doi:10.2498/cit.1002139

Trust Based Routing to Improve Network Lifetime of Mobile Ad Hoc Networks

Sumathy Subramaniam, R. Saravanan and Pooja K. Prakash

School of Information Technology and Engineering, VIT University, Vellore, India

Mobile Ad hoc Network is an impromptu wireless network consisting of mobile, self governing independent nodes. Routing in Mobile Ad hoc Networks has been a major concern due to its dynamic topology, lossy and unreliable links. In traditional routing, a single specific node is selected in prior as the potential next-hop forwarder for a packet. Unlike traditional routing, a category of routing technique termed Opportunistic Routing exploits the broadcast nature of wireless medium to compensate the unreliability of the packet transmissions in the channel. In Opportunistic Routing, one among the set of candidate nodes is selected as the potential next-hop forwarder using metrics like number of transmissions in a link, link error probability, cost, etc., for packet transmission. For selection and prioritization of candidates that ensures minimum number of transmissions from source to destination node, whilst improving the lifetime of the network on determining the residual battery energy, a new metric is proposed. This metric helps in improving the network lifetime considering the transmission powers in terms of the fraction of residual battery powers. Further, as nodes in mobile ad hoc networks are susceptible to attacks, a trust model based on direct, as well as indirect trust degrees from similar trusted neighbours is integrated in order to overcome the vulnerability due to attacks by malicious/selfish nodes and to provide reliable packet transmissions. Fading of trust is incorporated with a perspective to ensure the uncertainty of trust with time until it is updated.

Keywords: opportunistic routing, network lifetime, ETX, EAX, residual battery power, trust model, trust degree

1. Introduction

Mobile Ad hoc Networks (MANETs) are rapidly deployable, self-configuring networks that do not rely on any existing infrastructure. Devices connected by wireless links that make the topology of the network extremely dynamic require to emphasize routing in MANETs with a major concern. Traditional routing techniques are similar to those in wired networks where a path between a source and its destination is pre-determined and the traffic is sent along this sequence of nodes. In other words, a fixed next hop node is used as a forwarder for the packets. However, these techniques do not apply well in dynamic wireless environments where links are unreliable. Hence, transmitting packets over a pre-determined path as in traditional routing does not apply well.

Opportunistic Routing (OR) techniques that exploit the broadcast nature of the wireless medium are preferable in MANETs as they improve the packet forwarding probability in multi-hop wireless networks and do not require large routing tables. Each candidate node does not require maintaining the details of nodes beyond the knowledge of their neighbouring nodes. They are scalable for large networks and are known to increase the performance of wireless networks. In OR, a set of next-hop nodes are selected as candidates which act as the prospective forwarders prior to packet transmission and one of them is chosen on a per-packet basis according to its reachability at that instant.

The aim of OR in performing candidate selection and prioritization is to identify and prioritize potential candidates so as to minimize the number of transmissions from the source to the destination. Transmission of a packet basically requires candidate coordination in order to avoid duplicate re-transmissions. It involves in identification of the highest priority candidate that has received the packet and must forward it.

With several characteristics such as dynamic topology, multi-point hopping, constrained resources (limited bandwidth, computing power, physical security) finite battery energy, lack of a central administration, MANETs are prone to attacks by malicious or selfish nodes. Malicious node modifies the network traffic and the selfish nodes do not forward traffic from other neighbour nodes. This makes security issues one of the major concerns in ad hoc networks. Hence, a mechanism to evaluate the neighbours' forwarding behaviour to ensure reliability needs to be integrated.

An enhanced trust model based on the history of past interactions of both direct and recommendations from the trusted neighbours are used in the computation of the trust degree. While the former is based on direct interactions, the latter corresponds to the recommendations obtained by similar and trusted neighbours. Similar neighbours come into the picture as it is duly assumed that nodes that have similar trust degrees on a neighbour tend to have similar trust degrees on another neighbour too. Once the trust degrees are set, only the nodes that satisfy a pre-determined threshold value are used for packet transmission.

This paper proposes a new metric, for the selection and prioritization of candidates with the aim of improving the lifetime of the network considering the residual battery power of each node in the link and with reliable nodes as potential forwarders in the network.

The rest of the paper is organized as follows. Section 2 covers the background with sub-sections 2.1 and 2.2 discussing Opportunistic Routing and existing Trust Models respectively. Section 3 and its sub-sections discuss the proposed framework and Section 4 presents a sample illustration. The simulation results and analysis are presented in Section 5. Finally, the conclusion and future enhancements are given in Sections 6 and 7 respectively.

2. Background

2.1. Opportunistic Routing

Various candidate selection algorithms such as Extremely Opportunistic Routing (ExOR), Opportunistic Any-Path Forwarding (OAPF), Least-Cost Opportunistic Routing (LCOR) and Minimum Transmission Selection (MTS) are evaluated in terms of the number of transmissions needed to reach the destination, as discussed by Amir Darehshoorzadeh et al., (2011).

Based on the analysis of the existing literature, it is indicated that while ExOR is the fastest among the others, MTS and LCOR are the near-optimum algorithms with MTS outperforming LCOR with respect to candidate selection. However, both MTS and LCOR take longer time to compute the candidate sets. On the other hand, OAPF is a simple OR selection algorithm which is comparatively fast. It can be seen as an intermediate between ExOR and MTS and is hence preferable comparatively.

De Couto D. S. et al., (2005) proposed the Expected Transmission Count (ETX) metric which finds the path with the least expected number of transmissions (including re-transmissions) required for successfully delivering a packet to its destination. The ETX of a link is calculated as the reciprocal of the forward delivery ratio, d_f and that of a route is calculated as the sum of the ETX of each link in the chosen route.

In ExOR, an OR mechanism based on ETX metric proposed by Sanjit Biswas and Robert Morris (2005), the candidates for a node include all the next-hop nodes whose ETX to the destination is smaller than that from itself. Further, the candidates are then prioritized on the basis of the best-path ETX from the chosen candidate to the destination node. However, selecting many candidate nodes also in turn increases the complexity of candidate coordination, which becomes a drawback. Moreover, another drawback is that the ETX metric does not account for the fact that the candidates also in turn forward packets opportunistically, as discussed by Zhong Z. et al., (2006).

OAPF, a hop-by-hop routing scheme based on Expected Any-Path Transmission (EAX) metric is discussed by Zhong Z. et al., (2006) and Zhong Z. and Nelakuditi S. (2007). This EAX metric overcomes the aforesaid drawbacks of the ETX metric. For a given pair of source s and destination d, $EAX(s,d)$ computes 2 parts – (a) the expected number of transmissions for successfully relaying a packet to at least one of the candidate next hops and (b) the expected number of transmissions for delivering a packet from that candidate to the destination. It can be noted that for the best-path routing with just one candidate ($i.e.$if the candidate is the destination itself), EAX boils down to ETX. The candidate selection based on the EAX metric is an iterative refinement process where candidates are selected incrementally.

Mingming Lu et al., (2009) defined the Expected Utility under Opportunistic Routing (OpEU) metric. This metric considers the packet-error-rate of the directional link (u, v), the stability term which is concerned with the transmission of a packet by the candidate and the cost term which denotes the transmission power consumed at transmitter u for single transmission to v over the link (u, v) chosen such that it maximizes the expected utility. In Expected Energy Cost metric, defined by Xufei Mao et al., (2011) the Expected Energy Cost needed by OR to send a packet from node u to the target node, $C_u(Fwd)$ considers the minimum transmission power, $t_{u,v}$ incurred by node u to transmit a packet to node v over the link (u, v) in addition to the error probability, e_{uv}, of the link.

On the basis of analysis of EAX, OpEU and Expected Energy cost metrics used in opportunistic routing, it is observed that EAX considers expected number of transmissions between the source and the destination, but does not consider the transmission power incurred and the residual battery energy required. Expected Utility under Opportunistic Routing (OpEU) considers the transmission power incurred, but does not consider the expected number of transmissions and the residual battery energy. Expected energy cost metric considers the expected number of transmissions and the transmission power incurred, but does not consider the residual battery energy. Based on this comparison, it is evident that the Expected Energy Cost metric is better than the other two metrics. However, Expected Energy Cost metric has a drawback in that it does not take into account the residual battery energy at each node. As a result, the same route may be used repeatedly to forward data which would drastically reduce the lifetime of the network as a whole.

An energy-aware routing algorithm presented by Vazifehdan, J. et al., (2011) takes the residual battery powers into consideration and defines the weight, w_{uv}, of the link (u, v) as the ratio of the expected energy (transmission power) consumed by node u to transmit the packet to node v (E_{uv}) and the residual battery energy of node u (B_u). Once w_{uv} is assigned, the minimum cost path to each node is determined using Dijkstra's algorithm. This energy aware routing algorithm, however, is not an OR algorithm as the routes are pre-determined. This would not be appropriate for an application scenario bound to adopt opportunistic routing where the routes are required to be computed dynamically.

2.2. Trust Models

Sergio Marti et al., (2000) have proposed two techniques, namely watchdog and pathrater to deal with misbehaving nodes. The former technique is concerned with the identification of misbehaving nodes while the latter is concerned with avoiding the nodes identified as malicious by the watchdog. The drawback of this protocol is that it does not consider any mechanism to penalize those nodes that behave as selfish nodes.

Liu et al., (2004) proposed a trust model in which each node is assigned a trust level initially and the protocol could be integrated with any traditional routing protocol in Mobile ad hoc networks. But the nodes may behave in a manner to obtain a favourable status until a critical point in time. Pirzada, A. A. et al., (2004) discuss in their paper that the neighbour nodes are monitored during packet forwarding for updating the trust counter. If and when a neighbour forwards a packet, the packet is checked for its integrity by considering two factors. First factor is to verify if a packet can be forwarded and determines the precision of the forwarded packets. The second factor contributes towards identifying any modification attacks in the network.

In the trust mechanism defined by Xiaoqi Li et al., (2004) three components – belief, disbelief and uncertainty are considered along with the opinion of the neighbour nodes to determine the trust factor. Discounting combination is used when A already has an opinion about C, but wants to combine B's opinion about C as well. Consensus combination is used to combine different opinions about one node.

The trust model by Li X. et al., (2010) distinguishes between the control packets and data packets. The packet forwarding ratio is calculated as the ratio of the packets that have been forwarded correctly without any tampering. This forwarding ratio is calculated independently for control and data packets and the trust degree is finally calculated as their weighted sum. This model does not take care of the instability of data transmission through multi-hop nodes.

In Wei Gong et al., (2010) a trust vector with three components is used to represent the trust which is then normalized to get a single value. The first component is the experience component which is determined as the ratio of the packets that are actually forwarded to the packets that the node was responsible for forwarding. The second is the knowledge component that has to do with loss probabilities. The last component is the recommendation component that accounts for indirect trust calculation. A Bayesian based trust model is defined by Sancheng Peng et al., (2008). The trust degree is represented using the beta probability density function, $Beta(\theta|\alpha,\beta)$, where α and β are the amount of positive and negative ratings respectively. This function forms the basis for defining both the direct and indirect trust degrees. The final trust degree is then calculated as the weighted sum of the direct and indirect trusts.

A dynamic trust model is proposed by Hui Xia et al., (2012), where the trust is computed based on only the direct trust which is defined to have 3 parts. The first part is the historical trust, calculated as the weighted sum of the forwarding ratio of the control and data packets. This part also accounts for the trust decay. The second is the current trust which involves predicting the trust value of a node using fuzzy logic based on the existing trust and the node's forwarding capability. The final part is the route trust where the trust value between the source and the destination is calculated. However, this approach of determining the route trust is not possible in Opportunistic Routing as routes are not determined in prior.

Another trust model based on direct and indirect trusts is defined by Wang Bo et al., (2011). The calculation of the direct trust degree makes use of (a) trust aging factor that represents the fading of trust with time, (b) reward factor which is the positive impact for trust in successful interactions and (c) penalty factor which is the negative impact for trust in failure interactions. For the calculation of the indirect trust degree, a node obtains recommendations from similar neighbours. This similarity is calculated using the Pearson-r coefficient which is defined explicitly by Junhai Luo et al., (2008). Finally, the trust degree is calculated as the weighted sum of the direct and indirect trust degrees. Yanli Yu et al., (2012) provide an extensive literature survey and analysis on secure routing and securing data in wireless sensor networks.

It can be seen that all the trust models except those defined by Li X. et al., (2010), Pirzada A. et al., (2004) and Xia H. et al., (2012) make use of recommendations from neighbours. Trust models defined by Xia H. et al., (2012) and Wang Bo et al., (2011) consider decay of trust with time which is incorporated as a decrease in the trust on a node with time. This leads to a possibility that the trust on a node can eventually become null, resulting in its elimination from the network for future transmissions. This gap or possible drawback is overcome with the proposed technique.

Analysis shows that the trust model defined by Wang Bo et al., (2011) provides for an elaborate and rigorous computation of the trust in comparison to the others. It however has a weakness in that it considers only the similarity between a node and its neighbours for obtaining the recommendation as a result of which the original essence of trust is lost. This is illustrated with a simple example scenario with sample data as given in Table 1, where the Similarity and Direct trust components are tabulated.

Node k	**Similarity of node** $i, s(i,k)$	**Direct trust of node** $i, T^d(i,k)$
v_1	0.6	0.9
v_2	0.7	0.6
v_3	0.8	0.6

Table 1. Example scenario depicting similarity factor and direct trust values.

Here, for calculation of indirect trust, m neighbours are selected based on the similarity. The indirect trust of i on k, $T^r(i,k)$, has to be calculated using nodes a, b and c. If $m = 2$, nodes c and b are selected based on their similarity factor. It is observed that node a is not selected, even though the direct trust that node i has on node $a, T^d(i,a)$ is the greatest. This happens when neighbour nodes are selected only based on the similarity factor. Moreover, there also exist some scenario based problems as depicted in Figure 1.

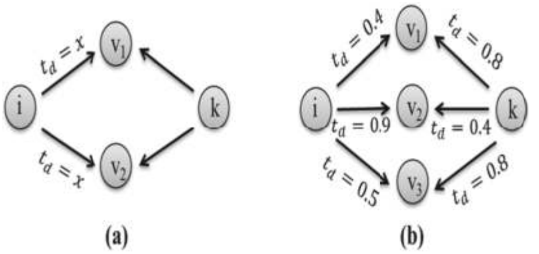

Figure 1. a), b) Scenario depicting effect on direct trust of node *i* on node *k*.

For example, for a node that has the same direct trust on all the nodes common to a trusted neighbour, the Pearson-r coefficient

$$s(i,k)= \frac{\sum\limits_{u\in CN(i,k)} (T^d(i,u)-T_i)*(T^d(k,u)-T_k)}{\sqrt{\sum\limits_{u\in CN(i,k)} (T^d(i,u)-T_i)^2}*\sqrt{\sum\limits_{u\in CN(i,k)} (T^d(k,u)-T_k)^2}}$$

cannot be calculated for determining the similarity between two nodes, *i* and *k*, with respect to their common nodes, $v_1, v_2 \in CN(i,k)$. In other words, when node *i* has the same direct trust $t_d = x$ on both the common nodes v_1 and v_2, similarity cannot be calculated as the standard deviation term at the denominator of the Pearson-r coefficient,

$$\sqrt{\sum_{u\in CN(i,k)} (T^d(i,u) - T_i)^2}, \quad \text{becomes 0.}$$

In order to overcome such scenario based problems and the drawbacks, a better approach for framing a trust model, incorporating both similarity and direct trust, is considered in the proposed trust model to determine the indirect trust.

3. Proposed Framework

A framework for Opportunistic Routing incorporating trust is proposed as depicted in Figure 2. On a logical level, it can be seen to have the following two modules.

(i) Routing Module: Mainly responsible for the selection and prioritization of candidates using the proposed metric that considers the fraction of the residual battery powers required for packet transmission.

(ii)Trust Module: Responsible for the elimination of malicious and selfish nodes. It is based on both direct trust and indirect trust (uses two factors, similarity and direct trust) degrees. It takes into consideration the fact that trust fades (becomes uncertain) with time.

3.1. Routing Module

As analysed in Section 2, using the Expected Energy Cost metric for selecting candidate next-hops has a drawback in that it reduces the lifetime of the network as a whole as the same route may be repeatedly used for packet routing in view of the low energies consumed. Ensuring that the nodes will be alive in the network for the maximum time possible to forward information, will directly help in increasing the lifetime of the network. In order to achieve this, an improvement in the existing Expected Energy Cost metric (Xufei Mao et al., 2011) is incorporated to define the proposed metric as follows,

$$C_u(Cd) = \frac{w + \sum\limits_{i=2}^{Cd^*} \prod\limits_{j=1}^{i-1} e_{uv_j}(1 - e_{uv_i})C_{v_i}}{1 - \prod\limits_{i=1}^{|Cd^*(u)|} e_{uv_i}} \qquad \text{(i)}$$

where, t_{uv} denotes the minimum transmission power required for node u to send a packet to neighbour node v over the link (u,v) and w is set to $\frac{t_{uv}}{B_u}$ such that the chosen t_{uv} minimizes the expected cost, where B denotes the residual battery power. It can therefore be seen that w denotes the fraction of the residual battery power required for transmission. Further, $Cd^*(u)$ denotes the candidate set (forwarder list) that can be reached using t_{uv} in the increasing order of the expected cost and e_{uv} denotes the error probability of link (u,v).

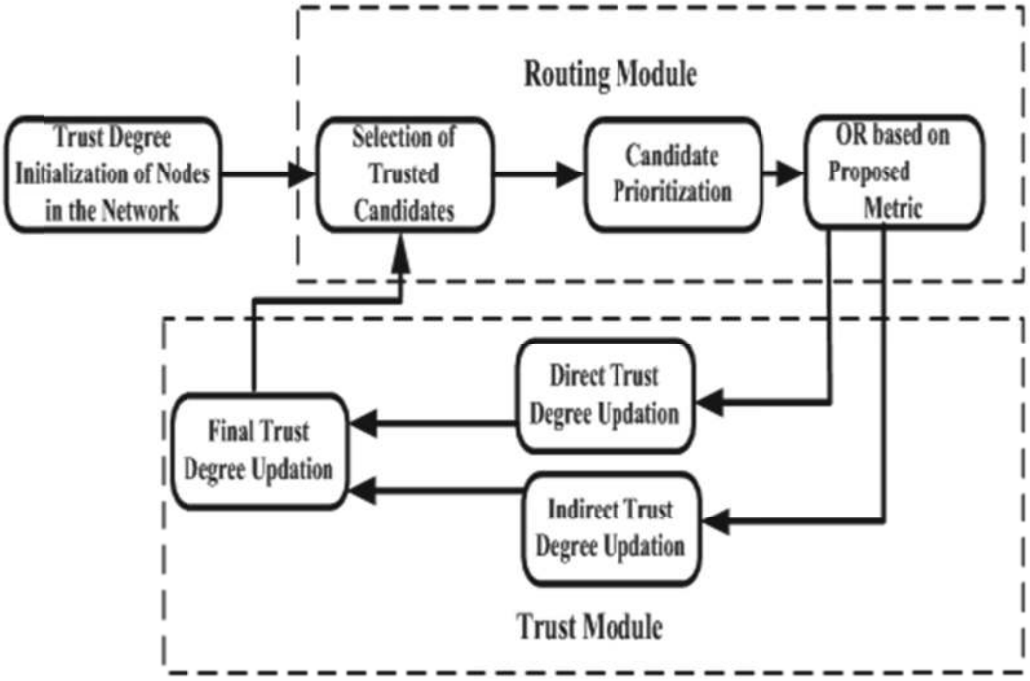
Routing Module
Trust Degree Initialization of Nodes in the Network
Selection of Trusted Candidates
Candidate Prioritization
OR based on Proposed Metric
Direct Trust Degree Updation
Final Trust Degree Updation
Indirect Trust Degree Updation
Trust Module

Figure 2. Proposed framework.

Unlike the Expected Energy Cost metric, the proposed new metric defines the cost as a function of residual battery energies. In eqn. (i), the first part,

$$\frac{w}{1-\prod_{i=1}^{|Cd^*(u)|} e_{uv_i}}$$

denotes the expected energy that node u must consume to send a packet to at least one node in its candidate set, Cd^*, and the second part,

$$\frac{\sum_{i=2}^{Cd^*}\prod_{j=1}^{i-1} e_{uv_j}\cdot(1-e_{uv_i})\cdot C_{v_i}}{1-\prod_{i=1}^{|Cd^*(u)|} e_{uv_i}}$$

denotes the expected total energy for the nodes in Cd to relay the packet to the target considering that v_i forwards the packet on receiving it and v_j, $0 < j < i$ (lower index of v implies higher priority) does not receive the packet correctly. The expected energies in both parts can be seen as the function of the residual battery energies.

The proposed metric defined in eqn. (i) is used for the selection and prioritization of candidate next-hops. The candidate selection is an iterative refinement process where candidates are selected incrementally. A node is added to the candidate set Cd of u only if its addition reduces the value of C_u. In the candidate selection process, C_d is set to 0, where d is the destination node. A sample illustration given in Section 4 describes the step by step candidate selection procedure.

3.2. Trust Module

In order to overcome the vulnerability due to attacks by malicious nodes (that modify network traffic) or selfish nodes (that do not forward traffic from other nodes), a trust model based on both direct and indirect trust degrees is integrated to evaluate the forwarding behaviour of the neighbour nodes.

The direct trust degree, $T^d(i,j)$, that node i has on node j is based on the direct interactions between them in the past. The fact that trust fades with time is taken into consideration. In order to address the issue raised in Section 2.2, the decay factor is defined such that the trust on a node approaches the value 0.5 instead of the value 0 with time. This approach is more applicable as the trust on a node becomes uncertain with time until it is updated next. The Trust-Aging factor

(TA) is defined in terms of exponential decay as follows.

$$TA = e^{-\lambda} \tag{ii}$$

where $\lambda = \frac{\Delta t}{\Delta t+1}$, such that Δt is the period between the current time and the past interaction. Using this definition of TA, in the absence of any transmission from node i to node j during Δt, $T^d(i,j)$ can be defined as follows.

$$T^d_{temp} = \begin{cases} T^d_{old} + ((1 - T^d_{old}) * (1 - TA)) \\ \quad \text{or } 0.5 \text{ whichever is less,} \\ \qquad\qquad T^d_{old} < 0.5 \\ 0.5 \qquad\qquad T^d_{old} = 0.5 \\ T^d_{old} * TA \text{ or } 0.5 \\ \quad \text{whichever is more,} \\ \qquad\qquad T^d_{old} > 0.5 \end{cases} \tag{iii}$$

For example, suppose that node i has a trust value of 0.8 on node j at time 1.0 and there are no subsequent interactions between them. From Figure 3, where the decay of trust with time is presented, it can be observed that the trust value reduces till it reaches 0.5 at time 1.6 ms (and will remain so until any further interaction occurs between the participating nodes). Similar observations can be noted when the trust value is 0.2 at time 1.0 ms. Trust value slowly increases till it reaches 0.5.

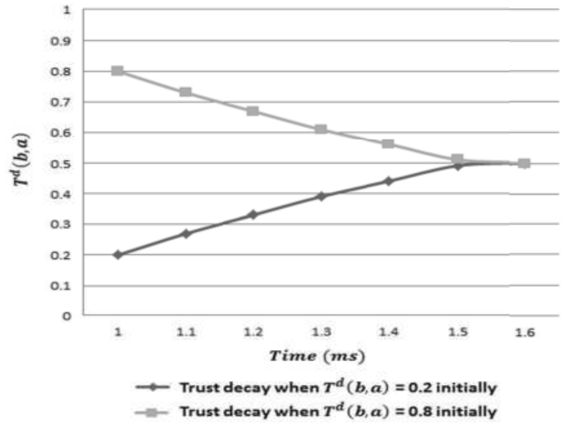

Figure 3. Decay of trust with time.

If, however, there exist any transmissions (successful or failure) from node i to node j during Δt, $T^d(i,j)$ has an alternate definition as follows.

$$T^d_{new} = T_{temp} * w_{old} + SP * w_{new} * TA \tag{iv}$$

where

- T_{temp} is calculated as defined in eqn. (iii)
- $SP = \frac{s}{N}$ is the Success Probability where s is the number of successful transmissions and N is the total number of transmissions from node i to node j during Δt
- w_{old} and w_{new} are the weights given for the earlier calculated trust and the newly calculated trust respectively.

The indirect trust degree, $T^r(i,j)$, that node i has on node j is based on the recommendations from the trusted neighbours of node i. To determine the neighbours whose recommendations have to be considered, two factors are considered (a) the similarity between the node i and its neighbours and (b) the direct trust that node i has on its neighbours.

In order to overcome the scenario-based problem specified in Section 2.2, instead of using the Pearson-r coefficient (as used in Wang Bo et al., (2011)) to calculate the similarity between nodes i and k, $sim(i,k)$, the Euclidean distance (in terms of the direct trusts) is used as follows.

$$sim(i,k) = 1 - e(i,k) \tag{v}$$

where

$$e(i,k) = \sqrt{\sum_{u \in CN(i,k)} (T^d(i,u) - T^d(k,u))^2}$$

denotes the Euclidean distance between nodes i and k. $CN(i,k)$ denotes the number of common neighbour nodes of i and k. $T^d(i,u)$ and $T^d(k,u)$ denote the direct trusts that nodes i and k have on node u respectively. Further, the selection of m neighbours for the calculation of the indirect trust can be done using $wt(i,k)$ the weight factor, which is defined using the similarity between node i and neighbour node k; $sim(i,k)$, and direct trust that node i has on neighbour k, $T^d(i,k)$. This, as can be seen, uses the trust values additionally for neighbour selection and is defined as follows,

$$wt(i,k) = 0.5 * s(i,k) + 0.5 * T^d(i,k) \tag{vi}$$

The neighbour nodes are arranged in the decreasing order of wt and the first m nodes are selected for the calculation of the indirect trust as follows.

$$T^r(i,j) = \frac{\sum\limits_{k \in m} T^d(k,j) * wt(i,k)}{\sum\limits_{k \in m} wt(i,k)} \qquad \text{(vii)}$$

Once the direct trust $T^d(i,j)$ and indirect trust $T^r(i,j)$ degrees are calculated, the total trust degree $T(i,j)$ between node i and node j is calculated as follows.

$$T(i,j) = \alpha * T^d(i,j) + \beta * T^r(i,j) \qquad \text{(viii)}$$

where α and β denote the weight factors for $T^d(i,j)$ and $T^r(i,j)$ respectively such that $\alpha + \beta = 1$. Node i includes node j in its candidate set only if $T(i,j)$ is greater than or equal to the pre-determined $T_{threshold}$.

Selfish and malicious nodes are eliminated by using a trust model based on direct and indirect trust. Candidate next-hops are selected based on the proposed metric, with the aim of minimizing the expected transmission cost C_u.

4. Sample Illustration

An example illustrating the results on using the proposed metric (eqn. (i)) for relaying a packet from source s to destination d for the network depicted in Figure 4 as used in Vazifehdan, J. et al., (2011) is presented.

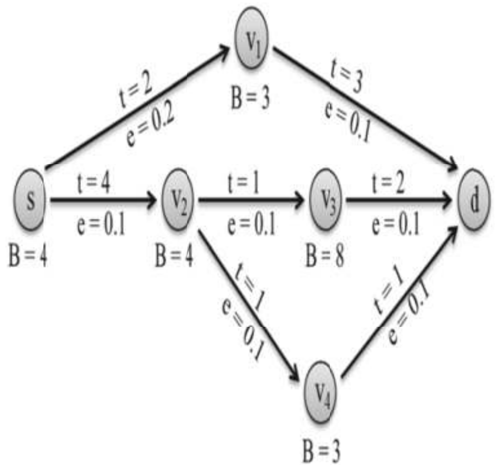

Figure 4. Illustrative example network.

(Note: In Figure 4, B – residual battery energy used to calculate w in each case, t – transmission power and e – error probability of the link.)

4.1. Routing Module

- C_d is set to 0 as d is the destination node.
- d has three neighbours v_1, v_3 and v_4. C_{v_1}, C_{v_3} and C_{v_4} is calculated after calculating w using

  $$\frac{w + (1 - e_{vd}) * C_d}{1 - e_{vd}},$$

  where $v = v_1$ or v_3 or v_4, as 1.11, 0.28 and 0.37 with t equal to 3, 2 and 1 respectively.
- v_2 has two neighbours v_3 and v_4 and both can be reached using $t = 1$. Since, $C_{v_3} < C_{v_4}$, v_3 has a higher priority than v_4. Adding both nodes v_3 and v_4 as candidates gives minimum cost. Hence, C_{v_2} is calculated after calculating w as

  $$\frac{w+((1-e_{v_2v_3})*C_{v_3})+((1-e_{v_2v_4})*e_{v_2v_3}*C_{v_4})}{1-e_{v_2v_3}*e_{v_2v_4}}$$

  resulting in the value 0.54.
- Source s has two neighbours v_1 and v_2. However, only v_1 can be reached on using $t = 2$ while both can be reached on using $t = 4$. Since, $C_{v_2} < C_{v_1}$, v_2 has a higher priority than v_1. Adding both nodes (in order) as candidates using $t = 4$ gives minimum cost. Hence, Cs is calculated (after calculating w) as

  $$\frac{w+((1-e_{sv_2})*C_{v_2})+((1-e_{sv_1})*e_{sv_2}*C_{v_1})}{1-e_{sv_2}*e_{sv_1}}$$

  resulting in the value 1.61

Hence, on the basis of the proposed metric, for the first packet transmission, the path $s \rightarrow v_2 \rightarrow v_3 \rightarrow d$ will be taken when all the nodes are available. If v_3 or v_2 is not available, paths $s \rightarrow v_2 \rightarrow v_4 \rightarrow d$ or $s \rightarrow v_1 \rightarrow d$ will be taken respectively. When the transmission power is not considered in terms of the residual battery power (Expected Energy Cost metric), the path $s \rightarrow v_1 \rightarrow d$ is chosen when all the nodes are available.

4.2. Trust Module

Consider a dynamic network similar to the network in Figure 4 where node v_2 is malicious or selfish. Initially, the trust degree for all the nodes is set to 0.5. According to the metric defined, assuming that the candidates of s include v_1 and v_2 with the latter having a greater priority, s chooses v_2 for the transmission of the first packet at time 0.1 units. After the first transmission, v_2 must be detected as a malicious node and hence s must not use it as its candidate for its subsequent transmissions. Hence, prior to the next transmission at time 0.2 units the trust model is updated as follows (Note: values of the various factors used are presented in Table 2).

- Δt = current time – time of last interaction $= 0.1$
- $\lambda = \frac{\Delta t}{\Delta t+1} = 0.091$
- $TA = e^{-\lambda} = 0.913$
- **Direct Trust**
  - $T^d(s, v_2)$
    - $s = 0; N = 1; SP = \frac{s}{N} = 0;$ $T_{temp} = 0.5$
    - $T^d(s, v_2) = T_{temp} * w_{old} + SP * w_{new} * TA = 0.25$
  - $T^d(v_2, v_3)$
    - $s = 1; N = 1; SP = \frac{s}{N} = 1;$ $T_{temp} = 0.5$
    - $T^d(v_2, v_3) = T_{temp} * w_{old} + SP * w_{new} * TA = 0.75$
- **Indirect Trust**
  - $T^r(s, v_2)$
    - No neighbours of node s have v_2 as their neighbour. Hence, $T^r(s, v_2)$ cannot be updated.
  - $T^r(v_2, v_3)$
    - Suppose that only one neighbour of v_2, i.e. v_4, has v_3 as its neighbour.
    - $sim(v_2, v_4) = 1 - e(v_2, v_4) = 0.7935$
    - $wt(v_2, v_4) = 0.5 * sim(v_2, v_4) + 0.5 * T^d(v_2, v_4) = 0.6468$ which is greater than $wt_{threshold}(0.6)$ and hence is considered.
  - $T^r(v_2, v_3) = \frac{T^d(v_4,v_3)*wt(v_2,v_4)}{wt(v_2,v_4)} = 0.5$
- **Trust degree** (weighted sum of T^d and T^r)
  - $T(s, v_2) = 0.325$
  - $T\,(v_2, v_3) = 0.675$

Factor	Value
w_{old}	0.5
w_{new}	0.5
Weighting Factor for T^d (α)	0.7
Weighting Factor for T^r (β)	0.3
Threshold value of $wt(wt_{threshold})$	0.6
Number of similar neighbours considered for calculation of Indirect Trust (m)	3
Threshold value of $T(T_{threshold})$	0.6

Table 2. Values of factors used in trust model.

Since $T(s, v_2)$ is less than the $T_{threshold}$ (0.6), node s does not use node v_2 as one of its candidates for the next packet transmission. Thus the trust for each node is evaluated and the nodes with trust value greater than the threshold is chosen as a reliable forwarding node.

5. Results and Discussion

The implementation of the proposed prototype is carried using the network simulator (NS-2.34). The network is constructed representing a 6 (5 nodes with 1 destination node: 5+1) node scenario and a 20 (19 nodes with 1 destination node: 19 + 1) node scenario with the maximum buffer size of interface queue being set to 1000 for regular nodes and 2 for attacker nodes. WirelessPhy interface was set to WirelessChannel which is defined in the simulation environment. MAC layer type was MAC/802_11 and Link layer type was LL.

The objective of increasing the network lifetime is met by using the proposed metric in the chosen simulation environment. The results obtained are graphically represented in Figure 5 for the transmission of 9 packets from s to d for the network depicted in Figure 4. The values determined using EAX, Expected Energy Cost and proposed metrics are presented in Table 3.

For the ease of understanding, the transmission powers are maintained unchanged for the transmission of all 9 packets. It can be seen from the results tabulated after the simulations as given in Table 3 that even after the transmission of 9 packets, the proposed metric ensures that all the 5 nodes (excluding d) are alive in the network and are not drained out.

However, the number of nodes alive is reduced to 4 and 3 after the transmission of packets 3 and 9 respectively in case of the Expected Energy Cost metric. Similarly, the number of nodes alive is reduced to 4 and 3 after the transmission of packets 6 and 9 respectively in case of the *EAX* metric.

Similar results are obtained when a network of $19 + 1$ nodes (Figure 6) is simulated for the transfer of 9 packets (Table 3). Initially, the number of nodes alive is considered to be 19 (excluding destination). Using both *EAX* metric and Expected Energy Cost metric reduces the number of nodes alive to 18 and 17 after the transmission of the 6 and 7 packets respectively, leading to the non-existence of routes to the destination for the consecutive packet transmissions.

However, the proposed metric ensures that 18 nodes (excluding destination node d) are still available even after the transmission of 9 packets and a route still exists from the source to the destination node. With a 6 node and a 20 node scenarios we can observe that the proposed metric extends the lifetime of the network and ensures a reliable path between the source and the destination.

The key to this objective is based on identifying the fraction of the residual battery power that will be required to forward a packet to the next hop. Apart from this, the other major factor that is considered is the error probabilities of the links. This factor contributes towards minimizing the number of transmissions required.

In order to prevent any sort of attacks on the participating nodes, the malicious and/or selfish nodes have to be eliminated. This is incorporated by using a trust model prior to the selection of candidates. This work demonstrates a trust model based on both direct and indirect trust degrees considering the fact that trust fades (becomes uncertain) with time. The incorporation of the fading of trust makes use of the concept of exponential decay.

	Number of Nodes (Y-axis)					
	5+1 nodes			**19+1 nodes**		
No. of Packets (X-axis)	***EAX* metric**	**Expected Energy Cost Metric**	**Proposed Metric**	***EAX* metric**	**Expected Energy Cost Metric**	**Proposed Metric**
0	5	5	5	19	19	19
1	5	5	5	19	19	19
2	5	5	5	19	19	19
3	5	4	5	19	19	19
4	5	4	5	19	19	19
5	5	4	5	19	19	19
6	4	4	5	18	18	19
7	4	4	5	17	17	19
8	4	4	5	17 (no routes)	17 (no routes)	19
9	3	3	5	17 (no routes)	17 (no routes)	18

Table 3. Number of nodes alive (excluding destination) in the network using different metrics.

The trust module is implemented in accordance with the trust model proposed in Section 4.2. Node v_2 is configured to be the malicious or selfish node for the network presented in Figure 4. In the absence of a trust model, two subsequent packets take the paths $s \rightarrow v_2 \rightarrow v_3 \rightarrow d$ and $s \rightarrow v_2 \rightarrow v_4 \rightarrow d$ respectively. Once the trust model is incorporated, after the transmission of the first packet, v_2 is detected as a malicious or selfish node and is eliminated for further transmissions. The path $s \rightarrow v_1 \rightarrow d$ is chosen for the transmission of the subsequent packets.

From the simulation results obtained with different network scenarios it is clearly evident that the proposed metric incorporating trust increases the life time of the network by ensuring that a trusted route exists between the source and the destination for data transmission. Moreover, a reliable route is established between the source and the destination in the ad hoc environment and can be scalable to large networks.

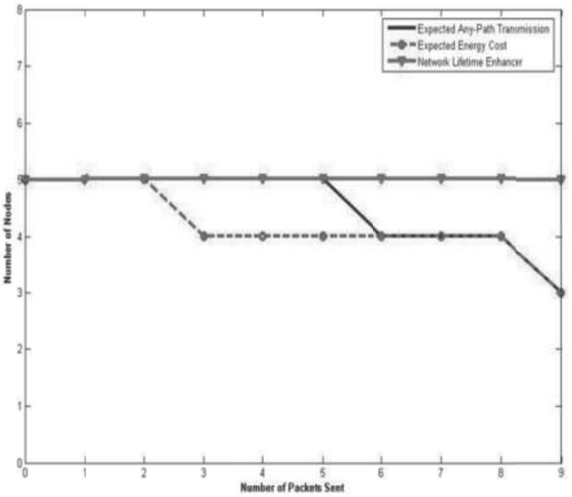

Figure 5. Analysis of the *EAX*, Expected Energy Cost and Proposed metric for a network of 5 + 1 nodes.

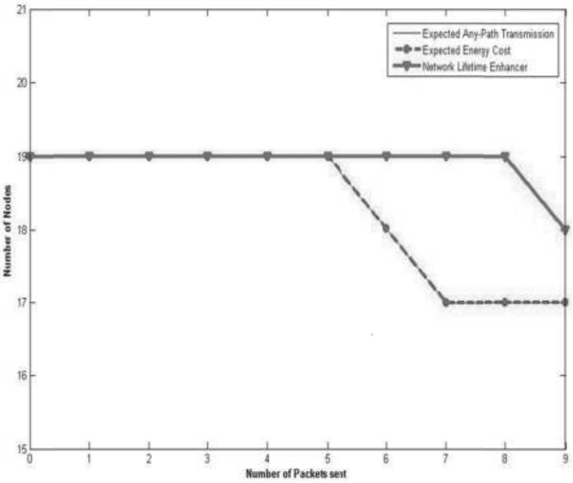

Figure 6. Analysis of the *EAX*, Expected Energy Cost and Proposed metric for a network of 19 + 1 nodes.

6. Conclusions

Various existing metrics for candidate selection using opportunistic routing like *ETX*, *EAX*, Expected Energy Cost and OpEU are analysed and based of the analysis, a new metric is proposed to overcome the gaps identified. Moreover, a modification to the existing trust model based on direct and indirect trust is proposed to enable its applicability in all the scenarios.

The proposed framework provides for an efficient transmission of packets by identifying the nodes with sufficient battery power and ensures that the transmission is reliable and secure on isolating the malicious node in the chosen route. For the transmission of packets in MANETs using OR, candidate selection (and prioritization) is done on the basis of the proposed metric which identifies suitable candidate next hops with the aim of minimizing the number of transmissions for successful delivery of the packets. Selection of the neighbours whose recommendations are considered for the calculation of indirect trust is based on the similarity between the node and its neighbours and the direct trust that the node has on its neighbours. The trust degree is finally calculated as the weighted sum of the direct and indirect trust degrees.

The simulation results obtained clearly indicate that the routing technique based on the proposed metric and incorporation of trust component outperforms the existing techniques in determining the trusted route and extends the lifetime of the network as a whole.

7. Future Enhancements

The current work is focused on increasing the lifetime of the network by selecting the potential forwarding candidates with the fraction of their residual battery power that will be required to forward a packet to the next hop. Also, a trust model prior to the candidate selection is incorporated. As an enhancement to the proposed work, further focus is to determine the delay incurred in transmission of a packet from the source to the destination so as to ensure better quality of service in mobile ad hoc networks.

References

[1] A. Darehshoorzadeh, L. Cerdí-Alabern, V. Pla, Modeling and Comparison of Candidate Selection Algorithms in Opportunistic Routing. *The International Journal of Computer and Telecommunications Networking*, **55**(13) (2011), pp. 2886–2898.

[2] D. S. J. De Couto, D. Aguayo, J. Bicket, R. Morris, A High-Throughput Path Metric for Multi-Hop Wireless Routing. *Wireless Networks*, **11**(4) (2005), pp. 419–434.

[3] H. Liu, B. Zhang, H. Mouftah, X. Shen, J. Ma, Opportunistic Routing for Wireless Ad Hoc and Sensor Networks. *Present and Future Directions, Communications Magazine, IEEE*, **47**(12) (2009), pp. 103–109.

[4] H. XIA, ZH. JIA, X. LI, L. JUA, E. H.-M. SHA, Trust Prediction and Trust-Based Source Routing in Mobile Ad hoc Networks. *Ad Hoc Networks*, Feb 2012 (available online) ISSN 1570-8705.

[5] J. LUO, X. LIU, Y. ZHANG, D. YE AND Z. XU, Fuzzy Trust Recommendation Based on Collaborative Filtering for Mobile Ad Hoc Networks. *33rd IEEE Conference on Local Computer Networks*, (2008), pp. 305–311.

[6] X. LI, P. JIA, P. ZHANG, R. ZHANG, H. WANG, Trust-Based On-Demand Multipath Routing in Mobile Ad Hoc Networks. *The Institution of Engineering and Technology Information Security*, **4**(4) (2010), pp. 212–223.

[7] M. LU, F. LI, J. WU, Efficient Opportunistic Routing in Utility-Based Ad Hoc Networks. *IEEE Transactions on Reliability*, **58**(3) (2009), pp. 485–495.

[8] A. A. PIRZADA, A. DATTA, C. MCDONALD, Trust-Based Routing for Ad Hoc Wireless Networks. *Proceedings of the 12th IEEE International Conference on Networks (ICON 2004)*, (2004), vol. 1, pp. 326–330.

[9] S. PENG, W. JIA, G. WANG, Voting-Based Clustering Algorithm with Subjective Trust and Stability in Mobile Ad Hoc Networks. *IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, EUC '08*, (2008), vol. 2, pp. 3–9.

[10] S. BISWAS, R. MORRIS, EXOR: Opportunistic Multi-Hop Routing for Wireless Networks. *ACM SIGCOMM Computer Communications Review*, **35**(4) (2005), pp. 133–144.

[11] S. MARTI, T. J. GIULI, K. LAI, M. BAKER, Mitigating Routing Misbehavior in Mobile Ad Hoc Networks. *Mobile Communications Proceedings, ACM*, (2000), pp. 255–265.

[12] J. VAZIFEHDAN, R. V. PRASAD, I. NIEMEGEERS, Minimum Energy Cost Reliable Routing in Ad Hoc Wireless Networks. *Consumer Communications and Networking Conference (CCNC), IEEE*, (2011), pp. 781–786.

[13] B. WANG, CH. HUANG, L. LI, W. YANG, Trust-based Minimum Cost Opportunistic Routing for Ad Hoc Networks. *Journal of Systems Software*, **84**(12) (2011), pp. 2107–2122.

[14] W. GONG, Z. YOU, D. CHEN, X. ZHAO, M. GU AND K.-Y. LAM, Trust Based Routing for Misbehavior Detection in Ad Hoc Networks. *Journal of Networks*, **5**(5) (2010), pp. 551–558.

[15] X. LI, M. R. LYU, J. LIU, A Trust Model Based Routing Protocol for Secure Ad Hoc Networks. *Aerospace Conference Proceedings, IEEE*, (2004), vol. 2, pp. 1286–1295.

[16] X. MAO, S. TANG, X. XU, X.-Y. LI, H. MA, Energy-Efficient Opportunistic Routing in Wireless Sensor Networks. *IEEE Transactions on Parallel and Distributed Systems*, **22**(11) (2011), pp. 1934–1942.

[17] Z. ZHONG, S. NELAKUDITI, On the Efficacy of Opportunistic Routing. *SECON'07*, (2007), pp. 441–450.

[18] Z. ZHONG, J. WANG, S. NELAKUDITI, Opportunistic Any-Path Forwarding in Multi-hop Wireless Mesh Networks. *Technical Report TR-2006-015*, USC-CSE(2006).

[19] Z. LIU, A. W. JOY, R. A. THOMPSON, A Dynamic Trust Model for Mobile Ad hoc Networks. *Proceedings of the 10th IEEE International Workshop on Future Trends of Distributed Computing Systems(FTDCS'04)*, (2004), pp. 80–85.

[20] Y. YU, K. LI, W. ZHOU, P. LI, Trust mechanisms in wireless sensor networks: Attack analysis and counter measures. *Journal of Network and Computer Applications*, (2012), pp. 867–880.

Received: February, 2013
Revised: April, 2013
Accepted: May, 2013

Contact addresses:
Sumathy Subramaniam
School of Information Technology and Engineering
VIT University
Vellore-14
India
e-mail: sumi_ravi2002@yahoo.co.in

R. Saravanan
School of Information Technology and Engineering
VIT University
Vellore-14
India
e-mail: rsaravanan@vit.ac.in

Pooja K. Prakash
School of Information Technology and Engineering
VIT University
Vellore-14
India
e-mail: poojamaiya@gmail.com

SUMATHY SUBRAMANIAM is a faculty member in the School of Information Technology and Engineering, VIT University, India. She received her B.E. in Electronics and Communication engineering from Vellore Engineering College affiliated to Madras University in 1995 and M.Tech in Computer Science and Engineering from VIT University in 2002. Her research interests include trust and reliability in wireless networks, routing in mobile ad hoc networks and ensuring QoS in scalable networks. She is a life member of Computer Society of India and of the Indian Society for the Technical Education. She has presented papers in international conferences and has published papers in reputed journals.

R. SARAVANAN is a Senior Professor in the School of Information Technology and Engineering at VIT University, Vellore, India. He received his PhD from Ramanujan Institute for Advanced Study in Mathematics, University of Madras in the year 1998. He has around 19 years of teaching and research experience. His areas of specialization include algorithms and analysis, mobile computing, cryptography and network security and digital image processing. He is a life member of the Computer Society of India and of the Ramanujan Mathematical Society. He has published many papers in various national / international conferences and journals.

POOJA K. PRAKASH is a graduate of M.S. (Software Engineering) in the School of Information Technology and Engineering, VIT University, Vellore. Her areas of interest include wireless networks, software engineering, image processing and trust management in mobile ad hoc networks.