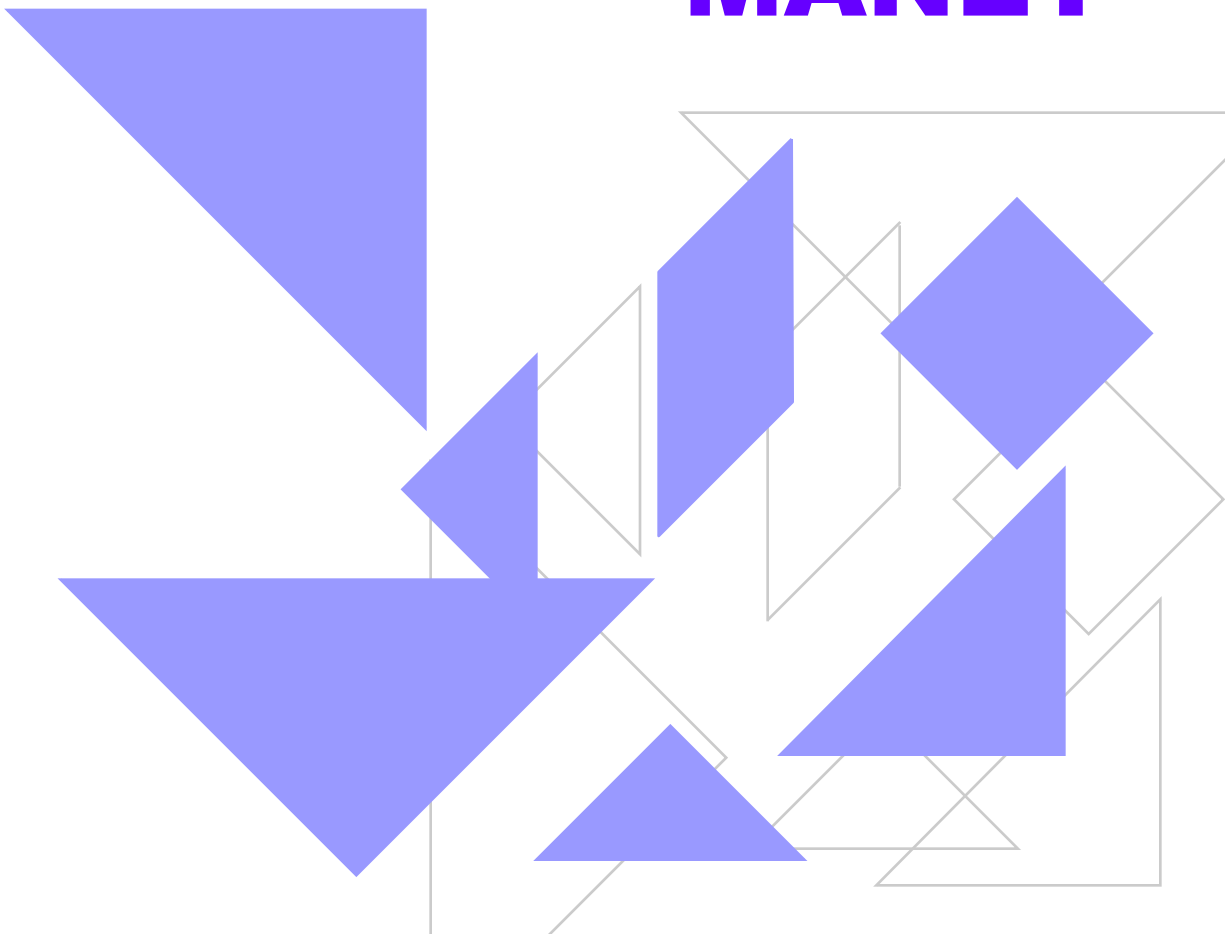
Thesis Scope



Objectives and Assumptions

- Objectives:
  - A self-organized, cost-effective, trusted routing protocol
  - Coalitional game models with security and throughput characteristic functions
  - An incentive routing scheme with a stable coalitional game solution
- Assumptions:
  - Watchdog mechanism or an intrusion detection system in each node
  - Pre-distributed cryptographic scheme as an assistance
  - Existing payment method

Part I: Trusted Routing Protocol for Security Issues of MANET



Related Work and Motivations

- Two categories of security solutions
  - Secure routing protocols
  - Key management mechanisms
- Most of the two categories of solutions require:
  - A trusted authority to issue certificates
  - A centralized server to monitor the networks
  - A secret association between certain nodes
  - Cryptographic authentication at each routing packet
- Disadvantages
  - Destroy the self-organization nature of MANET
  - Introduce huge performance overhead
  - Single point of failure
  - Less of efficiency and availability

Contributions of Part I

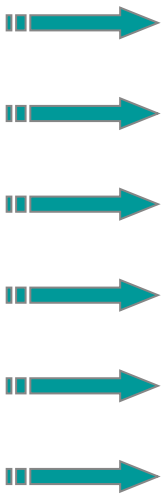
- We, for the first time, introduce the idea of "trust" and "trust model" into the design of secure routing protocols for MANET.
- We novelly derive our trust model based on subjective logic which can fully represent the properties of the trust relationships in MANET.
- We design a trusted routing protocol (TAODV) based on our trust model, which is both secure and cost effective.
- We also enhance the subjective logic to obtain a better trust evaluation.

What is Trust?

- Trust is fundamental in transactions, interactions, and communications of human life.
- Psychologically, trust is defined as a kind of subjective behavior.
- Sociologically, trust is a means for reducing the complexity of society.
- Mathematically, trust has been studied as a measurable variable, especially as a probability value.
- Trust is also related to cooperation, recommendation, and reputation.

Why Trust for MANET?

- Node relationships in MANET
  - Care about a certain functions
  - Can exist in each node pair
  - Good or bad nodes
  - Information sharing
  - Based on past evidences
  - Lack of enough information



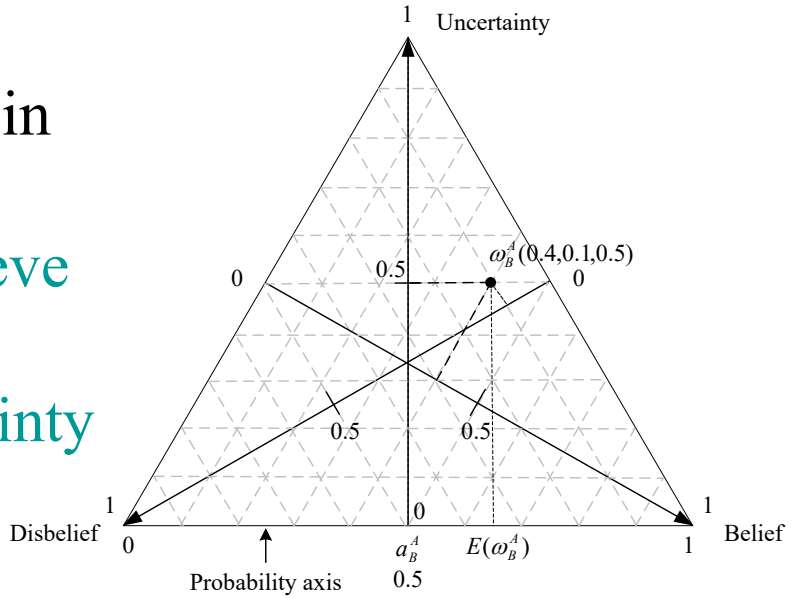
- Properties of trust relationships
  - Relativity
  - Pervasiveness
  - Asymmetry
  - Transitivity
  - Measurability
  - Uncertainty

Our Trust Model

- We choose subjective logic trust model as the basis of our trust model, because it
  - best expresses the subjectivity of trust;
  - best exhibits the properties of trust relationship in MANET, especially the uncertainty;
  - is more informative than single value trust representation;
  - is more reasonable with probability representation than discrete value representation;
  - is more flexible than upper/lower bound trust representation.
- We derive our trust model from subjective logic as follows.

Trust Representation

- Denote *opinion* $\omega_B^A \equiv (b_B^A, d_B^A, u_B^A)$ to represent the belief from node A to node B
  - b_B^A -- Probability that node A believe in node B
  - d_B^A -- Probability that node A disbelieve in node B
  - u_B^A -- Probability of node A's uncertainty about B's trustworthiness
  - $b_B^A + d_B^A + u_B^A = 1$
  - The relative atomicity a_B^A is set to 0.5 in our application.
  - The probability expectation $E(\omega_B^A) = b_B^A + a_B^A \cdot u_B^A$



Trust Mapping Between Evidence and Opinion Space

- Mapping from evidence space to opinion space:

$$\begin{cases} b_B^A = \frac{p}{p+n+2} \\ d_B^A = \frac{n}{p+n+2} \\ u_B^A = \frac{2}{p+n+2} \end{cases}$$

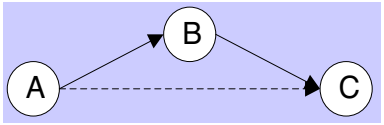
- Mapping from opinion space to evidence space:

$$\begin{cases} p = 2b_B^A / u_B^A \\ n = 2d_B^A / u_B^A \end{cases}, \quad where\ u_B^A \neq 0$$

  - p : positive evidences
  - n : negative evidences

Trust Combination

- Discounting operator : $\otimes$
  - Combine opinions along a path
  - Combine



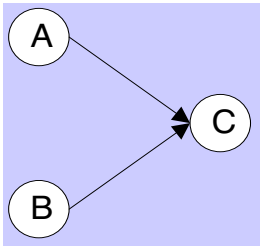
$$\left.\begin{array}{l}\omega\ (A \to B)\\ \omega\ (B \to C)\end{array}\right\} \Rightarrow \omega\ (A \to C)$$

  - Equation: Let $\omega_C^{AB} = (b_C^{AB}, d_C^{AB}, u_C^{AB})$, where

$$\begin{cases} b_C^{AB} = b_B^A b_C^B \\ d_C^{AB} = b_B^A d_C^B \\ u_C^{AB} = d_B^A + u_B^A + b_B^A u_C^B \end{cases}$$

Trust Combination

- Consensus Combination: $\oplus$
  - Combine opinions across multiple paths
  - Combine



$$\left.\begin{array}{l}\omega\ (A \to C)\\ \omega\ (B \to C)\end{array}\right\} \Rightarrow \omega\ (A,B \to C)$$

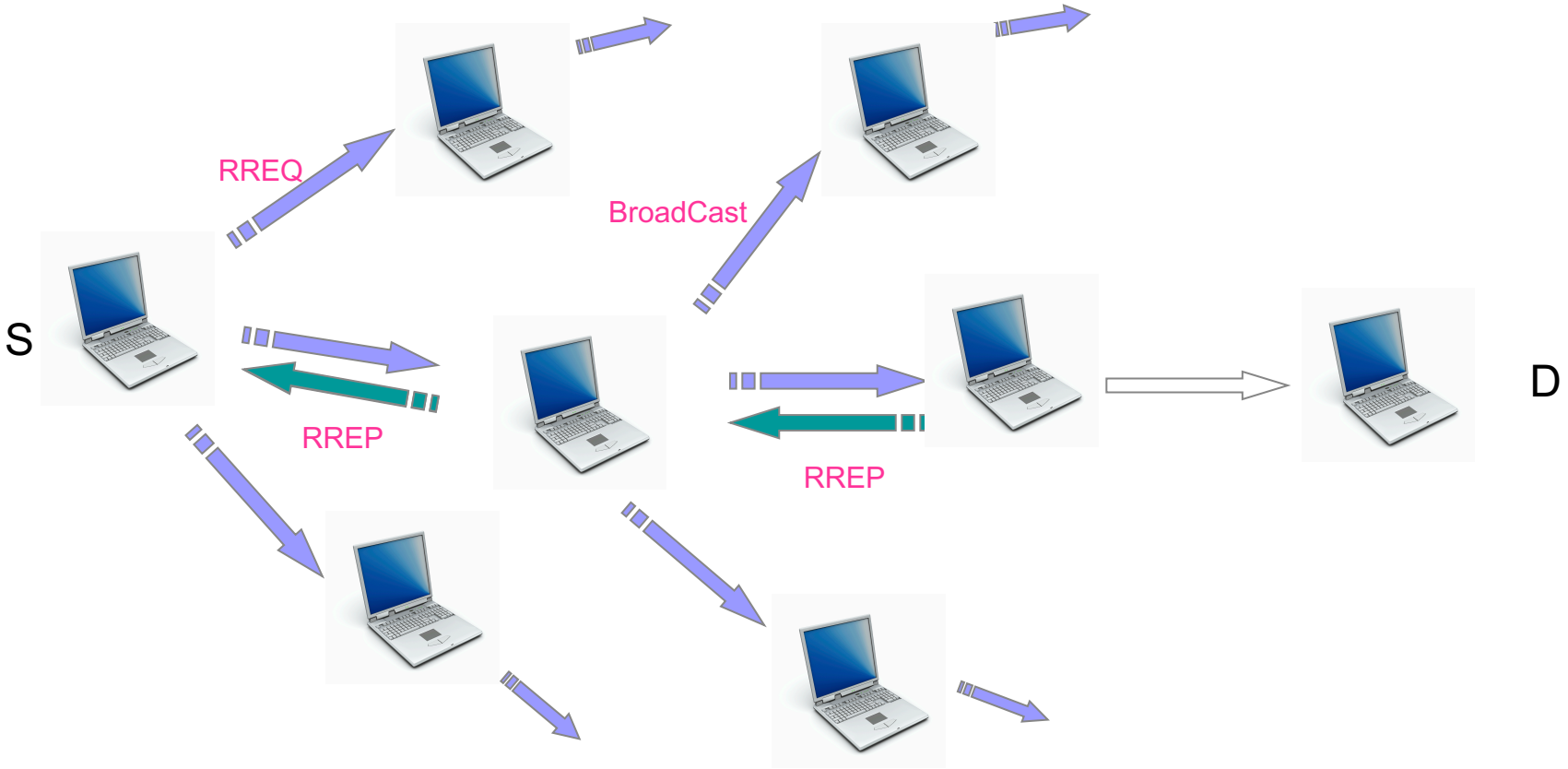
  - Equation: Let $\omega_C^{A,B} = (b_C^{A,B}, d_C^{A,B}, u_C^{A,B})$

$$\begin{cases} b_C^{A,B} = (b_C^A u_C^B + b_C^B u_C^A)/k \\ d_C^{A,B} = (d_C^A u_C^B + d_C^B u_C^A)/k, \quad where \quad k = u_C^A + u_C^B - 2u_C^A u_C^B \\ u_C^{A,B} = (u_C^A u_C^B)/k \end{cases}$$

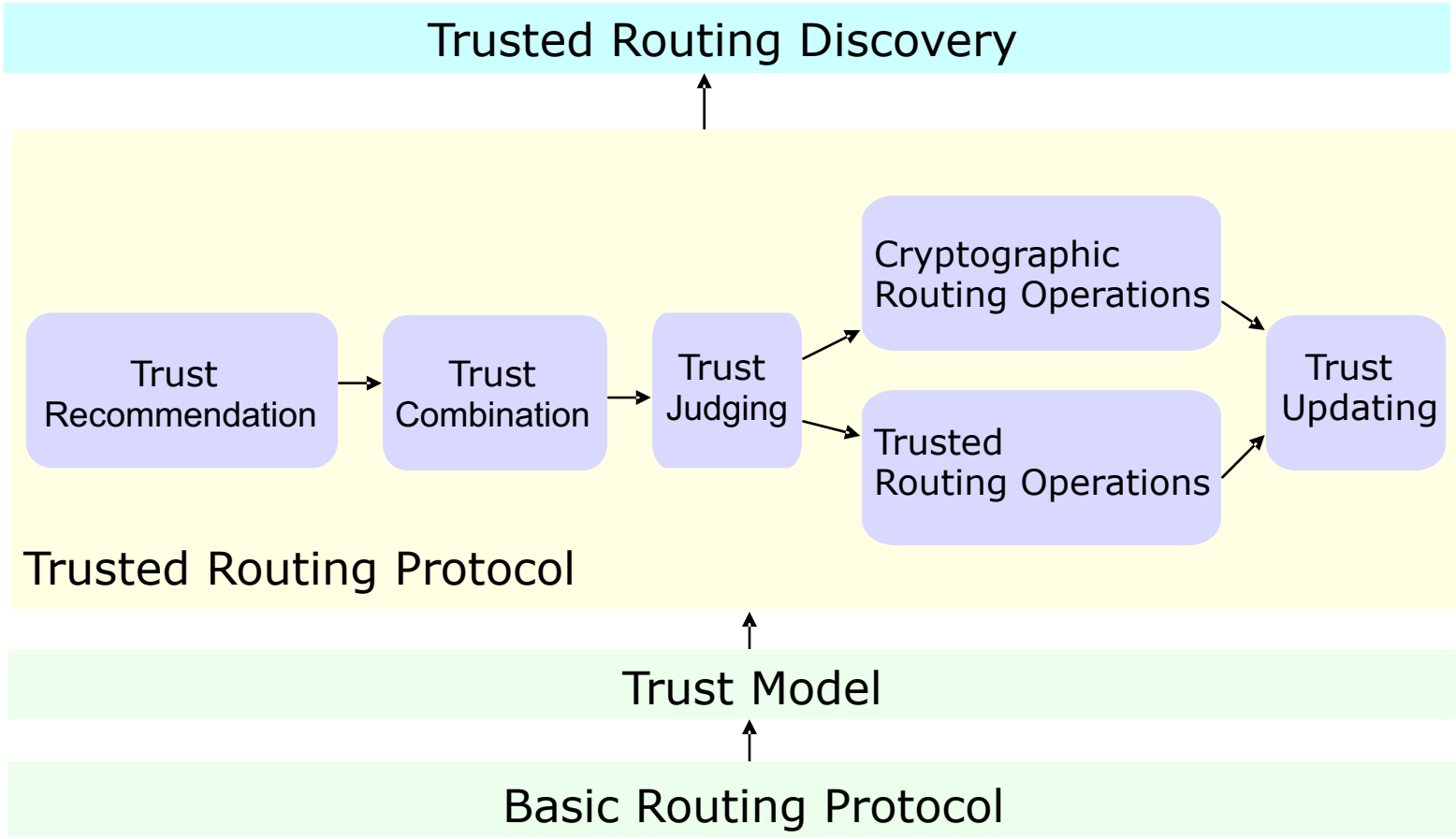
Trusted Routing Protocol for MANET

- Background of AODV
  - AODV (Ad Hoc On-Demand Distance Vector) is a popular routing protocol for MANET.
  - It is designed without security consideration.
  - It contains two main routing messages:
    - RREQ: Routing REQuest
    - RREP: Routing REPly
- We take AODV for example to design our Trusted AODV (TAODV) routing protocol based on our proposed trust model.

Routing Discovery in AODV



Framework of TAODV



Routing Table and Messages Extensions

- Add three fields into original routing table:
  - Positive events
  - Negative events
  - Opinion
- New routing table format

DestIP	DestSeq	...	HopCount	...	Lifetime	**Positive Events**	**Negative Events**	**Opinion**

- Add trust information into original AODV routing messages.
  - RREQ → Trusted RREQ (TRREQ)
  - RREP → Trusted RREP (TRREP)

Trust Judging Rules

- Predefined trust judging rules

b	d	u	Actions
		> h	Request and verify digital signature
	> h		Distrust a node for an expire time
> h			Trust a node and continue routing
≤ h	≤ h		Request and verify digital signature

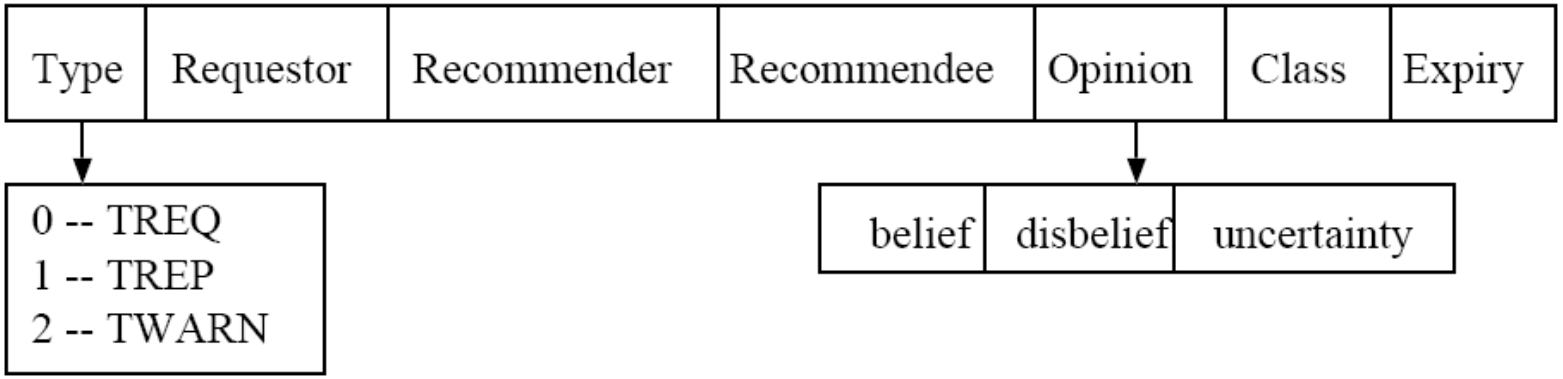
b – belief d – disbelief u – uncertainty
h – threshold which can be adjusted to meet different applications (default h=0.5)

Trust Updating Policies

- Update of evidences
  - Successful communication → Positive events increased
  - Failed communication → Negative events increased
  - Mapping from opinion space
- Update of opinions
  - Combination from recommendations
  - Mapping from evidence space

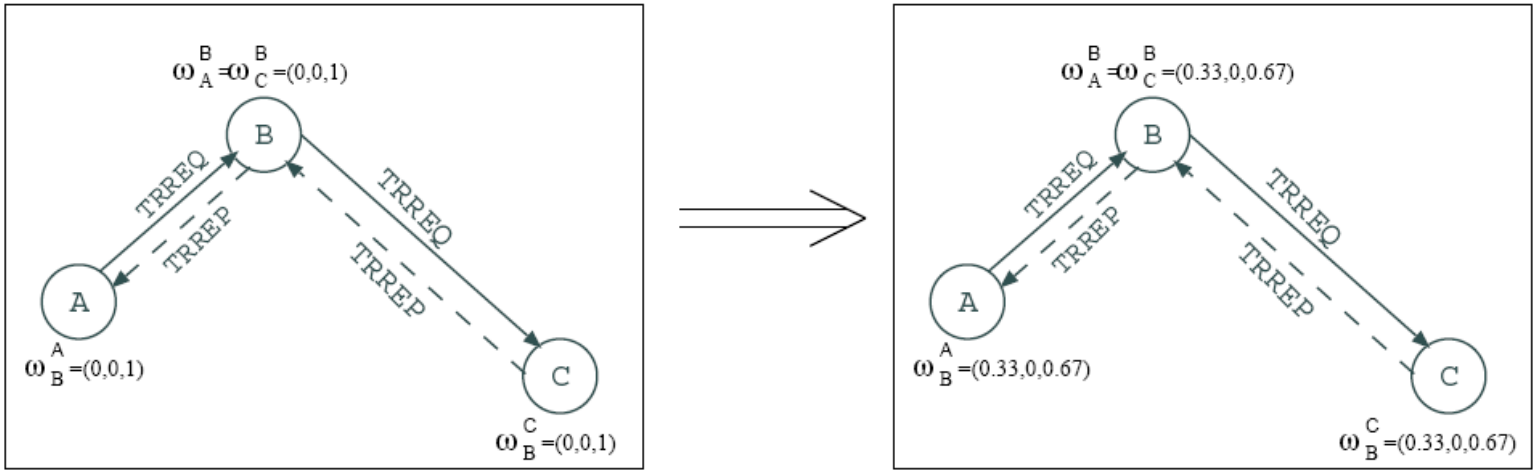
Trust Recommendation Protocol

- Exchange trust information
- Three types of messages:
  - TREQ: Trust REQuest
  - TREP: Trust REPly
  - TWARN: Trust WARNing
- Message structure:



Trusted Routing Discovery (1)

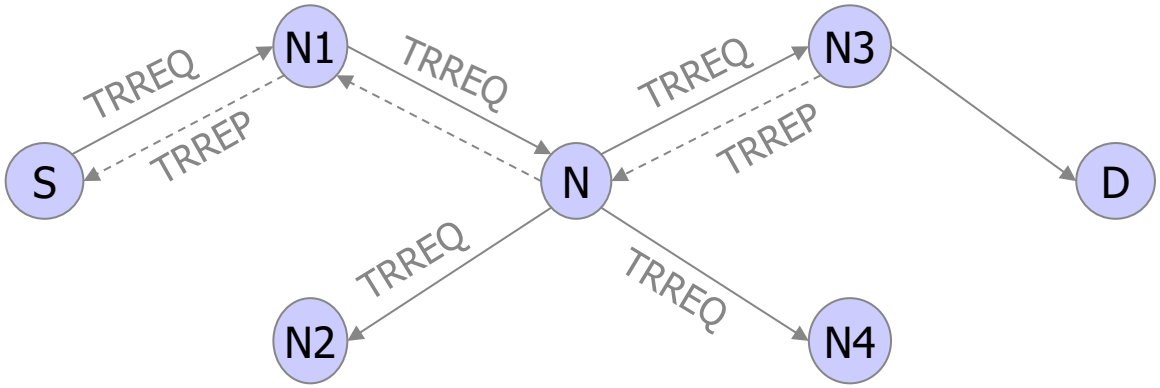
- Scenario I - Beginning of a TAODV MANET



- Initial opinions are all (0,0,1), set threshold h = 0.5
- Node A broadcasts TRREQ to discover a route to C
- Node B will authenticate A and C because of high uncertainty values (u=1) in its opinions to A and C
- Finally, if the authentication and the discovery succeed, the opinions all become (0.33,0,0.67)

Trusted Routing Discovery (2)

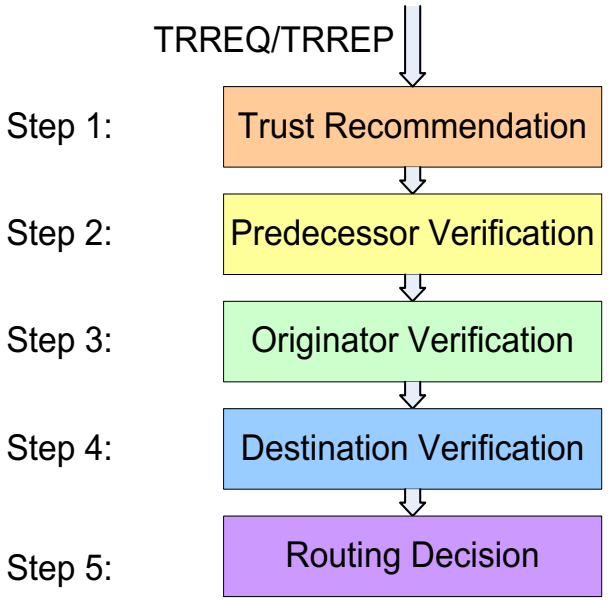
- Scenario II – A TAODV MANET After a Period of Running Time



  - Trust relationships have been established among almost all the nodes.
  - The values of uncertainty are getting smaller and smaller.
  - We take node N for example to illustrate the general procedures of TAODV.

Trusted Routing Discovery (3)

- On receiving TRREQ/TRREP, N will
  - Collect recommendations from its neighbors about the trustworthiness of the predecessor.
  - Then according to the value of the new combined opinion, it will trust, distrust or verify the source and the destination one by one.
  - If all the trust judging or digital signature verification pass, it will then perform the normal routing decisions. Otherwise, TWARN will be broadcasted.
- On receiving TREQ/TREP/TWARN
  - On TREQ, if the disbelief value is larger than the threshold, N will drop the TREQ; otherwise, N will reply TREP.
  - On TREP or TWARN, N will do opinion combinations to prevent malicious trust recommendations.



Performance Analysis

- Computation overheads are largely reduced
  - No need to perform cryptographic computations in every packet
  - Cost of each set of trust operations is $O(v)$ (v is the no. of average neighbors)
  - Cost of each set of signature operations is $O(k^3)$ (k is the length of signature)
- Not introducing much routing overhead
  - The routing message extensions are in short length.

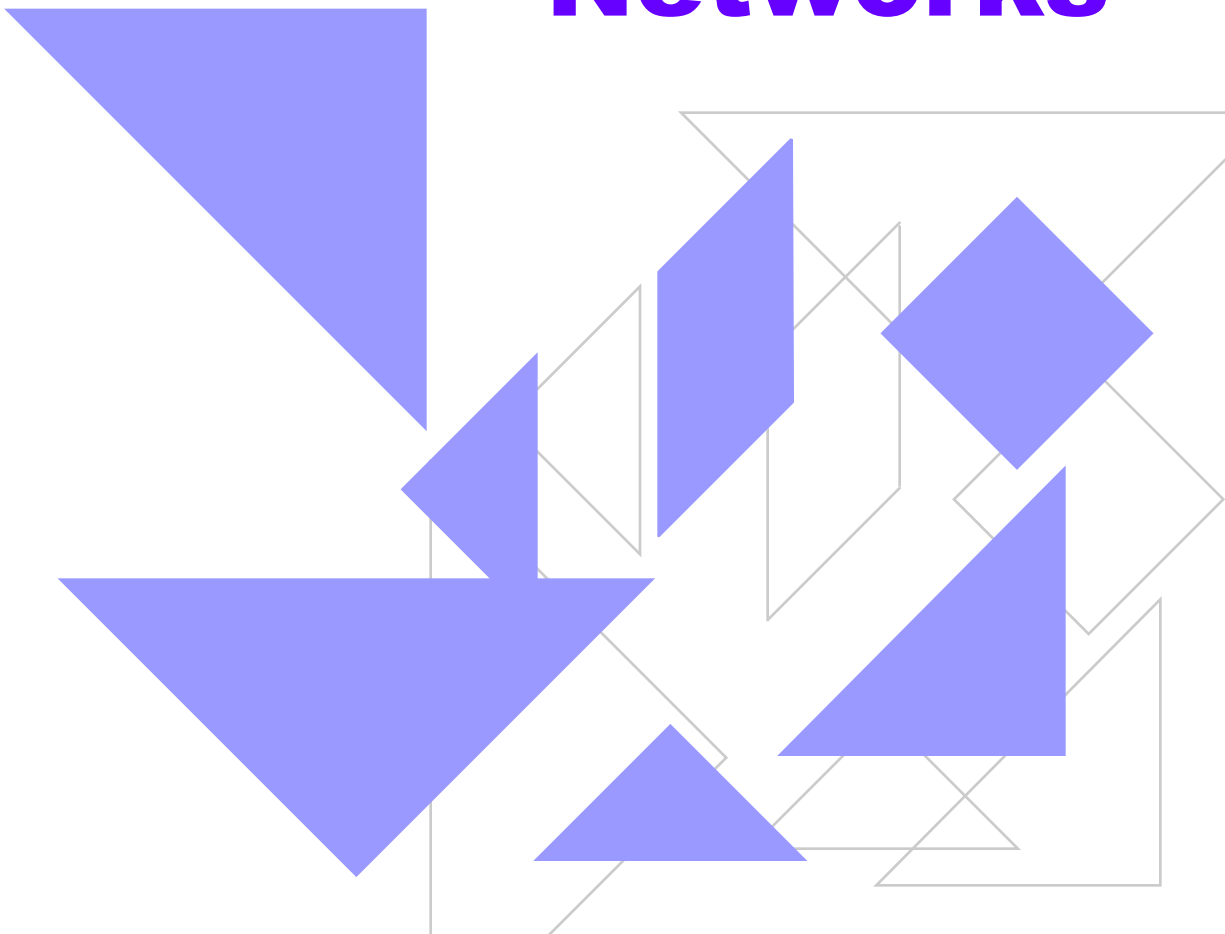
Security Analysis

- Based on our trust model, the risk of being compromised is largely reduced than the original routing protocol.
- Malicious nodes' trust value will be combined and propagated throughout the whole network. They will get large evidence penalties.
- The employment of trust model with the assistance of cryptographic authentication makes the network secure without sacrificing performance.
- The combination of different recommendations make the routing decision more reasonable and objective.

Flexibility and Scalability Analysis

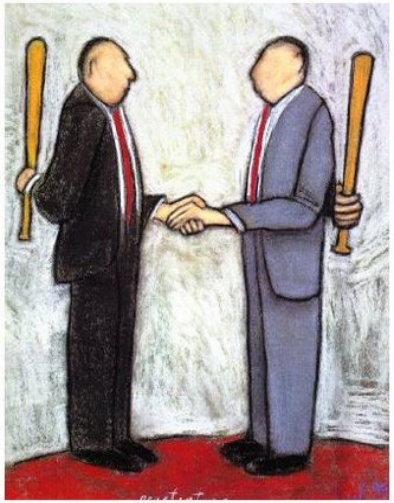
- Each node is given more flexibility to define its own opinion threshold.
- For high level security requirements, the threshold can be increased.
- For some non-critical applications, the threshold can be decreased.
- The protocol runs in a self-organized way, which remains the scalability of the network.

Part II: Coalitional Game Model for Security Issues of Wireless Networks



Motivations

- Why game theory for security issues of wireless networks?
  - Game theory studies competition or cooperation among a group of rational players.
  - Under the game rules, game theory provides threat or enforcement for players to achieve individual or social payoff maximization.
  - A wireless network is a network relying on cooperation among a group of nodes.
  - Malicious nodes show certain behavior patterns and must be rational enough.



Related Work

- In non-cooperative way
  - Form a two-player dynamic non-cooperative game with incomplete information.
  - The problem is that it does not make use of the cooperation property of MANET.
- In cooperative way
  - Nodes are clustered on the largest payoff defined by cooperation, reputation and quality of security.
  - The problem is that the formulation of reputation and quality of security is not convincing.

Our Goal and Challenge

- We will develop a cooperative game model for the security issues of wireless networks.
- The model can be applied to other types of wireless networks, e.g. wireless sensor networks.
- The game we employed is called a coalitional game.
- The key challenge is that how to define a proper payoff characteristic function for any coalition in the network which demonstrates the quality of security.

Contributions of Part II

- We define two characteristic functions, security and throughput, enforcing nodes in wireless networks to cooperate and form coalitions.
- The security characteristic function means the maximal security that a coalition can achieve. The throughput characteristic function means the maximal throughput and the most reliable traffic that a coalition can achieve.
- The payoff share is given by Shapley Value after proving the feasibility of this method.
- Coalition formation procedures are proposed with the integration to wireless routing protocols.

Game Overview

- The game is $\Gamma =< N, v >$, where
  - N is the set of nodes
  - v is the characteristic function that is associated with every nonempty subset S of N a real number v(S)
- The physical meaning of v(S) is the maximal payoff that a coalition can achieve.
- v(S) is the foundation of the coalition forming procedure and it confines the coalition to admit or exclude a node.
- Nodes that cannot join into any coalition are under very high suspicion of being malicious.

Security Characteristic Function

- Three design factors :
  - Support Rate
    - Nodes get more witnesses to testify for them when belonging to a coalition.
  - Cooperation Probability
    - Nodes in a coalition can take reference of other nodes' beliefs to get more reasonable and complete information.
  - Overlapping Distance
    - Nodes in closer distance will form a coalition so that they can provide more reliable link connection and decrease false positive alarm rate.

Three Factors

- Support Rate: Every node in a coalition S has |S|-1 number of witnesses:

$$T_t(S) = |S| - 1$$

- Cooperative Probability: Maximal average admitting probability among all members.

$$B_t(S) = \max_{j \in S} \left\{ \frac{\sum_{i \in I} p_{ij}}{|I|} \;\middle|\; I = \{i | i \in S, i \neq j, p_{ij} \neq 0\} \right\}$$

- Overlapping Distance: Maximal overlapping value among each of two nodes.

$$D_t(S) = \max_{i,j \in S} O_{ij}(t) \qquad O_{ij} = r_i + r_j - d_{ij}$$

Security Characteristic Function Definition

- Definition:

Definition (Security Characteristic Function)

The security characteristic function $v_t(S)$ is the linear combination of $T_t(S)$, $B_t(S)$ and $D_t(S)$:

$$v_t(S) = \begin{cases} 0, & |S| = 1 \\ \alpha T_t(S) + \beta B_t(S) + \gamma D_t(S), & |S| \geq 2 \end{cases}$$

where α, β and γ are weight parameters and $\alpha + \beta + \gamma = 1$.

- Based on $v_t(S)$, nodes can form coalitions to obtain its optimal payoff.

Coalition Formation Algorithm

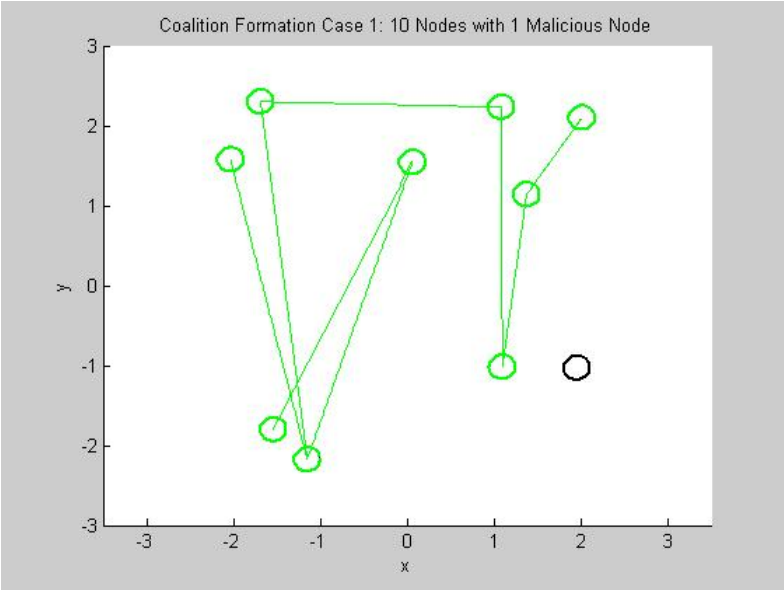
- The formation process is performed by rounds.
- At each round, each ungrouped node picks a target according to the highest security value of other ungrouped nodes, then publishes its choice for matching process.
- At each successful matching, new coalition is formed and merged with previous coalitions.
- The process will go on until there is no new coalition can be formed. The node that does not belong to any coalition would be under high suspicion.

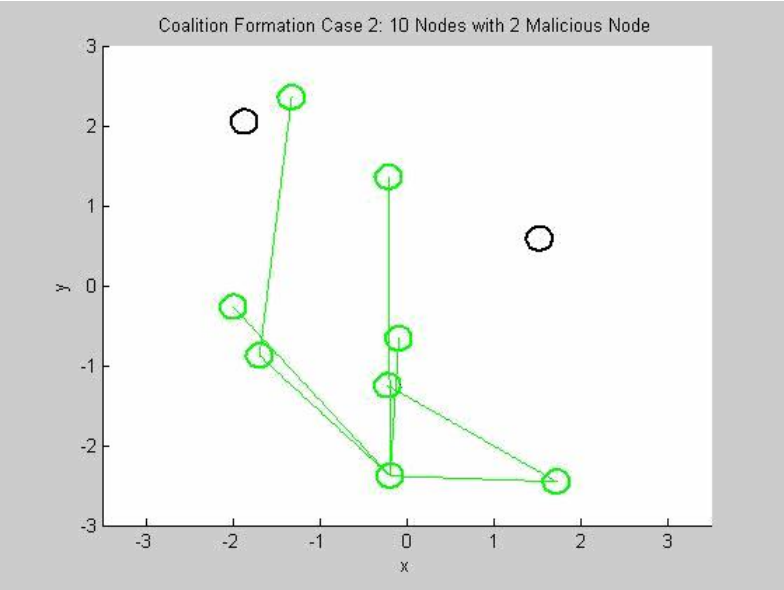
Simulation Setup

- 10 nodes with 1 or 2 malicious nodes randomly distributed.
- Initialize the support rate, cooperative probability, and overlapping distance for each entry in the routing table of the nodes.
- Run coalition formation algorithm round by round.
- Mark the nodes which do not form into any coalition.

Simulation Results

- Coalition formation demonstration
  - 10 nodes with 1 malicious node
  - 10 nodes with 2 malicious nodes





Throughput Characteristic Function

- The previous characteristic function does not consider the throughput performance when existing malicious nodes.
- We will design a throughput characteristic function to address this problem.
- The physical meaning of this function is the maximal throughput and the most reliable traffic that a coalition can achieve.
- It considers the trustworthiness and reliability of each routing path inside the coalition.

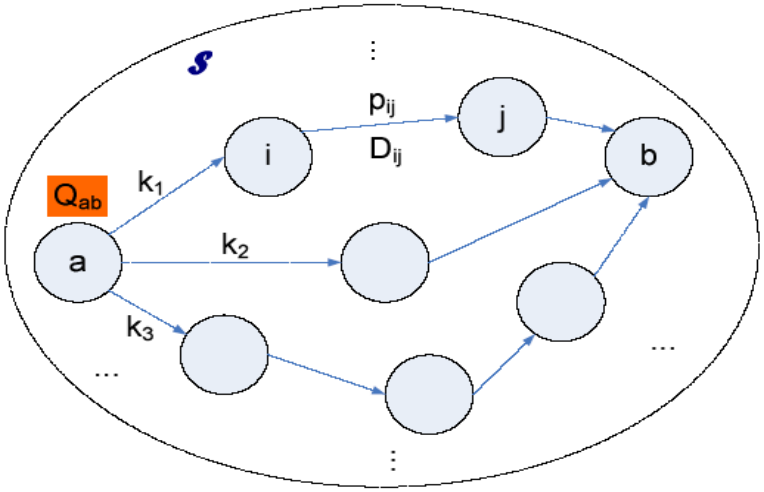
Formal Definition

Throughput Characteristic Function

The throughput characteristic value for any coalition S, $S \subseteq N$, is 0 where |S| = 1 and |S| = 0. For other coalition S where |S| >= 2, the throughput characteristic function v(S) is defined as:

$$v(S) = \frac{1}{\triangle t} \sum_{(a,b) \in SD, a,b \in S} Q_{ab} \cdot \max_{k \in P_{ab}(S)} \left\{ t(k) = \prod_{(i,j) \in k} \frac{p_{ij}}{D_{ij}^2} \right\}$$

- Q_{ab} is the required number of data packets transmitting between pair (a,b)
- $P_{ab}(S)$ is the set of routing paths inside coalition S which connect pair (a,b)
- $t(k)$ stands for the reliability evaluation of routing path k



Game Rules

- A node will join into a coalition only if it can get more payoff share than it stands individually.
- A node will deviate from the current coalition and join into another coalition only if it can get more payoff share there than that of here.
- A coalition will refuse to admit a node if the node cannot increase the total payoff of the coalition.
- A coalition will exclude a node if the node cannot benefit the coalition or even damage the total payoff of the coalition.
- Nodes who are finally failed to join into any coalition will be denied from the network.

Coalition Formation Procedure

- Introduce Gale-Shapley Deferred Acceptance Algorithm (DAA) to help nodes forming coalitions.
  - It was proposed to solve the stable marriage problem
  - It was proven that at the end of the algorithm, no one wants to switch partners to increase his/her happiness.
- The coalition formation procedure is conducted iteratively by all nodes.
- At each round, each source node will choose several preferences according to the reliability of each path t(k), then perform DAA algorithm to find a partner and admit it to the coalition.

Integration with Wireless Routing Protocols

- The model can be integrated with all kinds of routing protocols (AODV, DSR, DSDV, etc) in many types of wireless network (mobile ad hoc network, wireless sensor network, etc).
- Extend the original routing table of the protocol by adding coalition information.
- New control packet types are created for matching process.
- New dedicated timer is set up to control the iteration of coalition formation procedure.

Analysis by Game Theory (1)

- Speed of convergence and size of coalition:
  - In the coalition formation algorithm, at each round of formation, every coalition member tries to find a partner.
  - The coalition size is increased almost at an exponential time.
  - Therefore, the speed of coalition formation is fast which means the convergence time of formation is short.
  - And the size will keep growing until grand coalition is reached or all misbehavior nodes are identified.

Analysis by Game Theory (2)

- Non-emptiness of CORE:
  - The stable status of coalitional game is that no coalition can obtain a payoff that exceeds the sum of its members' current payoffs, which means no deviation is profitable for all its members.
  - The core is the set of imputation vectors which satisfies the following conditions:

1. $x(i) \geq v(i)$
2. $x(T) \geq v(T), \quad \forall T \in 2^N$
3. $x(N) = v(N), \ N$ is the player set

where $x(S) = \sum_{i \in S} x_i, \forall S \in 2^N$

Analysis by Game Theory (3)

- The relation between x(S) and v(S) has two situations.

  1. x(S) < v(S)
     - In this situation, the core is empty.
     - But our model still provides incentive for nodes to cooperate.
       - When |S| = 1, the node does not belong to any coalition. It cannot form a source-destination pair and consequently no throughput can be obtained.
       - While the payoff share in the coalition is always larger than 0.
     - The above reasons imply that the rational nodes always have incentive to cooperate with each other.

Analysis by Game Theory (4)

2. x(S) >= v(S)
   - If this situation can be reached, the core is nonempty.
   - The stable outcome will last for a certain time under certain conditions.
   - In the mobile ad hoc network, the current equilibrium may be destroyed and the network is enforced to re-form again.

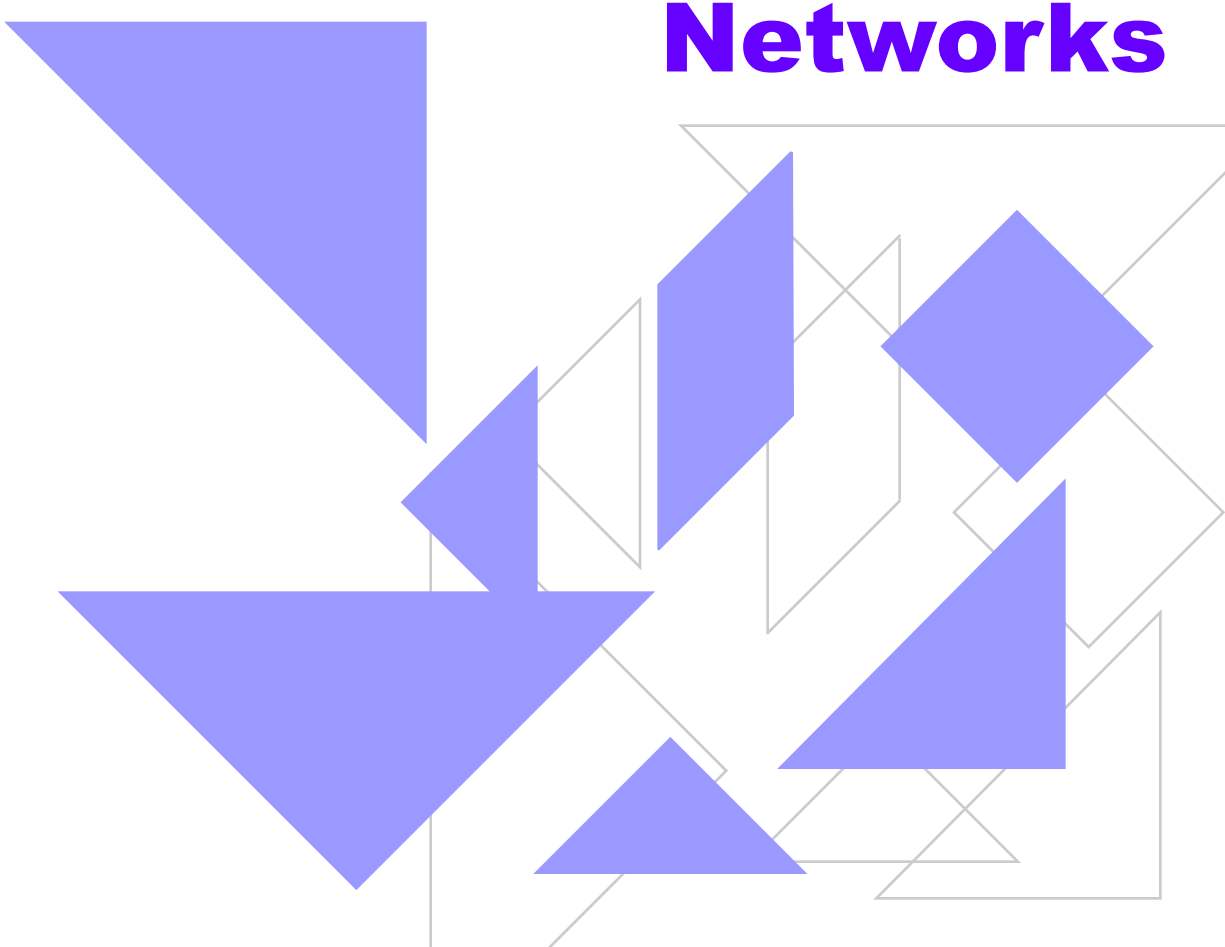
Analysis by Game Theory (5)

2. x(S) >= v(S) (con'd)
   - If that is the case, we can observe x(S) − v(S). The difference between them means how hard the core status will be destroyed.
   - The larger the difference, the low probability that the S will deviate. Then we can get the probability of the core keeps as follows:

$$p_{keep} = 1 - \prod_{S} [\ 1 - p_{deviate}(x(S) - v(S))\ ]$$

   where $p_{deviate}(x(S) - v(S)$ can be approximated as an exponential distribution for further investigation.

Part III: Incentive Routing Scheme and Coalitional Game Model for Selfishness Issues of Wireless Networks



Motivation (1)

- Incentives are needed to encourage cooperation among selfish nodes in wireless networks.

- Monetary Incentive Scheme
  - Nodes get payments for forwarding data packets based on their declared costs.
  - The problem is how to avoid cost cheating.
- Reputation Incentive System
  - Nodes are punished based on their bad reputations.
  - The challenge is how to combine and propagate reputations.

Motivation (2)

- Game Theoretic Formulation
  - The above schemes are often analyzed by non-cooperative game methods.
  - The problem is that they do not make use of the cooperation nature of wireless networks.
  - No effective coalitional model has been proposed.
- Our goal
  - Design an incentive routing and forwarding scheme that combines payment and reputation together, and analyze the scheme with a coalitional game model.

Challenges

1. How to obtain a combined and globalized reputation value.
2. How to design the payment algorithm that integrates reputation values.
3. How to write the value function of the game which can represent the collective payoff of the coalition.
4. How to find the stable solution of the game.

Contributions of Part III

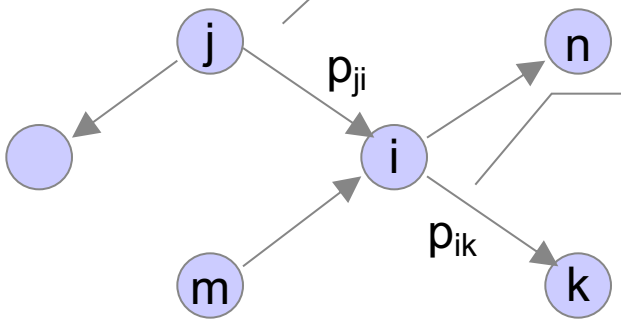
- First, we design an incentive routing and forwarding scheme that integrates reputation information into a payment mechanism, which can increase the throughput as well as the security of the network.
- Second, we introduce a heat diffusion model to combine the direct and indirect reputations together and propagate them from locally to globally.
- Third, unlike others, we model this incentive scheme using a coalitional game method. A characteristic value function of the coalition is designed and we prove that this game has a core solution.

Heat Diffusion Model

- We employ a heat diffusion model to fulfill the first challenge.
- Why heat diffusion?
  - In heat diffusion, heat comes from all incoming links of a node and diffuses out to its successors through some media.
  - If heat is diffused on a weighted graph, then the amount of heat that each node obtains will reflect the underlying graph structures.
  - If heat is diffused on a weighted reputation graph, then the process of heat diffusion can be deemed as a combination and propagation of reputations.

Heat Diffusion Example

- Example



$$\lambda p_{ji} f_j(t) \Delta t / l_j$$

$$\lambda p_{ik} f_i(t) \Delta t / l_i$$

p_{ji}: weight in the reputation graph

λ : thermal conductivity

l_j : number of successors of j

- The heat difference at node i:

$$f_i(t+\Delta t) - f_i(t) = \lambda \left(\sum_{j:(j,i)\in E} \frac{p_{ji}}{l_j} f_j(t) - \mu_i \sum_{k:(i,k)\in E} \frac{p_{ik}}{l_i} f_i(t) \right) \Delta t$$

Heat Diffusion Formulation

- The heat difference at node *i* in a matrix form:

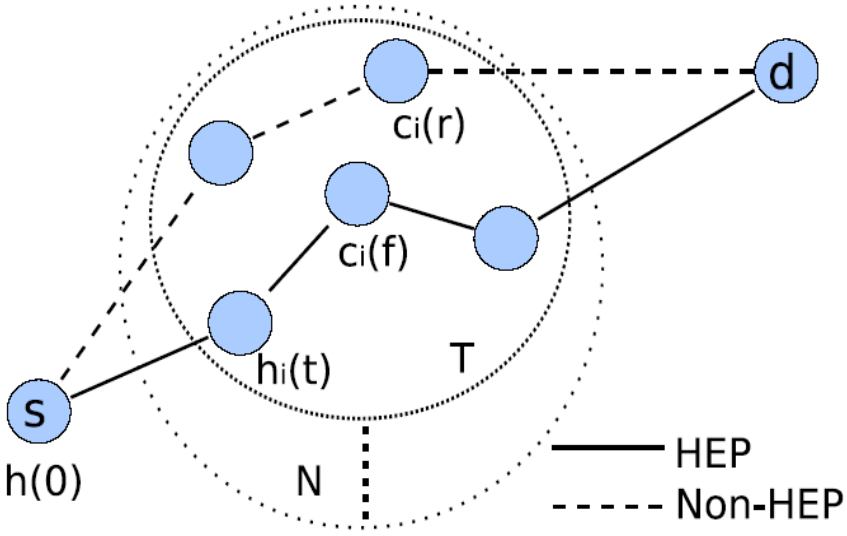
$$\boldsymbol{f}(t) = e^{\lambda t \boldsymbol{H}} \boldsymbol{f}(0)$$

$$H_{ij} = \begin{cases} p_{ji}/l_j, & (j,i) \in E, \\ -(\mu_i/l_i) \sum_{k:(i,k)\in E} p_{ik}, & i = j, \\ 0, & otherwise. \end{cases}$$

- Based on the reputation graph, the amount of heat of a node reflects a combined reputation belief from the viewpoint of the heat source.

Incentive Routing and Forwarding Scheme

- Basic Notations
  - Heat diffuses on this reputation graph G
  - s is source, d is destination
  - Initially, heat of s is f(0), others' heat is 0. The initial balance of s is h(0).
  - Costs for forwarding and routing are $c_i(f)$ and $c_i(r)$
  - Intermediate nodes get $f_i(t)$ during heat diffusion
  - s pays $h_i(t)$ proportional to $f_i(t)$ to intermediate nodes
  - s discovers a route called Highest Effective Path (HEP)



Incentive Routing Algorithm

- First, each node i claims its forwarding cost to s.
- Then s performs the heat diffusion process.
- Instead of choosing the lowest cost path (LCP), s chooses a highest effective path (HEP): $f_i(t) \geq \theta$ with lowest cost.
- After data transmission, s pays $h_i(t)$ to each node according to $f_i(t)$.
- Adjust heat threshold θ.
- The reputation graph then is updated in the neighborhood.

How Is Incentive Achieved?

- Nodes are paid by their reputations, not by their claimed cost, which can prevent cost cheating.
- Nodes need to be cooperative to get high reputations so that more payments can be awarded.
- Selfish nodes' reputation would be decreased locally and be globally reflected in the heat diffusion process, so that less payments can be paid to them.
- Forwarding data packets will get higher reputation than forwarding routing packets.
- To transmit their own packets, nodes need to pay to other nodes, so that they'd better be always cooperative and earn enough utilities.

Our Coalitional Game

- Utility characteristic function v(T):
  - Takes into account the amount of payment and the costs of nodes in T.
  - Each path in the coalition contributes a payoff.

$$w_P(T) = \sum_{i \in T} h_i - \sum_{i \in P} c_i(f) - \sum_{i \notin P} c_i(r)$$

  - The path contributing the maximal payoff is HEP_T.
  - We take this maximal payoff as the value of our function, which means the maximal collective utility that T can guarantee.

$$v(T) = \max_{P \subseteq T} \left(\sum_{i \in T} h_i - \sum_{i \in P} c_i(f) - \sum_{i \notin P} c_i(r) \right)$$

Utility Characteristic Function

- Re-write the function with HEP_T

Definition: Utility Characteristic Function

The value of any coalition is 0 when there is no path between s and d inside coalition T. Otherwise,

$$v(T) = \sum_{i \in T} h_i - \sum_{i \in HEP_T} c_i(f) - \sum_{i \notin HEP_T} c_i(r)$$

Non-emptiness of the Core

- Recall the three conditions of the core:

1. $x(i) \geq v(i)$
2. $x(T) \geq v(T), \quad \forall T \in 2^N$
3. $x(N) = v(N), \ N$ is the player set

where x(i) is the payoff share of node i in the grand coalition, and

$$x(T) = \sum_{i \in T} x(i)$$

- The core is possibly empty in different games.

Core Solution

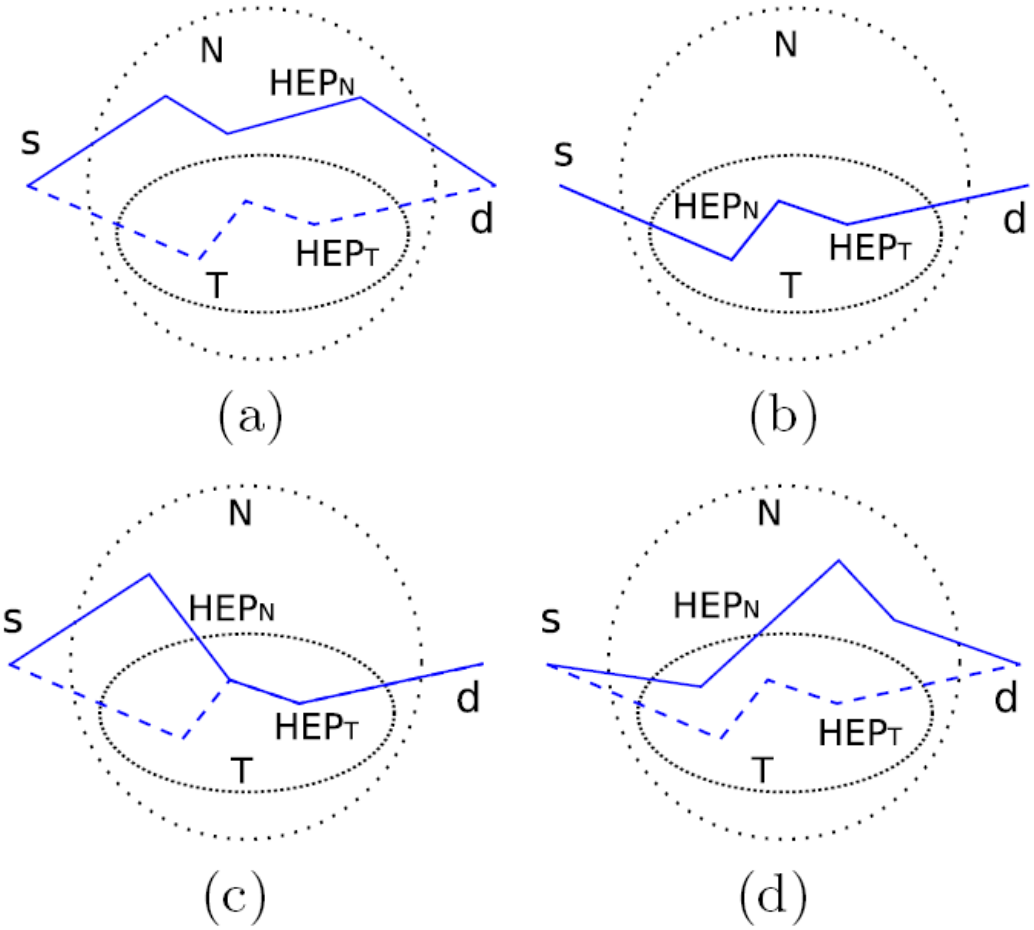
Theorem: Core Solution

Under the condition of $h_i \geq c_i(f)$ for each node i, the following payoff profile x is in the core of the coalitional game where

$$x(i) = \begin{cases} h_i - c_i(f), & i \in HEP_N \\ h_i - c_i(r), & i \notin HEP_N \end{cases}$$

Proof of Core Solution

- x(i)≥v(i), x(N)=v(N) are straightforward.
- To prove x(T)≥v(T):
  - In total there are four situations of HEP in grand coalition N and in any coalition T.
  - Calculate x(T) and v(T) for each situation, compare them, and get proved.

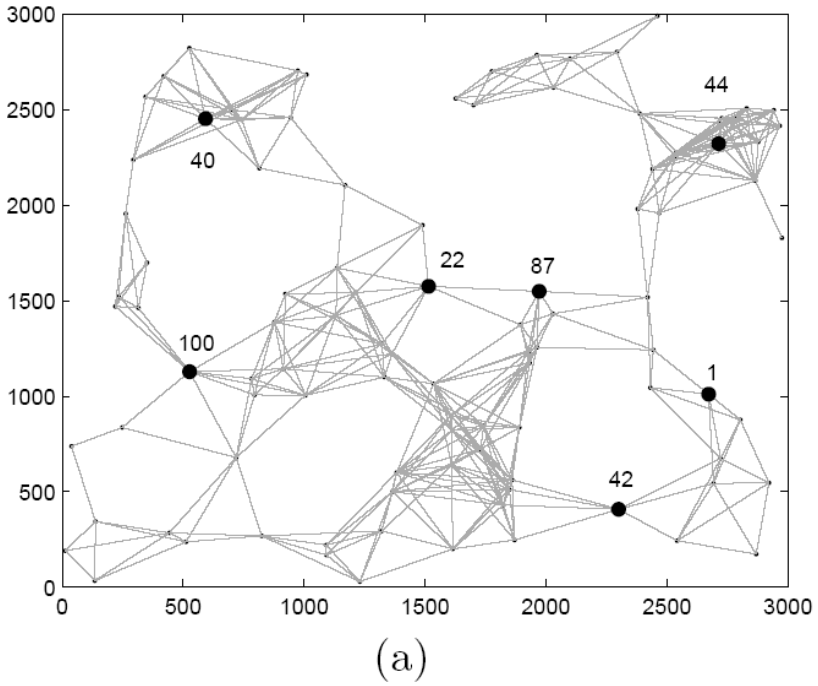


Evaluation Setup

- Each node has an initial balance of 100.
- Each directed link has a local reputation weight.
- At each round a source-destination (s, d) pair is randomly selected.
- s performs the incentive routing and forwarding algorithm to discover HEP to d, and pays to the intermediate nodes.
- The thermal conductivity λ is set to 1.
- The evaluation runs for 1000 seconds.

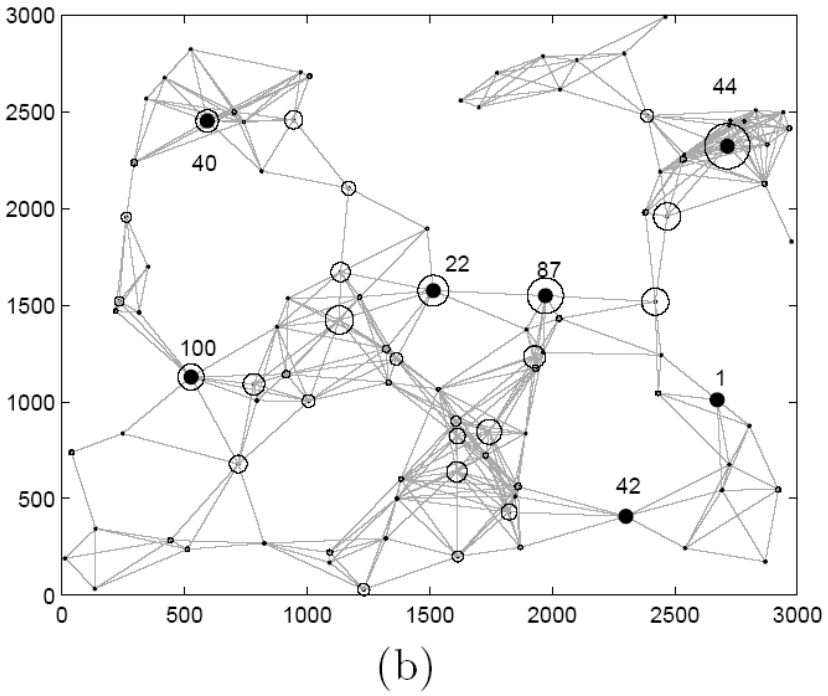
Network Topology

- 100 nodes in an area of 3000 by 3000 meters.
- The radio range is 422.757 meters.
- Some representative nodes shown in black dots.



Overview of Cumulative Utilities

- A circle means the cumulative utility of the node.
- The larger the circle is, the more utility the node has.
- Nodes in the high density area have large circles around them (like node 44).
- Nodes in the sparse area have indistinctive circles.



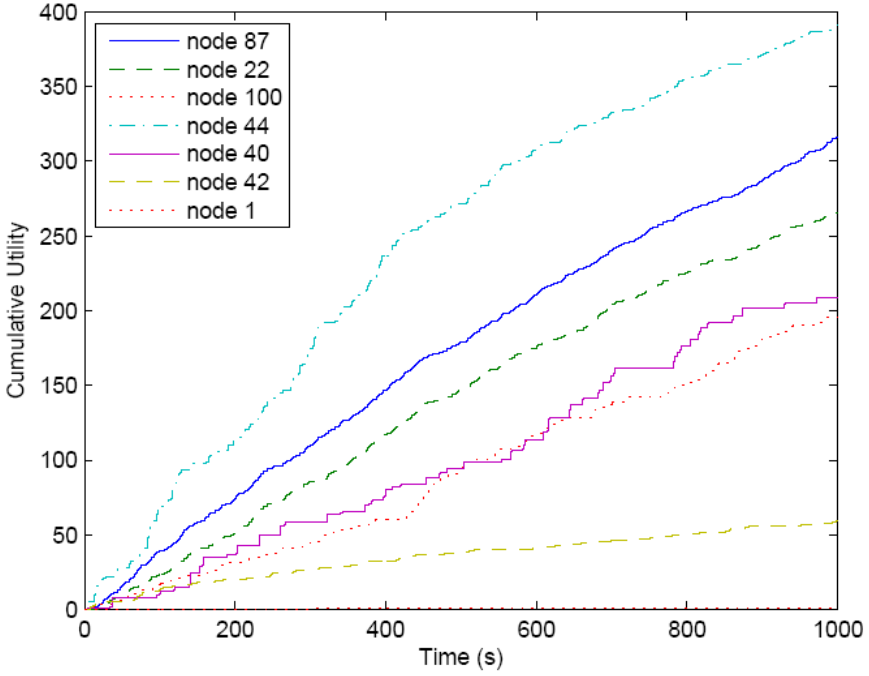
(b)

Cumulative Utilities of Selected Nodes

- The evaluation starts from the core of the coalitional game:

  Nodes are cooperative.

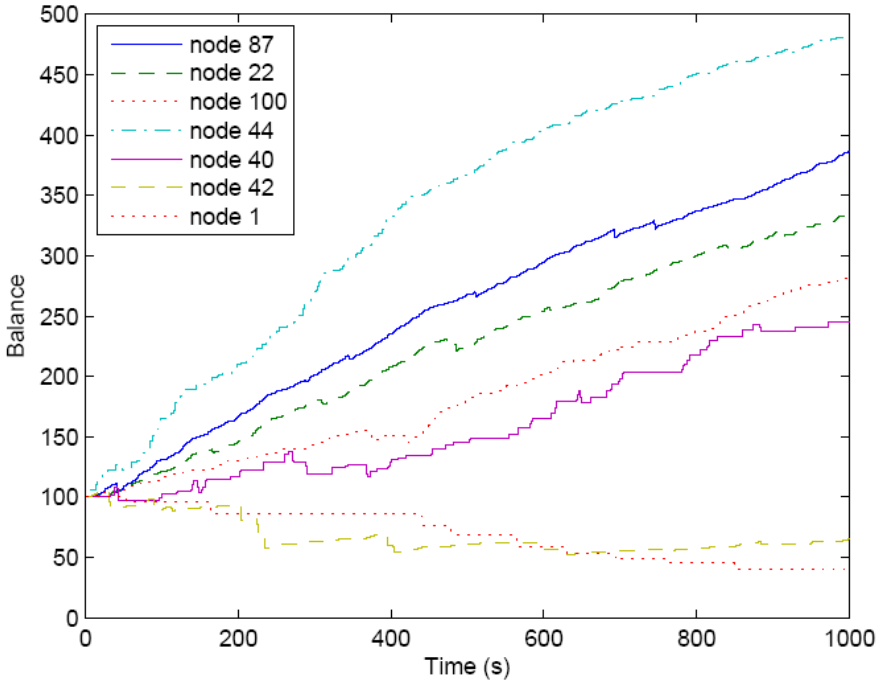
- The cumulative utilities are increased steadily.



(a)

Balance of Selected Nodes

- Most of nodes' balance increases steadily.
- Some nodes in sparse area (like node 42 and node 1) have less chance to earn utilities to pay for their own data transmission.
- In summary, the scheme is incentive for nodes to be cooperative.



(b)

Future Work

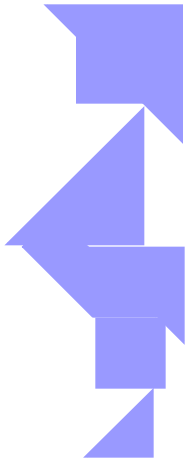
- Apply subjective logic to other applications, such as social computing, information retrieval and so on.
- Study other forms of cooperative games to better formulate the situations of wireless networks.
- Design more effective payment schemes to encourage cooperation as well as prevent cost cheating.

Conclusions

- We, for the first time, introduce the idea of “trust model” into the design of secure routing protocols of MANET, which largely reduce the performance overhead than traditional cryptographic solutions.
- We propose a novel coalitional game model for the formulation of security issues in wireless networks.
- We also present an incentive routing and forwarding scheme for the selfishness issues of wireless networks based on heat diffusion model and analyze the scheme by a coalitional game model.

Q & A

Thank you!

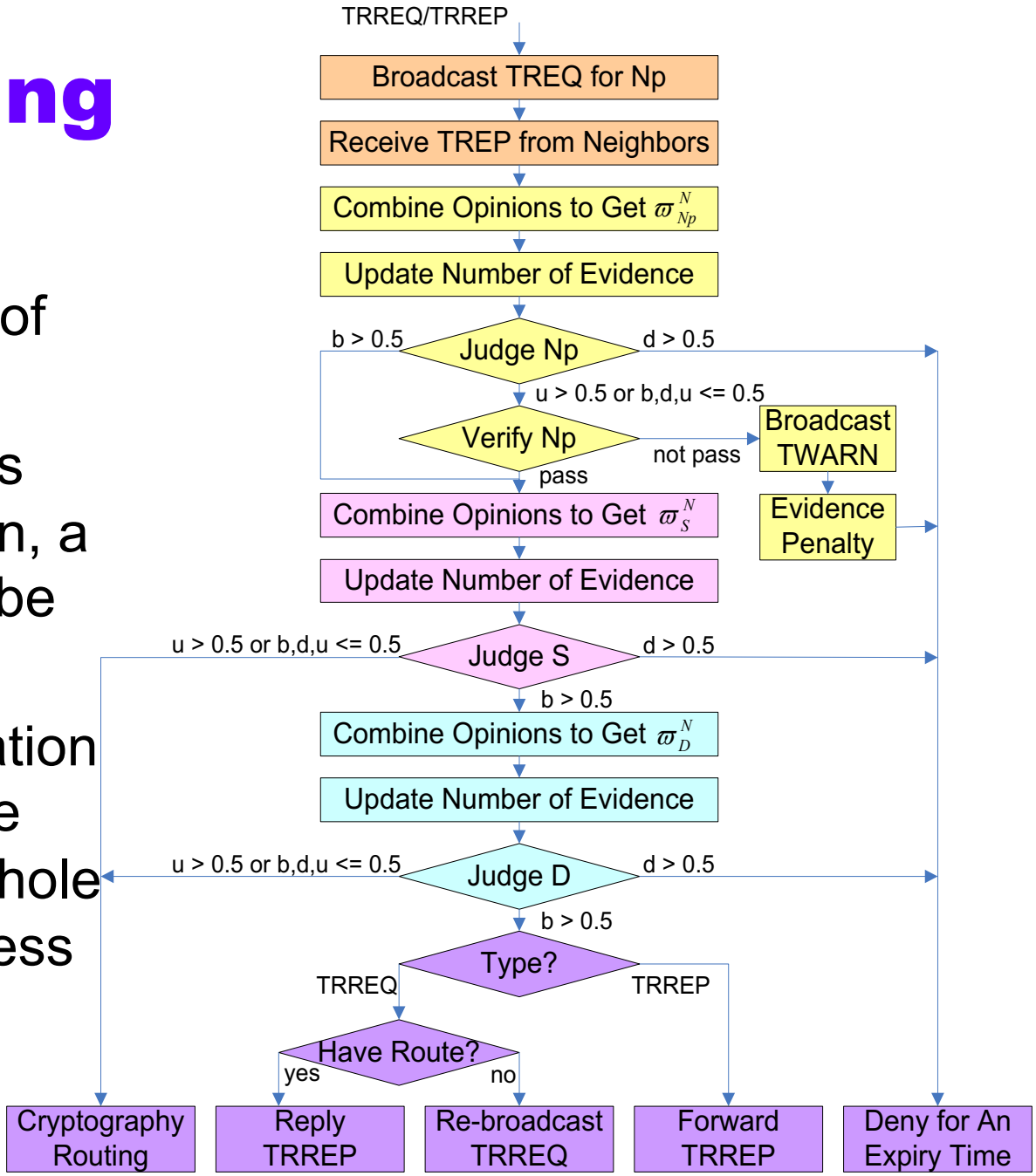


Appendix A: Related Trust Models

- Direct and recommendation trust model
  - Represent trust by one continuous value
  - Basis of many other trust models
- Dempster-Shafer theory trust model
  - Represent trust by upper and lower bound pair
  - Represent trust relationship by trust matrix
  - Combine two matrices using Dempster-Shafer theory
- Subjective logic trust model
  - Represent trust by *opinion*
  - *Opinion* has belief, disbelief, and uncertainty values
  - Combine opinions using two subjective logic operators

Appendix B: Trusted Routing Discovery

- Np is the predecessor of the packet.
- If the predecessor does not pass the verification, a TWARN message will be broadcasted.
- If the source or destination node does not pass the verification, then the whole routing discovery process will use cryptographic method.



Appendix C: Trust Evaluation with Enhanced Subjective Logic

- Most trust models lose intuitiveness or disobey common human belief in some cases.
- Subjective logic also introduces counter-intuitiveness:
  - The value of uncertainty is only related to the number of positive and negative events, while human usually expect the result according to the ratio of positive and negative events.
  - The mapping function of u is not reasonable in some cases.
- Next, we are going to propose an enhanced subjective logic trust model.

Flaws of Subjective Logic

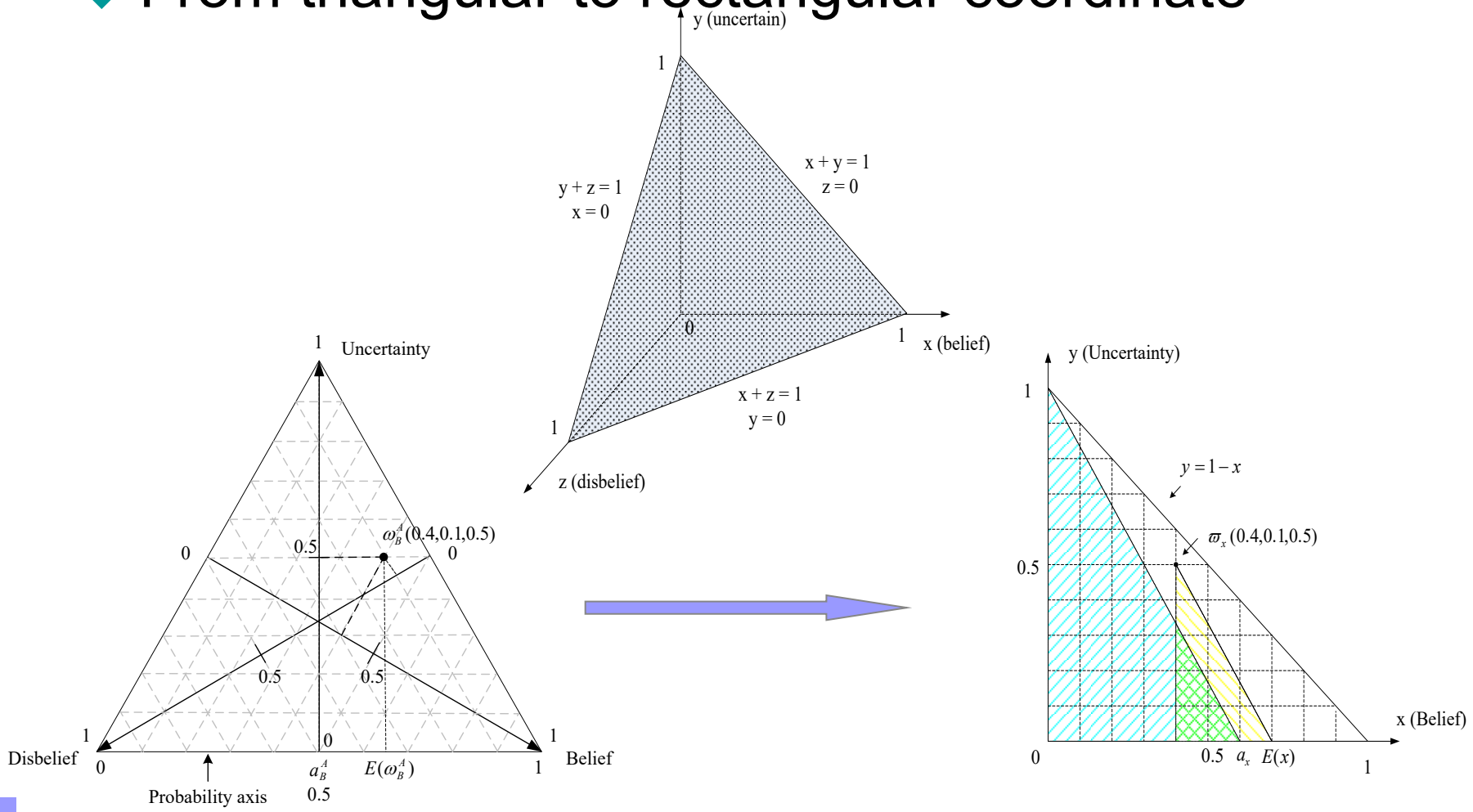
- Let's look at the mapping equation of `u`:

$$u_B^A = \frac{2}{p+n+2}$$

  - When the number of `p` and `n` are nearly equal and both large enough, the value of `u` will be limited to `0`, which means total certainty.
  - While from common human belief point of view, the uncertainty in this case should be very high.

Illustrating Opinion in a New Way

- From triangular to rectangular coordinate



Re-Distribution of Opinions

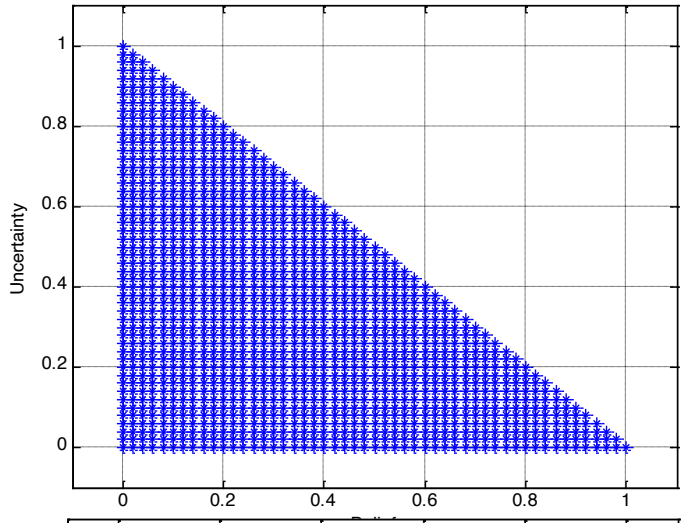
- In the case of `p` and `n` are large and nearly equal, the opinion is around `(0.5,0.5,0)`.
- We would like to re-distribute opinions to other values.
- Possible solutions to re-calculate u:

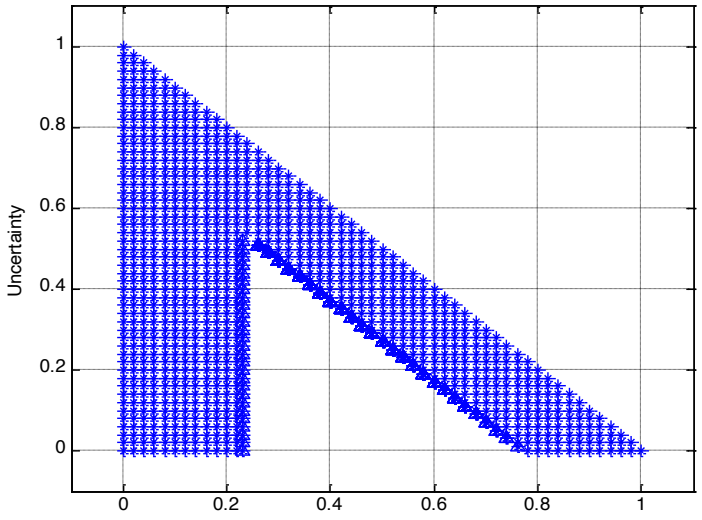
1. $$\begin{cases} b' = b, \quad u' = 1 - b - \varepsilon, & \text{if } b > d \\ b' = \varepsilon, \quad u' = u, & \text{if } b < d \end{cases}$$

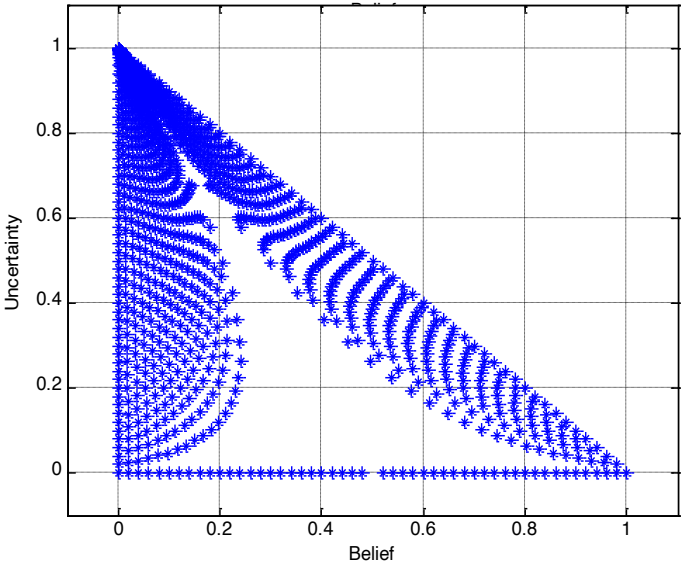
   where ε is the allowable uncertainty value

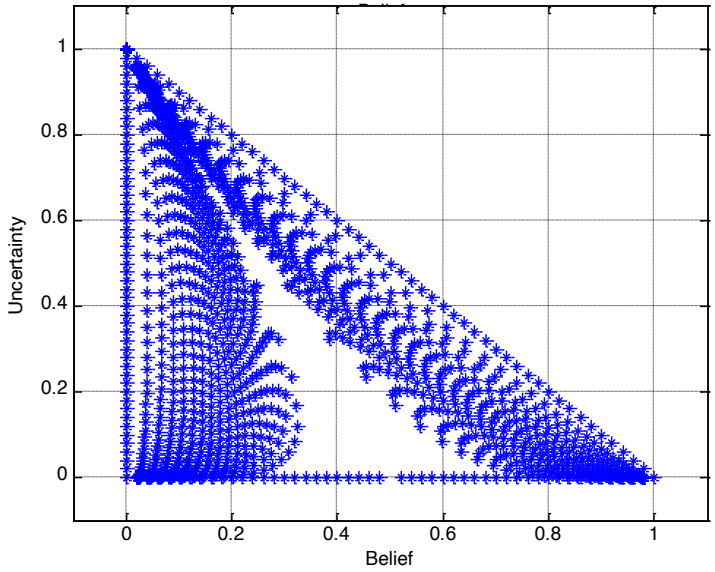
2. $$u' = u^{|b-d|}$$
3. $$u' = u^{\log(b/d)}$$

Possible Re-Distribution Figures









Possible Re-Distribution Functions

- After re-calculating `u`, we adjust `b` and `d` according the ratio of original `b` and `d` to meet the equation of `b+d+u=1`.
- Observing these figures we can intuitively get that the last one pushes the opinions more evenly and more consistently with the original opinion distribution.
- So, we will employ the last function in simulation to justify its feasibility and validity.

Simulation Setup

- Initial node model:
  - We put `100` nodes randomly in a `100*100` square.
  - Each node has `8` neighbors in average.
  - When the network is "born", nodes are assigned to be bad nodes or good nodes.
  - We define a percentage of bad nodes `m`, e.g. `m=30%`
  - Nodes in neighborhood knows if their neighbors are good or bad.
  - We select a good node as delegate to evaluate the global indirect trust.

Simulation Setup

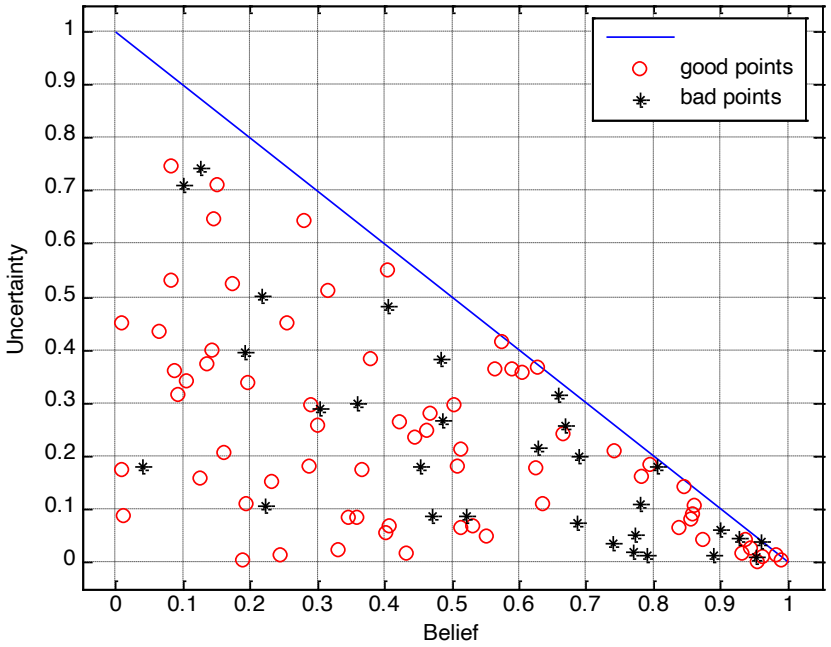
- Opinion assignment model. Initially
  - Bad nodes have best opinion for their neighboring bad nodes, e.g. `(0.9,0.05,0.05)`.
  - Bad nodes have worst opinion for their neighboring good nodes, e.g. `(0.05,0.9,0.05)`.
  - Good nodes adjust their direct opinions to their neighbors according to Beta distribution around low belief and high uncertainty.
- The initial opinions from delegated good node to all other nodes has high uncertainty.
- We want to make the uncertainty lower and lower, which means that the node will have more and more definite opinions about other nodes' trustworthiness.

Simulation Rounds

- At each simulation round, four things happen:
  1. Each node performs an interaction with its neighbors. For bad node neighbors, negative events will increase by a count, and for good node neighbors, positive events will increase by a count.
  2. According to the new evidence events, update the opinions in neighborhood using mapping function.
  3. Push the opinions using the re-distribution function.
  4. Combine all the opinions from the selected good nodes to all other nodes through different paths using the discounting and consensus algorithm.

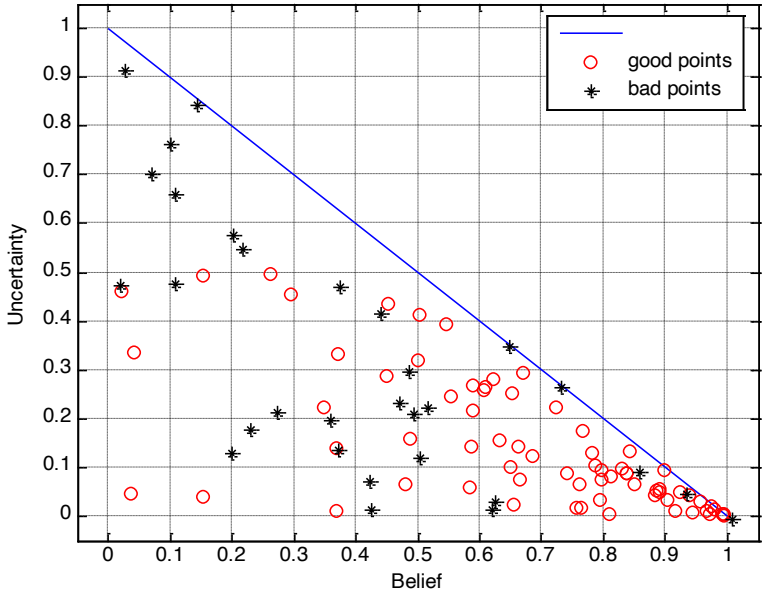
Simulation Results

- Initial opinion distribution

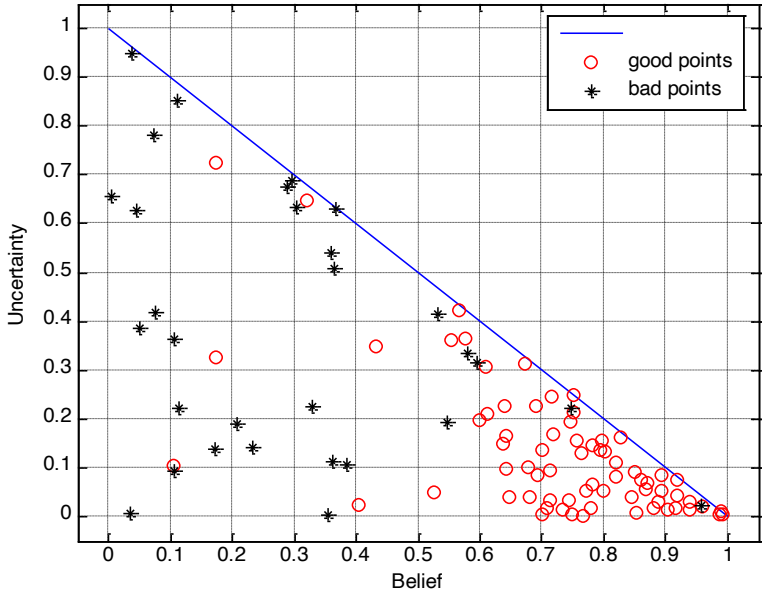


Simulate Results

- After 30 rounds



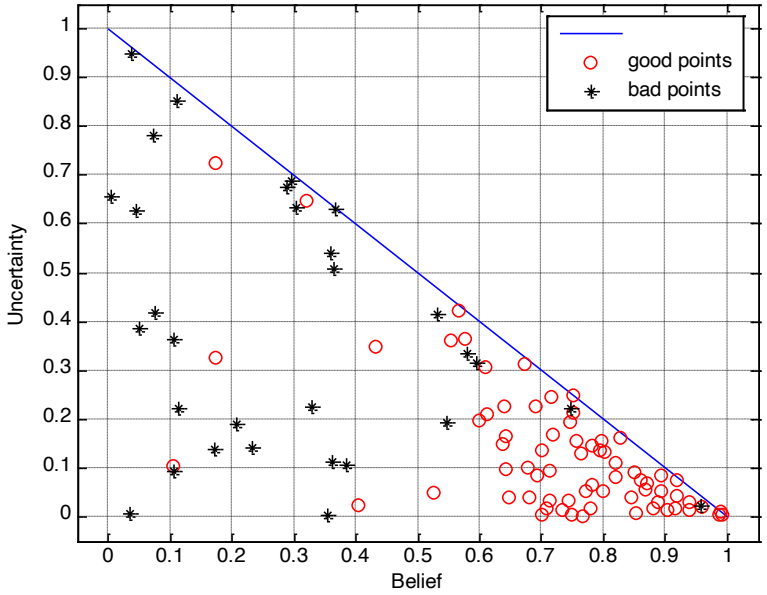
Subjective Logic Distribution

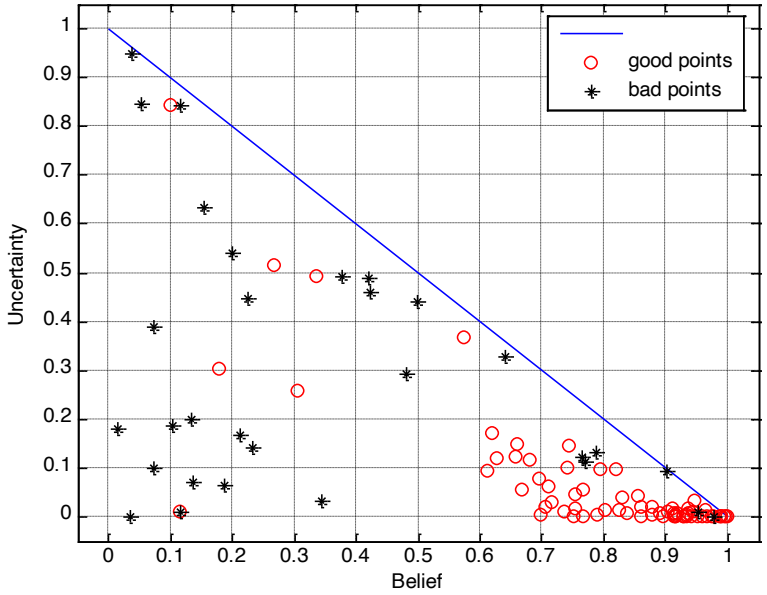


Improved Opinion Distribution

Simulation Result

- After 30+1 rounds





Subjective Logic Distribution

Improved Opinion Distribution

- We can observe from the results that the re-distributed opinions converg better than the original subjective logic opinions after 30 rounds.

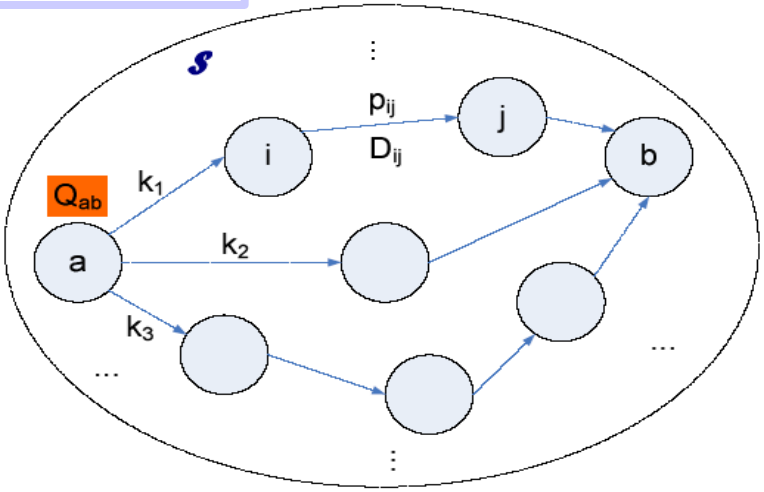
Appendix D: Throughput Characteristic Function

Throughput Characteristic Function

The throughput characteristic value for any coalition S, $S \subseteq N$, is 0 where |S| = 1 and |S| = 0. For other coalition S where |S| >= 2, the throughput characteristic function v(S) is defined as:

$$v(S) = \frac{1}{\triangle t} \sum_{(a,b) \in SD, a,b \in S} Q_{ab} \cdot \max_{k \in P_{ab}(S)} \left\{ t(k) = \prod_{(i,j) \in k} \frac{p_{ij}}{D_{ij}^2} \right\}$$

- Q_{ab} is the required number of data packets transmitting between pair (*a,b*)
- $P_{ab}(S)$ is the set of routing paths inside coalition *S* which connect pair (*a,b*)
- $t(k)$ stands for the reliability evaluation of routing path *k*



Throughput Characteristic Function (1)

where

1. Δt is a certain time interval
2. *SD* = {(*a*,*b*) | (*a*,*b*) *is a source - destination pair }*
3. Q_{ab} is the required number of data packets transmitting between pair (*a*,*b*)
4. $P_{ab}(S)$ is the set of routing paths inside coalition *S* which connect pair (*a*,*b*)
5. $k \in P_{ab}(S)$ is one of the path in $P_{ab}(S)$ and *k* = {(i, *j*) | *i, j are the adjacent nodes on the same routing path }*
6. *t*(*k*) stands for the reliability evaluation of routing path *k*
7. p_{ij} is the trustworthiness of path (*i, j*)
8. D_{ij} is the distance between node *i* and *j* □

Throughput Characteristic Function (2)

P(S):

- For each coalition S, we generate a weighted directed graph G(S), where
  - Vertexes are nodes inside the coalition
  - Edges represent routing direction between two nodes
  - Weights are trustworthiness of this edge
- Perform routing discovery procedure on the graph and discover the first several possible routing paths P(S) for each source-destination pair inside S.
- The number of routing paths is related to |S|. When |S| increases, more possible paths can be found and more reliable routing and forwarding transmission can be obtained.

Throughput Characteristic Function (3)

t(k):

- For every possible routing path $k \in P_{ab}(S)$ between source-destination pair, we get a trustworthiness evaluation t(k).

- The maximal value of t(k) over all k indicates the maximal payoff that the source-destination pair can benefit from the coalition.

Throughput Characteristic Function (4)

pij : Trustworthiness of routing path from i to j is obtained from two ways:

- Direct experience: Fraction of observed successful transmission times by all the transmission times between i and j .

$$p = \frac{u_{succ}}{u_{all}}$$

- Indirect recommendation: Comes from node i's neighbors. Each neighbor of i returns probability opinions about both i and j , then i combines them together.

$$p' = \frac{\sum_{l \in NB_i} p_{il} p_{li} p_{lj}}{|NB_i|}$$

Throughput Characteristic Function (5)

- Indirect Recommendation:
  - Note that we consider not only neighbors' recommendations towards j but also towards i , which represents the opinions towards the routing path from i to j .
  - Multiplying by node i 's own evaluation to its neighbors, we then get the more believable indirect probability p' of communication from i to j .
- Direct experience and indirect recommendation have different weights, we then present the combined probability like this:

$$p_{ij} = \alpha p + (1-\alpha)p'$$

$$= \alpha \frac{u_{succ}}{u_{all}} + (1-\alpha)\frac{\sum_{l \in NB_i} p_{il}p_{li}p_{lj}}{|NB_i|}$$

Appendix E: Payoff Allocation Inside the Coalition (1)

- How to fairly distribute the gains among all the coalition members
  - Some members contribute more than others
  - Shapley value is applicable to this problem if v(S) satisfies:

    1. $v(\phi) = 0$
    2. $v(S \cup T) \geq v(S) + v(T)$

    whenever S and T are disjoint subsets of N.
- The share amount that player i can gets is:

$$x_i(v) = \sum_{S \subseteq N \setminus \{i\}} \frac{|S|!(n - |S| - 1)!}{n!} (v(S \cup \{i\}) - v(S))$$

Payoff Allocation Inside the Coalition (2)

Theorem

Shapley Value method is applicable to the payoff allocation inside coalitions given our proposed throughput characteristic function v(s).

Proof:

1. From definition of v(S), we get v(Φ) = 0.
2. On the basis of v(S), we have:

$$v(S) = \frac{1}{\triangle t} \sum_{(a,b) \in SD, a,b \in S} Q_{ab} \cdot \max_{k \in P_{ab}(S)} \left\{ t(k) = \prod_{(i,j) \in k} \frac{p_{ij}}{D_{ij}^2} \right\}$$

$$v(T) = \frac{1}{\triangle t} \sum_{(a,b) \in SD, a,b \in T} Q_{ab} \cdot \max_{k \in P_{ab}(T)} \left\{ t(k) = \prod_{(i,j) \in k} \frac{p_{ij}}{D_{ij}^2} \right\}$$

Payoff Allocation Inside the Coalition (3)

$$\Longrightarrow \quad v(S \cup T) =$$

$$\frac{1}{\triangle t} \sum_{(a,b) \in SD, a,b \in S \cup T} Q_{ab} \cdot \max_{k \in P_{ab}(S \cup T)} \left\{ t(k) = \prod_{(i,j) \in k} \frac{p_{ij}}{D_{ij}^2} \right\}$$

- The larger the coalition becomes, the more number of possible routing paths can be discovered. Accordingly, the maximal reliability increases when obtained from a larger set. So we get $v(S \cup T) \geq v(S) + v(T)$. $\square$

Appendix F: Attacks to MANET

Attack Method	Motivation/Result	Influence to Security Services
Eavesdropping	Obtain contents of messages	Loss of Confidentiality
Masquerading (e.g. Rushing attack)	Impersonate good nodes /Routing Redirection /Routing table poisoning /Routing Loop, etc.	Loss of Authenticity
Modification (e.g. Man-in-Middle)	Make a node denial of service /Obtain keys, etc.	Loss of Integrity
Tunneling (e.g. Wormhole)	Attract traffic /Routing Redirection	Loss of Confidentiality and Availability
Flooding	Denial of Service	Loss of Availability
Dropping	Destroy normal routing progress	Loss of Non-reputation and Availability
Replaying/Delaying	Destroy normal routing progress /Destroy normal data transmission	Loss of Access Control and Integrity

Appendix G: An Example of Trust Combination

- Node A has three neighbors N_1, N_2, N_3. We have:

$$\omega_{N_1}^{A} = (0.90, 0.00, 0.10) \qquad \omega_{B}^{N_1} = (0.90, 0.00, 0.10)$$

$$\omega_{N_2}^{A} = (0.00, 0.90, 0.10) \qquad \omega_{B}^{N_2} = (0.90, 0.00, 0.10)$$

$$\omega_{N_3}^{A} = (0.10, 0.00, 0.90) \qquad \omega_{B}^{N_3} = (0.90, 0.00, 0.10)$$

- First: Discounting Combination

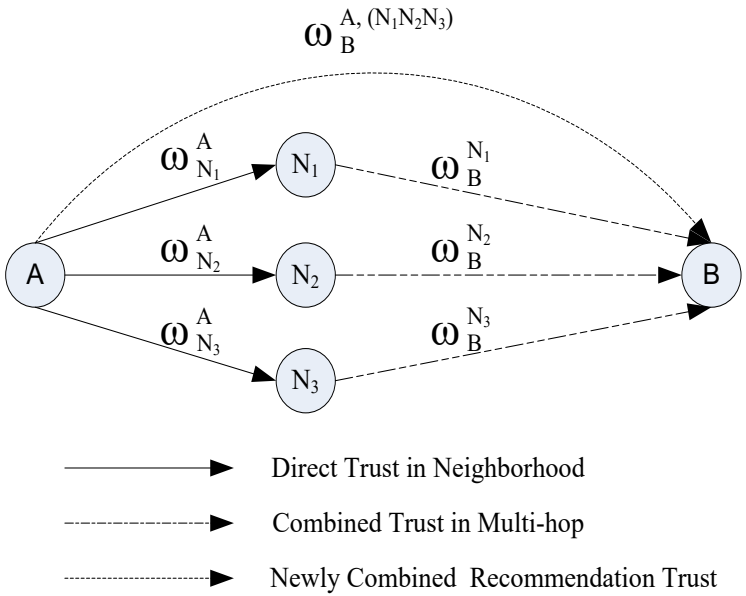
$$\omega_{B}^{A,N_1} = (0.81, 0.00, 0.19)$$

$$\omega_{B}^{A,N_2} = (0.00, 0.00, 1.00)$$

$$\omega_{B}^{A,N_3} = (0.09, 0.00, 0.91)$$

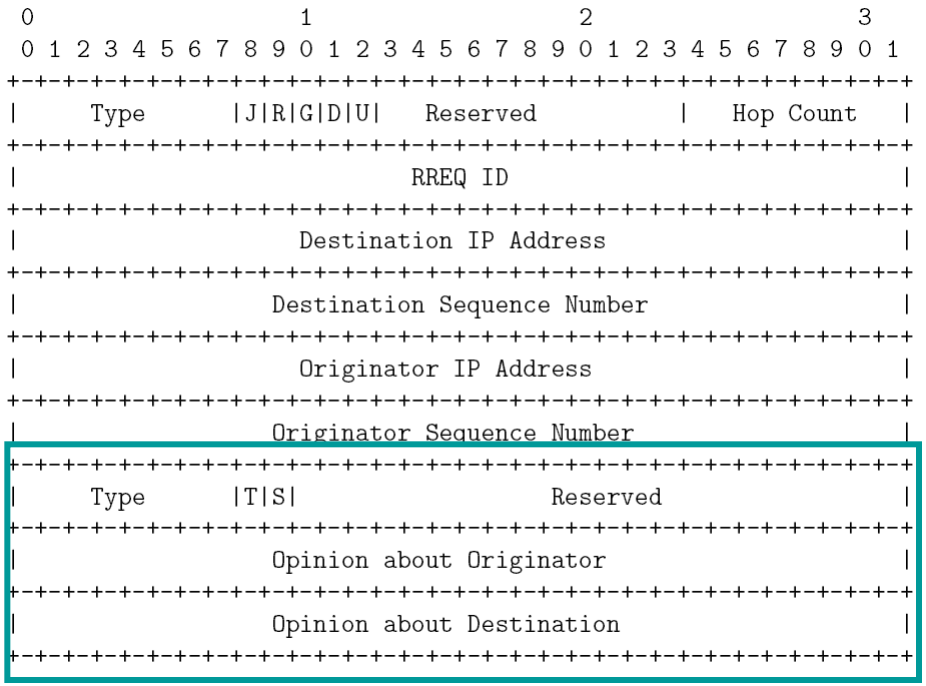
- Second: Consensus Combination

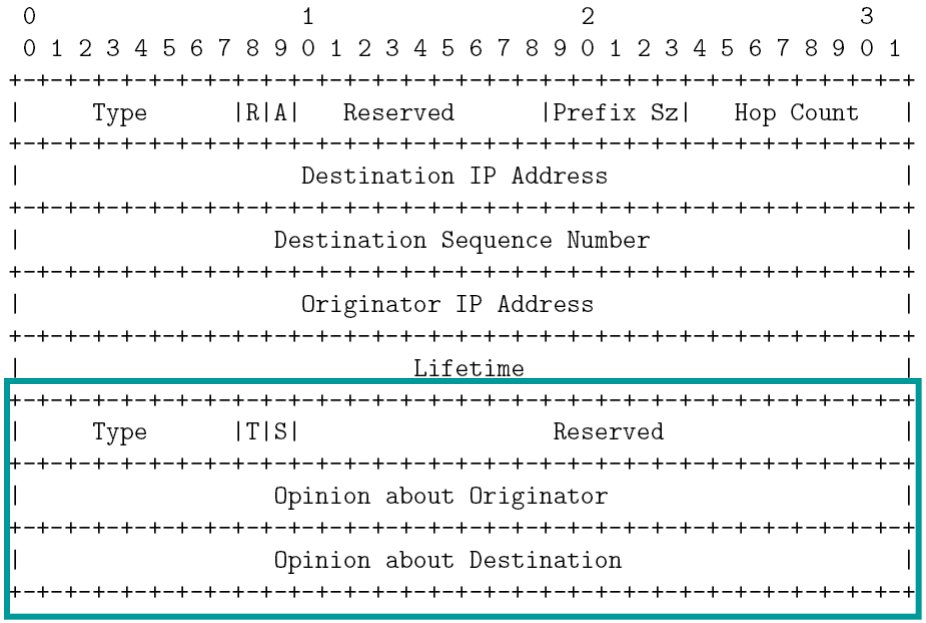
$$\omega_{B}^{A,(N_1N_2N_3)} = (0.8135, 0.0000, 0.1865)$$



Appendix H: Routing Message Extensions

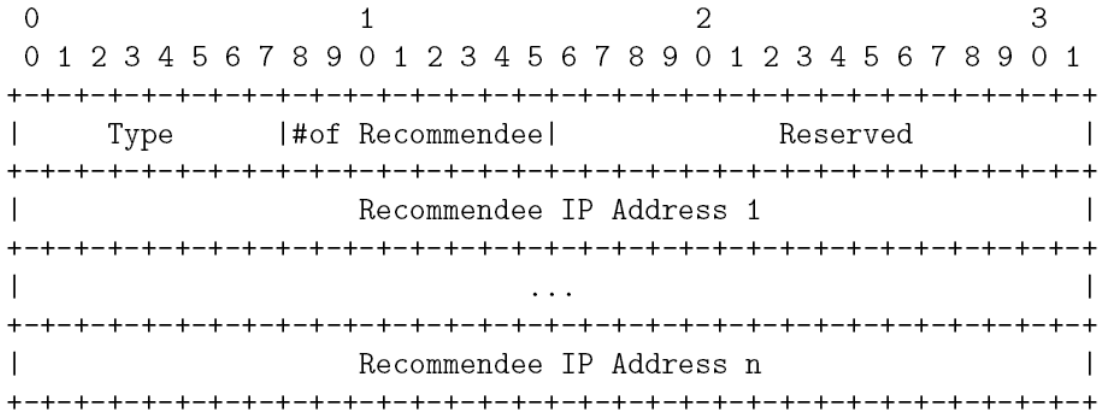
- Add trust information into original AODV routing messages.
  - RREQ →
    Trusted RREQ (TRREQ)
  - RREP →
    Trusted RREP (TRREP)





Trust Recommendation Protocol

- TREQ:



- TREP: