PAPER

Uncertainty Mitigation for Trustworthiness-Oriented Applications in Wireless Ad Hoc Networks

Feng LI[†], **Jie WU**[††], ***and*** **Avinash SRINIVASAN**[†††],

SUMMARY Link and node trustworthiness are important metrics in wireless ad hoc networks. Many existing wireless ad hoc network routing algorithms assume the availability of precise trustworthiness information. This, however, is an unrealistic assumption given the dynamics of wireless ad hoc networks. Therefore, a realistic method is needed to evaluate trustworthiness by mitigating uncertainty in the estimation process. In this paper, we propose a novel trustworthiness estimation model that accounts for uncertainty as well as two uncertainty mitigation schemes. We then illustrate the effectiveness of our schemes using a utility-oriented routing algorithm as a sample application. An extensive simulation study shows that these two uncertainty mitigation schemes significantly increase path stability and the long-term total benefit of the wireless ad hoc network.

key words: *Trustworthiness, risk, uncertainty, wireless ad hoc networks.*

1. Introduction

Wireless ad hoc networks operate in an infrastructureless wireless medium that is subject to message loss. This message loss is usually represented by a single metric called link trustworthiness. Various routing optimization problems have been formulated previously based on link trustworthiness, with little or no information on how to obtain credible trustworthiness values. Usually, the trustworthiness value is captured through monitoring where the behavior of a node (and the corresponding links) is monitored and recorded by its neighbors. These monitoring mechanisms typically use a simplistic trustworthiness estimation model for each link (i, j): it is the fraction of link (i, j)'s successful forwardings.

The trustworthiness estimated in this manner has an *uncertainty* component introduced either by an inadequate number of observations or by subtle changes in node behavior. Systematic ways of characterizing uncertainty in wireless ad hoc environments is still an unexplored territory. In this paper, we explicitly define the uncertainty metric to measure the possible variations and inaccuracies in the quantified trustworthiness metric, and propose two novel schemes for mitigating uncertainty: the unified metric scheme and the dynamic threshold scheme.

In the unified metric method, we use a metric called *risk factor* to reflect the negative consequences associated with uncertainty in the estimated trustworthiness. The unified metric is then computed as the weighted sum of the original optimization metric and the risk factor. Note that the optimization metric is application dependent. The unified metric is then used as the new optimization metric.

The dynamic threshold method operates in two phases. In the first phase, each node calculates a threshold for uncertainty, which is based on its characteristics, associated cost, and expected return. A candidate set of nodes are chosen based on their uncertainty level. In the second phase, the best path is selected by applying the original optimization algorithm on the candidate node set. Here, we strictly restrict our discussions to the routing process. However, the proposed schemes can be used for mitigating uncertainty of any optimization process in wireless ad hoc networks.

A utility-oriented routing model is used as a sample application to show the validity of our trustworthiness estimation model using the aforementioned uncertainty mitigation schemes. This model views the wireless ad hoc network as a real-world marketplace in which the system gains benefit for a completed message delivery service. Different values of benefit reflect different qualities or priority requirements of the routing requests. Each intermediate node has to incur a cost to relay a packet (e.g. cost in terms of energy). If the packet is lost during transmission, then there is no benefit. In this sample application model, utility, defined as the expected benefit of a path, is the original routing metric. In computing utility, trustworthiness plays a critical role. Therefore, our trustworthiness evaluation model, along with the uncertainty mitigation schemes, can aid users in making informed decisions.

In summary, our contributions are as follows: 1) We propose a distributed mechanism to identify underlying uncertainty in trustworthiness estimation. 2) We devise two novel schemes for uncertainty mitigation in wireless ad hoc networks, and present formal algorithms for both schemes. 3) We integrate uncertainty mitigation into a routing application for proof of concept. 4) We evaluate the schemes' applicability through extensive simulation and analysis.

2. Trustworthiness Estimation Model

Highly dynamic environment and self-organizing nature are two important characteristics of wireless ad hoc networks that make the precise evaluation of trustworthiness very critical for routing, QoS management, and intrusion detec-

[†] F. Li is with the School of Engineering and Technology, Indiana University-Purdue University Indianapolis, Indianapolis, IN 46022, U.S.A. E-mail: see http://www.engr.iupui.edu/~fengli/

[††] J. Wu is with the Department of Computer and Information Sciences, Temple University, Philadelphia, PA 19122, U.S.A. E-mail: see http://www.cis.temple.edu/~wu/

[†††] A. Srinivasan is with the Department of Mathematics, Computer Science, and Statistics, Bloomsburg University of Pennsylvania, Bloomsburg, PA 17815, U.S.A. E-mail: see http://facstaff.bloomu.edu/avinash/

DOI: 10.1587/trans.E0.??.1

Copyright © 200x The Institute of Electronics, Information and Communication Engineers

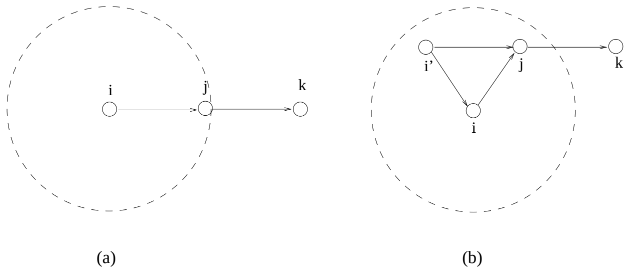


Fig. 1 Neighbor monitoring mechanism.

tion. However, these two characteristics make the process of gathering trustworthiness information extremely challenging.

Neighbor monitoring is a unique mechanism that helps to evaluate trustworthiness. Exploiting the promiscuous nature of broadcast communication in wireless media, nodes are able to track the outgoing packets of their one-hop neighbors through passive observation. When a node i sends a message through its neighbor j, the forwarding behavior of j can be monitored by node i. Similarly, j's behavior can also be monitored by any other node k that is a common neighbor of both i and j.

Bayesian inference is a statistical inference in which evidence or observations are used to update or to newly infer the probability that a hypothesis may be true. Beta distribution, $Beta(\alpha,\beta)$, is used here in the Bayesian inference, since it only needs two parameters that are continuously updated as observations are made. To start with, each node in the network has the prior $Beta(1,1)$ for all its neighbors. The prior $Beta(1,1)$ implies that the distribution of the trustworthiness metric p complies with the uniform distribution on $[0,1]$, which indicates complete uncertainty as there are no observations. If node i forwards a packet to the destination through j, i will classify the observation result as a success when i overhears j forward that packet. In this case, i increments $\alpha_i^j = \alpha_i^j + 1$. Here, α_i^j is node i's recorded metric α towards node j (Similar notations are used for other metrics). Otherwise, i will consider it to be a failure and increment $\beta_i^j = \beta_i^j + 1$. Each node can then estimate its neighbor's trustworthiness based on its accumulated observations using the Bayesian inference [3].

In this system, we use a triplet to represent the node's opinion towards trustworthiness: $(b,d,u) \in [0,1]^3$ and $b + d + u = 1$, where b, d, and u designate belief, disbelief, and uncertainty respectively in the statement that the transmission between two nodes is reliable. It should be noted that the entire opinion space is divided into two regions: certainty $(1-u)$ and uncertainty u. Now the opinion triplet (b,d,u) is derived from $Beta(\alpha,\beta)$.

There are two important attributes of uncertainty. First, when $(\alpha+\beta)$ is higher, it implies that there is more evidence, which consequently lowers uncertainty u. Second, when the evidence for success or failure dominates, there will be less uncertainty when compared to the situation in which there is equal evidence for both success and failure. This is because, for any given $(\alpha+\beta)$, uncertainty u will be at its peak when $\alpha = \beta$. Therefore, we define uncertainty u as the normalized variance of $Beta(\alpha,\beta)$ as follows:

$$u = \frac{12 \cdot \alpha \cdot \beta}{(\alpha+\beta)^2 \cdot (\alpha+\beta+1)} \tag{1}$$

The numerator and denominator in Equation 1 guarantee the latter and the former attributes respectively. This is also illustrated in Fig. 2. The variance is multiplied by a constant 12, which makes $u = 1$ when $\alpha = \beta = 1$. Equation 1 illustrates one of the possible definitions of uncertainty that complies with the summarized two properties.

The total certainty, which is $(1-u)$, can be divided into b and d according to their proportion of supporting evidence. Since the proportion of supporting evidence for the statement that the transmission between two nodes is reliable is $\frac{\alpha}{(\alpha+\beta)}$, b and d can be calculated as follows: $b = \frac{\alpha}{(\alpha+\beta)} \cdot (1-u)$ and $d = (1-u) - b = \frac{\beta}{(\alpha+\beta)} \cdot (1-u)$.

In the Bayesian procedure, the probability that the next packet will be successfully forwarded by the corresponding neighbor is given as: $p = \frac{b}{1-u} = \frac{\alpha}{\alpha+\beta}$.

Assume in Fig. 1(b), node i records $((\alpha_i^j,\beta_i^j) = (4,2))$ and node i' records $((\alpha_{i'}^j,\beta_{i'}^j) = (8,4))$ towards node j. The estimated trustworthiness will be the same, which is $p_i^j = p_{i'}^j = 0.66$. However, i's uncertainty toward j: $u_i^j = 0.38$ is much higher than i''s uncertainty towards j: $u_{i'}^j = 0.20$ according to Equation 1. Fig. 2 showcases the behavior of uncertainty when $(\alpha,\beta) \in [1,10]^2$.

3. Uncertainty Mitigation Schemes

According to the design of our trustworthiness estimation model, the uncertainty metric is defined as the information ordering between no knowledge and total certainty, to reflect the degree of confidence in the estimated trustworthiness. Uncertainty is obviously unfavorable when we want to use the estimated trustworthiness. The uncertainty metric itself is inapplicable when we make decisions based on the original optimization metric. Therefore, risk is introduced to account for the possible fluctuation in the original optimization metric caused by the existence of uncertainty in the estimation. This serves as a bridge to integrate uncertainty into the optimization process.

There are numerous ways to mitigate uncertainty. We propose two different schemes and discuss their design in detail in the remaining part of this section.

3.1 Dynamic Threshold Scheme

The dynamic threshold scheme is the more conservative of two schemes that we propose. To begin with, a node receives a request to participate in routing. The node then considers all possible next hop nodes and computes its uncertainty towards them using the accumulated observations. Then, threshold T is calculated to reflect its acceptable uncertainty level. Nodes with uncertainty above the threshold

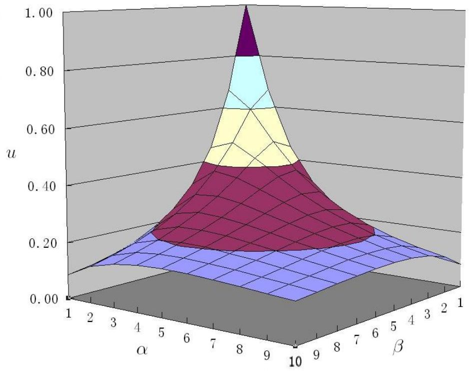


Fig. 2 Uncertainty illustration.

T are filtered out. From the remaining qualified nodes, the best node is chosen after running the original routing algorithm.

T should be dynamically determined based on the expected *cost* and *return*. This is necessary in order to accommodate the varying criticality of transactions. The cost and the return are computed by node i after receiving the request. The expected gain is represented as $G \in [0, \infty]$. Let $\tilde{C}$ represent normalized cost, and $\tilde{C}$ equals the ratio of the cost a node is required to invest in a given transaction and the maximum amount of cost that a node can invest in a single transaction. In this scheme, T can be defined as Equation 2:

$$T = 1 - \tilde{C}^{\frac{G}{\lambda}} \tag{2}$$

Here, λ is the characteristic factor that reflects a node's attitude towards risk: conservative (a large number) or aggressive (a small number). A higher λ will lead to a lower T which makes the filtering more conservative. Intuitively, when the cost of a particular transaction is high, a node may not be willing to accept higher uncertainty. On the contrary, when the associated returns are high, T will be pushed higher, and consequently, nodes accept more uncertainty. According to Equation 2, a larger $\tilde{C}$ will lead to a lower T. On the other hand, a larger G will lead to a higher T since $\tilde{C} \in [0, 1]$.

In our model, T is dynamic. Note that a static implementation of T is much easier. However, it is inflexible and contradictory to the general experiences of the uncertainty mitigation decision process.

In Fig. 1(b), assume node i records $((\alpha_i^j, \beta_i^j) = (1, 7))$ towards node j and $T = 0.10$. From Equation 1, $u_i^j = 0.13$. Now, since $u_i^j > T$, node i will discard node j's request.

3.2 Unified Metric Scheme

The unified metric scheme views uncertainty from a completely different perspective. It is more aggressive compared to the dynamic threshold scheme. Similar to the above scheme, the process begins with a request. After receiving the request, the node will compute its risk factor R that reflects the possible fluctuations in the outcome of a transaction. The uncertainty captured by the reputation system is used in the computation of R as follows:

$$R = u \cdot G^2 \tag{3}$$

Here again, $G \in [0, \infty]$ is the expected gain. The motivation behind Equation 3 is as follows: with the same G, higher uncertainty leads to higher risk; and with the same uncertainty, higher G, which implies that successful packet relay in this hop is critical, leads to higher risk. The unified metric $\tilde{M}$ itself is computed as the weighted sum of the risk factor R and the original routing metric M. Once the $\tilde{M}$ is computed, it is used as the original routing metric in the path selection process. $\tilde{M}$ is calculated as follows:

$$\tilde{M} = M - \lambda \cdot R \tag{4}$$

where λ is the node's characteristic factor in the given scenario and M is the original routing metric. However, since risk is always unfavorable, it is considered to be a penalty and subtracted from the original metric when computing $\tilde{M}$.

Consider Fig. 1(b), $M_i = M_{i'} = 50$, $R_i = 20$, $R_{i'} = 30$, and $\lambda_i = \lambda_{i'} = 0.8$. Now, according to Equation 4, $\tilde{M}_i = 34$ and $\tilde{M}_{i'} = 26$. Consequently, node i will be chosen during path selection since maximum $\tilde{M}$ is the routing criteria here. With the original routing metric, either A or B could be chosen. But, with our unified metric scheme, we enable the path selection process to choose the path with implicit uncertainty mitigation.

4. An Application: Utility-Oriented Routing

In utility-oriented routing [18], each routing is considered to be a transaction. Utility, defined as the expected benefit of the transaction, is chosen as the primary routing metric. This model sets up an ideal platform to demonstrate the effectiveness of our trustworthiness estimation model and the uncertainty mitigation schemes. This is because, in utility-oriented routing, the primary routing metric is derived from trustworthiness. In [18], trustworthiness is assumed to be static and obtainable. We consider this to be a strong and unrealistic assumption. In our methodology, we relax this assumption and use a realistic trustworthiness estimation model that takes into account the underlying uncertainty. In [18], there are two parameters that influence path selection: topology and packet value. However, using our trustworthiness estimation model, two additional parameters influence path selection: uncertainty u and nodes' attitude λ.

4.1 Utility-oriented Routing: Model Overview

We consider a source s that intends to send a packet to a destination k. s will get a benefit v if the packet is successfully delivered to d. The network is modeled as a unit disk graph. For each link (i, j) in the graph, there are two associated properties: cost and trustworthiness. Cost c_i^j is the minimal energy level required to connect i and j, while trustworthiness p_i^j is the ratio of packets forwarded by j and the packets sent by i. For illustration, we first consider a single-link route from s to k with trustworthiness p^k_s and cost c^k_s. Since k receives a packet with probability p^k_s, s has the same probability of getting the benefit v at the cost c^k_s. Note that s gets v if and only if the packet is delivered to k. From an economic perspective, the expected utility of this route is the difference between the expected benefit and the route's cost:

$$U = v \cdot p^k_s - c^k_s \tag{5}$$

Consider the multi-hop route $< s = 1, \cdots, k-1, k >$. Here, the utility is calculated as follows:

$$U = v \cdot \prod_{j=1}^{k-1} p_j^{j+1} - \sum_{i=1}^{k-1} c_i^{i+1} \prod_{j=1}^{i-1} p_j^{j+1} \tag{6}$$

However, an important observation in a multi-hop route is that the source s realizes the benefit v if and only if the transmission is successful on each link (i, j) between s and k. Thus, from the destination's point of view, any intermediate node can be considered the virtual source and the corresponding utility can be calculated from that virtual source to the destination. On the other hand, from the source's point of view, any intermediate node can be considered the virtual destination. Then the source's benefit will be equal to the intermediate node's utility. This method can be extended to multi-hop routes by recursively applying Equation 5 starting from destination k.

4.2 Application of the Trustworthiness Estimation Model

A neighbor monitoring mechanism is employed to gather information for estimating trustworthiness. While sending packets to its next-hop neighbor j, a node i will also try to over-hear and count the number of packets that j further forwards. If j forwards a packet sent by i, then i will consider this a successful forwarding and increment α^j_i. Otherwise, i increments β^j_i. When i needs to evaluate its utility and uncertainty for routing purposes, it will calculate (b, d, u) from the recorded α^j_i and β^j_i using the Beta function. Once the triplet is computed, the estimated trustworthiness is computed based on the triplet. To keep the integrity of this method, the destination node should send an acknowledgement to its one-hop neighbors when it receives a packet.

4.3 Application of the Unified Metric Scheme

The unified metric scheme is an iterative approach in which each node will combine the calculated risk with utility to obtain the $\tilde{M}$ based on λ. $\tilde{M}$ is then broadcast in the neighborhood. This process continues until a path has been successfully selected with $\tilde{M}$ as the primary routing metric. Here, $\tilde{M}$ is computed using Equation 4 where M is replaced by utility U which is the primary routing metric.

Now consider the utility-oriented routing model with nodes i and j, and assume j invites i. Here, without uncertainty, i's expected gain G would be j's broadcast utility U_j. This, however, changes in our estimation model, which accounts for uncertainty. Here, i's expected gain will be j's broadcast unified metric $\tilde{M}_j$. Therefore, in Equation 3 we should define $G = \tilde{M}_j$ before computing R. Algorithm 1 shows the steps involved in our unified metric uncertainty mitigation scheme.

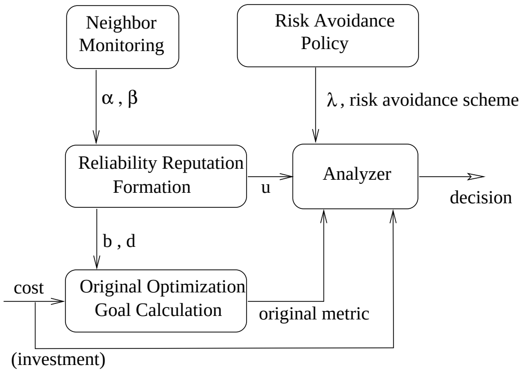


Fig. 3 The flow of decision.

Algorithm 1 Unified Metric

```
Initialize the selected node set← $\emptyset$;
while $s \notin$ the selected node set do
    Find node $i$ with the largest $\tilde{M}_i$ in the unselected node set;
    Add $i$ to the selected node set;
    Delete $i$ from the unselected node set;
    For each neighbor $j$ of $i$ that hasn't been selected, Relax$(i, j)$;
end while
```

Relax(i, j)

```
Calculate node $j$'s utility based on $i$'s: $U^i_j = U_i \cdot p^i_j - c^i_j$;
Calculate node $j$'s risk factor in choosing node $i$ as the next-hop node:
    $R^i_j = u^i_j \cdot (\tilde{M}_i)^2$;
Calculate $\tilde{M}_j$ in choosing node $i$: $\tilde{M}^i_j = U^i_j - \lambda \cdot R^i_j$;
Update $U_j$ and $\tilde{M}_j$ if $\tilde{M}_j < \tilde{M}^i_j$;
```

Although Algorithm 1 is centralized, a distributed implementation can be realized by using a back-off timer on each node. $\tilde{M}$ could be treated as the summary of topology information along with the underlying uncertainty. Each node locally determines its next-hop node based on the above summarized information. The distributed implementation can be gracefully integrated into a reactive routing protocol, such as AODV [20] or DSR [10].

The value of the back-off timer on each node i is set to $(v - \tilde{M}_i)$. This value reflects the value of $\tilde{M}$. If there is no transmission delay, the node with maximum $\tilde{M}$ will always broadcast the route reply first. However, due to transmission delays, this implementation can only be an approximation.

4.4 Application of the Dynamic Threshold Scheme

When using the dynamic threshold scheme, each node will filter requests by the dynamic uncertainty threshold and calculate the remaining utility. The utility U is then broadcast in the neighborhood. Nodes in the network should have a maximum possible transmission range. Therefore, each

Algorithm 2 Dynamic Threshold

```
Initialize;
while $s$ is not selected do
    Find node $j$ with the largest $U_j$ in the nodes with status unselected;
    Mark $j$ as selected;
    For $j$'s each neighbor $i$ with status unselected, Relax($j, i$);
end while

Relax($j, i$)
Calculate utility: $(U_i)' = U_j \cdot p_i^j - c_i^j$;
Find the uncertainty threshold: $T = 1 - \tilde{C}^{\frac{G}{\lambda}}$;
if $(U_i)' \geq R_i$ and $u_i^j \leq T$ then
    Update $U_i \leftarrow (U_i)'$;
end if;
```

node can calculate the amount of energy c_{max} associated with the maximum possible communication range. Therefore, the normalized cost $\tilde{C}$ is: $\tilde{C} = c_i^j / c_{max}$. Expected gain G is the other important metric, which is the expected utility U_i in this model. T can be calculated using Equation 2.

Algorithm 2 exploits an idea similar to Dijkstra's shortest path algorithm [6] while using utility as the routing metric and applies the uncertainty mitigation scheme. All nodes except the destination will have the zero initial utility and the unselected status at the beginning. The algorithm works backwards from the destination. A node will be marked as selected when it has the largest utility among all the unselected nodes and relax its neighbors. Node i, when relaxed by node j, calculates $(U_i)'$ and compares with the original U_i. If $(U_i)' > U_i$, then i calculates T according to Formula 2 and compares it with u_i^j. It then follows the rules below:

1) If $u_i^j > T$, reject. u is higher than acceptable.

2) If $u_i^j \leq T$, accept. $U_i \leftarrow (U_i)'$.

A distributed implementation of Algorithm 2 can be realized in a similar manner as suggested for Algorithm 1 with two minor modifications. First, when being relaxed by a neighbor, the node will compute T and decide whether it should reject the request. Second, the value of the timer for a node i is $(v - U_i)$, which reflects j's current utility since utility is the primary routing metric.

4.5 Example

An example can be given as shown in Fig. 4, where the packet value $v = 100$. If node s sends 10 packets to node i and observes that i successfully forwards only 9 of them, then s records $(9, 1)$ for (α_s^i, β_s^i) with $c_s^i = 10$. Similarly, other nodes record their observations in the tuple (α, β) as shown in Fig. 4.

In the unified metric scheme, nodes will be relaxed starting from the destination. Assume $\lambda = 0.1$ is uniform throughout the network. Now let us consider the scenario in which all the nodes excluding s have completed their computation. Assume s has received a relaxation request from i, k, and j. s will compute U_s and $\tilde{M}_s$ using U and $\tilde{M}$ from i, k, and j respectively. s will then choose the node that yields the largest $\tilde{M}_s$ as its next-hop node. For instance, using U_i and $\tilde{M}_i$, s computes $U_s^i = 21.09$ and $\tilde{M}_s^i = 20.02$ with a risk factor of 10.74. Similarly, $U_s^j = 25.00$ and $\tilde{M}_s^j = 18.32$ with a risk factor of 66.81. Therefore, s will not accept j's relaxation request since the associated risk factor is very high. So, with the unified metric scheme, the path $s - i - i' - k$ is finally selected. Similar results can be observed using the dynamic threshold scheme.

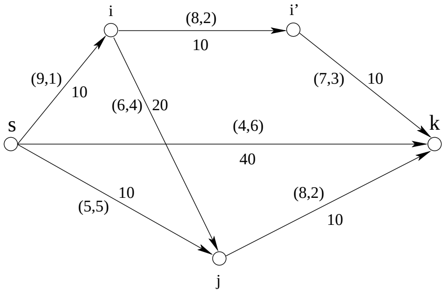


Fig. 4 An example illustrating utility-oriented routing with the uncertainty mitigation schemes.

For further discussion, assume node s records one more failure from its neighbors i and j. Now we have $(\alpha_s^j, \beta_s^j) = (5, 6)$ and $(\alpha_s^i, \beta_s^i) = (9, 2)$. If we consider only utility and choose j as s's next-hop, then the new $U_s^j = 15.74$ which drops very quickly from the previous scenario. However, when using the unified metric scheme we choose i, and new $U_s^i = 20.01$, which remains stable with very little variation.

5. Analysis

The mitigation schemes provide more information about the possible fluctuation caused by the uncertainty in trustworthiness estimation. To simplify the discussion, these attributes are presented under the utility-oriented routing application.

Attribute 1: (Selection Stability): Both schemes increase path selection stability.

Proof: The trustworthiness is estimated from the results of neighbor monitoring. As the evidence accumulates, the value of the estimated trustworthiness stabilizes. If the variation is large enough, another route will become the best path under the given routing criterion, thereby causing changes in the selected path.

Consider a simple situation: two nodes i and j have a common neighbor k which is the destination. Assume at first $U_i \geq U_j$, because of which the path containing node i is selected. After some time, node i will accumulate more evidence towards the trustworthiness $p_i^k = \frac{\alpha_i^k}{\alpha_i^k + \beta_i^k}$. Assume with all parameters remaining the same, the new $(p_i^k)'$ decreases to a point that makes $(U_i)' < U_j$. Without uncertainty mitigation schemes, the selected path should be changed because ΔU_i is large enough. Assume $((\alpha_i^k)', (\beta_i^k)')$ are the new results causing the change. The ΔU_i will be:

$$\Delta U_i = \left(\frac{\alpha_i^k}{\alpha_i^k + \beta_i^k} - \frac{(\alpha_i^k)'}{(\alpha_i^k)' + (\beta_i^k)'} \right) \cdot U_T \tag{7}$$

Using the unified metric scheme, the path selection decision at the beginning will be based on $\tilde{M}_i$ and $\tilde{M}_j$. If $\tilde{M}_i \geq \tilde{M}_j$ at the beginning, node i will be selected. After we get $((\alpha_i)', (\beta_i)')$ from the observation, $\Delta\tilde{M}_i$ will be:

$$\Delta\tilde{M}_i = \Delta U_i - \lambda \cdot \Delta R_i \tag{8}$$

where $\Delta R_i = (u_i - (u_i)') \cdot \tilde{M}_d$. The uncertainty will always decrease as evidence accumulates. So $\Delta R_i \geq 0$, $\Delta\tilde{M}_i \leq \Delta U_i$. Hence, the probability that the selected path changes to include node j also decreases.

The dynamic threshold approach increases path stability from a completely different perspective. It defines the dynamic threshold of uncertainty as:

$$T = 1 - (\frac{c_j^i}{c_{max}})^{\frac{U_j}{\lambda \cdot c_j^i}} \tag{9}$$

This threshold will block out nodes that are sensitive to change in trustworthiness before they are selected because of high utility. Using the above setup, if node i is more sensitive to trustworthiness changes and its uncertainty towards k is large enough in the beginning, it will be blocked out and the change in the selected path will not occur. □

Path selection stability is a measure of the frequency of change in the selected path. The underlying reason for this change is the accumulating observations and the corresponding change in the estimated trustworthiness metric.

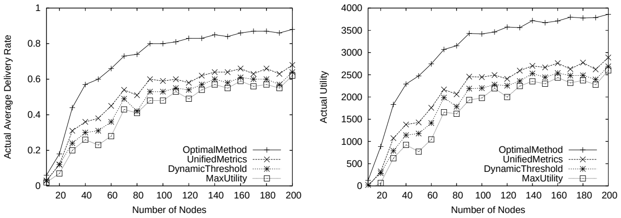
Attribute 2: (Eventual Optimality): After accumulating enough observations, the utility-oriented routing mechanism using either of the proposed uncertainty mitigation schemes will achieve path selection optimality.

Proof: The observations are represented as (α,β). After a sufficiently long time, the total number of observations increases to a large number, say $\alpha + \beta \to \infty$. Then the uncertainty metric $u_i^j \to 0$. In the unified metric scheme, the risk factor $R \to 0$, and $\tilde{M}_i = U_i$. The path selection scheme based on unified metric $\tilde{M}$ or utility U_i will produce the same result. For the dynamic threshold scheme, $u_i^j < T$ is always true because $T > 0$. No node will be filtered out. Therefore, Algorithm 1 and 2's eventual optimality is equal to the optimality of the algorithm that selects a path with maximum utility. The proof of the maximum utility algorithm's optimality can be seen in our previous work [18]. So both mitigation schemes eventually achieve optimality.□

Attribute 3: (Character Reflection): Both uncertainty mitigation schemes can reflect a node's risk-evading or risk-seeking attitude.

Proof: Nodes' attitudes towards risk are reflected by characteristic factor λ in both the proposed schemes. To validate our claim, we assume all other parameters are the same, with node i as the subject, and show how λ influences the result.

In the unified metric scheme, $\tilde{M}_i = U_i - \lambda \cdot R_i$ where λ is the weight of the risk factor. λ is indicative of a node's risk-seeking behavior as the weight of the risk factor will be scriptsize, while a larger λ indicates otherwise.



(a) Delivery ratio (b) Average utility

Fig. 5 Performance comparison.

In the dynamic threshold scheme, the threshold T reflects nodes' attitude. According to Equation 2, a larger λ leads to a larger T which indicates that the node accepts larger uncertainty, as less requests will be filtered out and more neighbors will qualify with acceptable uncertainty. □

6. Simulation Evaluation

In this section, we evaluate the performance of the proposed uncertainty mitigation schemes through simulations. Without loss of generality, cost is modeled as the energy consumption. We compare the utility-oriented routing method with/without uncertainty mitigation schemes.

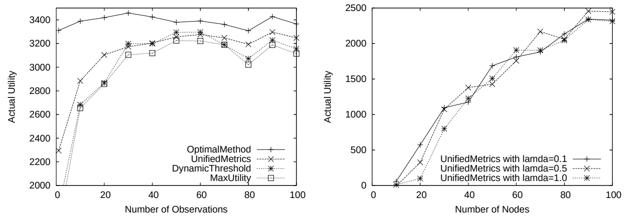
The optimal method is the original MaxUtility algorithm using the actual trustworthiness. Since this information can not be directly recorded in a real wireless ad hoc network, this optimal method is not applicable in real life settings and it is used as a benchmark to evaluate the performance of our algorithms. The MaxUtility method is the original MaxUtility algorithm using the estimated trustworthiness, but it does not consider the uncertainty metric.

6.1 Simulation Environment

We develop a stand-alone, discrete event simulator to evaluate our schemes. This simulator only implements the network layers and it makes simple assumptions regarding lower layers. We set up the simulation in a $900m \times 900m$ area. In our experiments, the energy cost between any two nodes is proportional to their distance.The actual stability of each link is randomly generated (uniform distribution) in the range $[0, 1]$. For each set of specified parameters, we run each algorithm 100 times and use the average value of the results to evaluate the performance.

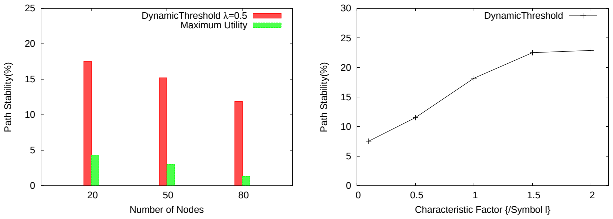
In our simulation, the packet value $v = 5,000$. λ is uniform for the entire network to reflect the network's risk attitude with a default value of 0.5. The system scale parameter $a = 0.001$ for both the schemes. Each node accumulates l observations before route discovery where l is a random number in $[0, 15]$.

After all nodes in the network complete accumulating l observations of their neighbors, the route discovery phase begins. Each algorithm selects the best path and 500 packets



(a) Number of observations l (b) Characteristic factor λ

Fig. 6 The effect of different parameters.



(a) Number of nodes n (b) Characteristic Factor λ

Fig. 7 Path stability with different (a) n, (b) λ.

are transmitted over each selected path for which the total cost, delivery ratio, and packet value are recorded. The average utility is then calculated based on these metrics. In our simulations, there are two tunable parameters: the number of nodes n and the total number of observations $l = \alpha + \beta$.

6.2 Simulation Results

We adjust the number of nodes in the network to compare the performance of utility-oriented routing with and without uncertainty mitigation schemes. The number of nodes decides the node density, which in turn determines the communication cost and node degree.

In Fig. 5 (a), the delivery ratio of the optimal method is much higher than the other three methods that use estimated trustworthiness based on neighbor monitoring. The estimated trustworthiness metric is inaccurate and contains uncertainty. Hence, there is a difference between the optimal path and the selected path for these three algorithms. The unified metric scheme and dynamic threshold scheme exploit the uncertainty information implied in the monitoring results while MaxUtility algorithm only considers the direct estimated trustworthiness metric.

Because our schemes avoid nodes with high uncertainty, they achieve a better delivery ratio compared to MaxUtility. Another point that is worth noticing in Fig. 5 (a) is that as the number of nodes in the network increases, the differences in the delivery ratio between the optimal method and other three methods becomes larger. When node density is higher, there are more possible paths to choose from. With inaccurate trustworthiness information, it would be harder to find a path that achieves a higher packet delivery ratio. Fig. 5 (b) shows the average utility. It is clear that our mitigation schemes outperform the MaxUtility algorithm, which omits the uncertainty in trustworthiness evaluation.

Fig. 6 (a) illustrates the change in average utility when observations accumulate. When more observations are accumulated, the estimation of the trustworthiness metric becomes more accurate and tends to stabilize. The uncertainty in estimation is reduced. Therefore, the differences between the optimal method and the two uncertainty mitigation schemes decrease when the number of observations before route discovery increases.

Fig. 6 (b) compares the two uncertainty mitigation schemes with different characteristic factors λ. The results indicate that using the same uncertainty mitigation scheme, whether $\lambda = 1.0$ or $\lambda = 0.1$ leads to better average utility is totally random. It complies with our experience. Although considering risk helps us to make more informed decisions, the answer to ‘whether the risk seeking or evading attitude is better’ depends on the specific application domain.

Fig. 7 (a) shows another advantage of our uncertainty mitigation schemes. In this simulation, we run the algorithms with the number of observations l in $[0, 15]$, $[30, 45]$ and $[60, 75]$. Using the uncertainty mitigation scheme, a great improvement in path stability can be seen as uncertainty is considered beforehand.

Although the nodes’ risk attitude cannot improve the average utility, it has a strong impact on path stability. From Fig. 7 (b) we can see that the path stability increases as λ increases. When nodes are risk-evading, the paths seem to be more stable.

7. Related Work

Trustworthiness is an important metric in wireless ad hoc networks [8][16]. Many routing algorithms [5][7][18] consider this metric and compute their routing metrics on the basis of quantified trustworthiness. The method of collecting trustworthiness information in a distributed manner and evaluating the inaccuracies and uncertainty in the collected value remains undiscussed. It allows nodes to form trust opinions towards trustworthiness according to its own observations, and uses a metric to measure the uncertainty. This uncertainty-centric reputation system is unique [15], as only a few of the existing reputation systems [1][2][3][22] explicitly consider the uncertainty metric [11][17].

In this paper, to evaluate the possible fluctuation in the routing metric caused by existing uncertainty, risk is introduced. The methods to identify and quantify risk are widely studied in many trust-management systems [9][12]. The SECURE project [4] analyzes a notion of trust that is inherently linked to risk. Risk is evaluated on every possible outcome of a particular action and is represented by the outcome’s intrinsic cost. [19] and [13] combine risk and trust. In [19], the authors explicitly avoid expressing measures of trust directly. Instead, they develop a model around other elements such as transaction values and the transaction history. Trustworthiness trust and decision trust are distinguished in [13].

We use utility-oriented routing as a sample application in this paper. Other works also use utility as the optimization objective. A price-based scheme is presented in

[14] to effectively allocate resources among multiple multi-hop flows. This approach maximizes the aggregated utility of flows, while maintaining basic fairness among multiple flows. In [21], a market-based approach is proposed to efficiently allocate bandwidth.

8. Conclusion and Future Work

Evaluating and quantifying trustworthiness is of critical importance in wireless ad hoc networks. Existing optimization algorithms in wireless ad hoc networks assume the availability of precise trustworthiness information, which is unrealistic due to the dynamics of ad hoc networks. In this paper we have presented a novel trustworthiness estimation model that accounts for uncertainty, and two uncertainty mitigation schemes. Through simulations, we have evaluated the performance of our schemes on an existing utility-oriented routing protocol in evaluating trustworthiness under different levels of uncertainty. However, since uncertainty may change constantly as new observations are made, the path re-selection cost in our schemes can be high. In our future research, we will investigate opportunistic routing methods to reduce the path re-selection cost of our schemes to make them more robust.

References

[1] S. Bansal and M. Baker. Observation-based cooperation enforcement in ad hoc networks. *CoRR*, cs.NI/0307012, 2003.

[2] S. Buchegger and J. Boudec. Performance analysis of the confidant protocol. In *Proc. of ACM MobiHoc*, pages 226–236, 2002.

[3] S. Buchegger and J.Y.L. Boudec. A robust reputation system for p2p and mobile ad-hoc networks. In *Proc. of the Second Workshop on the Economics of Peer-to-Peer Systems*, 2004.

[4] V. Cahill, E. Gray, J. Seigneur, C. Jensen, Y. Chen, B. Shand, N. Dimmock, A. Twigg, J. Bacon, C. English, W. Wagealla, S. Terzis, P. Nixon, G. Serugendo, C. Bryce, M. Carbone, K. Krukow, and M. Nielsen. Using trust for secure collaboration in uncertain environment. *IEEE Pervasive Computing*, 2(3):52–61, 2003.

[5] C. Chiu, E. Wu, and G. Chen. Stability aware cluster routing protocol for mobile ad-hoc networks. In *Proc. of IEEE ICPADS*, 2002.

[6] T. Cormen, C. Leiserson, R. Rivest, and C. Stein. *Introduction to Algorithms, Second Edition*. 2001.

[7] D. Couto, D. Aguayo, J. Bicket, and R. Morris. A high-throughput path metric for multi-hop wireless routing. In *Proc. of ACM MobiCom*, 2003.

[8] M. Gerharz, C. de Waal, M. Frank, and P. Martini. Link stability in mobile wireless ad hoc networks. In *Proc. of IEEE LCN*, 2002.

[9] T. Grandison and M. Sloman. A survey of trust in internet application. 2000.

[10] D. B. Johnson and D. A. Maltz. Dynamic source routing in ad hoc wireless networks. *Mobile Computing*, 1994.

[11] A. Josang. An algebra for assessing trust in certification chains. In *Proc. of the Network and Distributed Systems Security Symposium*, 1999.

[12] A. Josang, R. Ismail, and C. Boyd. A survey of trust and reputation systems for online service provision, 2006.

[13] A. Josang and S. Presti. Analysing the relationship between risk and trust. In *Proc. of the Int'l Conf. on Trust Management*, 2004.

[14] B. Li, Y. Xue, and K. Nahrstedt. Price-based resource allocation in wireless ad hoc networks. Technical report, UIUCDCS-R-2003-2331, Univ. of Illinios at Urbana-Champaign, 2003.

[15] F. Li and J. Wu. Mobility reduces uncertainty in MANETs. In *Proc. of IEEE INFOCOM*, 2007.

[16] F. Li, Y. Yang, and J. Wu. CPMC: An efficient proximity malware coping scheme in smartphone-based mobile networks. In *Proc. of IEEE INFOCOM*, 2010.

[17] F. Li, Y. Yang, J. Wu, and X. Zou. Fuzzy closeness-based delegation forwarding in delay tolerant networks. In *Proc. of IEEE NAS*, 2010.

[18] M. Lu and J. Wu. Social welfare based routing in ad hoc networks. In *Proc. of ICPP*, 2006.

[19] D. Manchala. Trust metrics, models and protocols for electronic commerce transactions. In *Proc. of the IEEE ICDCS*, 1998.

[20] C. Perkins. Ad hoc on demand distance vector (aodv) routing ietf. *Internet Draft, draft-ietf-manet-aodv-00.txt*, 1997.

[21] Y. Qiu and P. Marbach. Bandwidth allocation in wireless ad hoc networks: A price-based approach. In *Proc. of IEEE INFOCOM*, 2003.

[22] G. Wang and J. Wu. Flowtrust: Trust inference with network flows. In *accepted to appear in Frontiers of Computer Science in China*, 2011.

Feng Li received his Ph.D. in Computer Science from Florida Atlantic University in Aug. 2009. His Ph.D. advisor is Prof. Jie Wu. He joined the Department of Computer, Information, and Leadership Technology at Indiana University-Purdue University Indianapolis (IUPUI) as an assistant professor in Aug. 2009. His research interests include the areas of mobile computing, security, and trust management. He has published more than 20 papers in conferences and journals.

Jie Wu is chairman and professor in the Department of Computer and Information Sciences, Temple University. His research interests include the areas of wireless networks and mobile computing, routing protocols, fault-tolerant computing, and interconnection networks. He has published more than 450 papers in various journals and conference proceedings. He serves in the editorial board of the IEEE Transactions on Mobile Computing. He has served as an IEEE Computer Society distinguished visitor and is the chairman of the IEEE Technical Committee on Distributed Processing (TCDP). Dr. Wu is a fellow of the IEEE.

Avinash Srinivasan received his Ph.D. in Computer Science from Florida Atlantic University in Aug. 2008. His Ph.D. advisor is Prof. Jie Wu. He joined Bloomsburg University of Pennsylvania an Assistant Professor in Computer Forensics in Aug. 2008. He has been actively engaged in research on network security, forensic analysis, reputation and trust-based security models for wireless and sensor networks, and terrorist network modeling. He has published 22 papers in conferences and journals.