Journal of Software Engineering and Applications, **2013, 6, 319-327**
doi:10.4236/jsea.2013.66040 Published Online June 2013 (http://www.scirp.org/journal/jsea)

Opportunistic Unicast and Multicast Routing Protocol for VANET

Zhizhong Jie, Chuanhe Huang[*], Liya Xu, Bo Wang, Wenzhong Yang, Xi Chen

Computer School, Wuhan University, Wuhan, China.
Email: zzjie@whu.edu.cn, [*]huangch@whu.edu.cn

Received April 16th, 2013; revised May 18th, 2013; accepted May 26th, 2013

ABSTRACT

Vehicular *Ad Hoc* Network (VANET) is a new paradigm of wireless network. Reliable and efficient unicast and multicast routing protocols are critical for VANETs. As a possible solution, opportunistic routing (OR) has received much attention recently. This paper focuses on the aspect of soft security by building trust opportunistic forwarding model in VANET. It incorporates the trust mechanism into OR to enhance the security of routing in resisting malicious attacks. In this paper, we proposed a trusted minimum cost opportunistic unicast routing protocol (TMCOR) and a multicast routing protocol (TMCOM). The simulation results show TMCOR and TMCOM have good throughput, average delay and security gains compared with existing protocols.

Keywords: Forwarding; Degree of Trust; Trusted Opportunistic Routing; VANET

1. Introduction

Vehicular *Ad Hoc* Network (VANET) is becoming an active research area in recent years. VANET is a multihop mobile network designed to offer a wide range of road applications such as safety warning, congestion avoidance and mobile infotainment [1]. VANET has particularly important applications in sparse and rural areas because of the lack of fixed communication infrastructure. That is the reason why routing algorithms appropriate for these circumstances and the design of such a routing protocol is challenging [2,3].

Recently, opportunistic routing has been increasingly recognized by more and more researchers. Opportunistic routing can deal with the lossy, unreliable and varying link quality. The main idea of opportunistic routing is that multiple nodes can potentially be served as the next-hop forwarders instead of pre-selecting a single specific node to be the next-hop forwarder. Once the current node transmits a packet via a single-hop broadcast, all the candidate nodes that have received the packet will determine which one or ones would actually forward the packet according to some criteria (e.g. the one that is closest to the destination will perform the forwarding while the rest will simply drop the packet). As a result, opportunistic routing can take advantage of the potentially numerous unreliable wireless links to forward packet. The most distinct character that opportunistic routing differs from traditional routing is that it exploits the broadcast nature of wireless medium and defers to the forwarder nodes after packet transmissions. This can cope with unreliable and unpredictable wireless links.

There are two main benefits in the opportunistic routing. First, opportunistic routing can combine multiple weak links into one strong link. Second, a traditional routing has to trade off between link quality and the amount of progress that each transmission makes. Opportunistic routing exploits these occurrences to skip some hops and increases the throughput at the same time.

In this paper, we present a trust model based on the concept of trust degree and apply this model to opportunistic routing in VANET. Our model builds a trust relationship for each node with all its neighbors and recommended trust degree. The recommendations improve the trust evaluation process for nodes.

2. Related Work

Biswas and Morris introduced the novel ExOR [4] protocol and showed that network nodes can achieve superior performance than the traditional forwarding by opportunistically forwarding the received data packets [5-8]. introduced several opportunistic routings in wireless net-

[*]Corresponding author.

works. Mingming Lu *et al.* proposed an efficient opportunistic routing [9] and an opportunistic routing algebra based on utility [10]. K. Zeng *et al.* [11] analyzed the end-to-end throughput of opportunistic routing in multi-rate and multi-hop wireless networks, and introduced a multi-rate geographic opportunistic routing in wireless *ad hoc* networks [12]. [13] analysed the efficacy of opportunistic routing. [14] introduced an opportunistic routing in multi-radio, multi-channel and multi-hop wireless networks. In [15], Chachulski *et al.* introduced the MORE opportunistic routing protocol to address issues in ExOR and achieved high throughput in wireless networks. When nodes have malicious behavior, the adoption of such opportunistic routing protocols might reduce network throughput. [16,17] incorporated the concept of trust into VANET including many trust model and secure routing protocols.

The researches on the trust model in MANET have been extensively performed for a wide range of applications in many areas, such as peer-to-peer computing and E-commerce. Sun *et al.* [18] proposed a trust model based on entropy. [19] suggested a semiring-based trust model. Peng *et al.* [18,20] advised a trust model based on Bayesian theory. [21] introduced a trust management framework for mobile *ad hoc* networks.

There are many scholars who focus on secure and trust routing, which can be mainly classified into two categories: cryptographic technique and non-cryptographic technique. The cryptographic technique mainly focuses on traditional safety mechanisms called hard security strategy. These traditional safety mechanisms are not efficient in confidentiality and authentication in VANET. The other non-cryptographic technique is taken into account as auxiliary way to ensure the soft security of routing. There are some solutions to this issue. Watchdog and Pathrater mechanism [22] are two extensions to the DSR algorithm. Sprite [23] is a simple, cheat-proof, credit-based system for MANET.

On the traditional concept in a network, multicast transmission is a transmission from a single source to a group of destination nodes, and multicast transmission in VANET is normally a transmission from a single source to multiple destinations within a specific geographic region. One of the earliest multicast routing protocols in MANET is called On-Demand Multicast Routing Protocol (ODMRP). By maintaining and using a mesh topology, ODMRP provides path redundancy in forwarding multicast packets to all destination nodes. Another routing protocol is Adaptive Demand-Driven Multicast Routing (ADMR) protocol, ADMR uses tree topology in creating multicast trees or links between the sources, receivers and forwarding nodes [24]. [25] proposed a multicast routing and wavelength assignment in WDM networks. And [26] focused on QoS Multicast Routing in *Ad Hoc* Networks.

3. Trust Opportunistic Forwarding Routing

This paper integrates quantitative analysis of cost and the secure factor in opportunistic routing. We can adequately utilize the merits of opportunistic routing and make up the security deficiency of opportunistic routing with trust mechanism, which can be further considered as a guideline to design a high trust VANET.

3.1. Degree of Trust

Trust in entities is based on the fact that the trusted entity will not act maliciously. Trust has the following characteristics: it is subjective (different nodes may have different perceptions of the same node's trustworthiness), asymmetric (two nodes don't need to have similar trust in each other) and time dependent (it grows and decays over a period of time and it is based on previous similar experiences with the same party). In VANET, a trust relationship that formed from direct interactions can be characterized as direct trust. A trust relationship or a potential trust relationship built from recommendations by a trusted node or a chain of trusted nodes, which create a trust path, is called indirect trust. Moreover, the use of recommendations can speed up the convergence of the trust evaluating process. In this paper, the total trust relationship among nodes also contains these two parts.

Definition 1 Direct trust degree is used to indicate that node *i* directly observes its neighbor node *j* with past direct interactions periodically, which is introduced with multiple constraints: time aging factor, reward factor and penalty factor.

The penalty factor is used to distinguish the impact of successful and failed interactions for the evaluation of trust. The successful interaction means the neighbor node not only transmits a packet to its all next-hops, but also forwards devotedly (correct modification if required). The failed interaction means the neighbor node does not forward correctly by launching black hole attacks, greyhole attacks and modification attacks. The purpose of concerning the reward and penalty factor is to encourage cooperation within a VANET by providing some measurements to the benevolent and cooperating nodes. So, direct trust degree can be calculated as follows denoted by $T^d_{\text{new}}(i,j)$:

$$T^d_{\text{new}}(i,j)=\begin{cases}1-TF*T^d_{\text{old}}(i,j) & \left(s=0\ or\ f=0, T^d_{\text{old}}(i,j)>0\right)\\ 1-TF*\left(RF*S-PF*F\right)*T^d_{\text{old}}(i,j)+\left(RF*S-PF*F\right) & \left(s=0\ or\ f=0, T^d_{\text{old}}(i,j)>0\right)\\ 0 & \text{otherwise}\end{cases} \tag{1}$$

where: $0 \le T_{\text{new}}^{d}(i,j) \le 1$, *TF* is a time aging factor, which represents that the trust fades with time during the period Δt, that is, $TF = \Delta t/(\Delta t + 1)$. *RF* is a reward factor, which denotes the positive impact for the trust in successful interactions during the time period Δt. *PF* is a penalty factor, which denotes the negative impact for the trust in failure interactions during the time period Δt. So, *RF* and *PF* satisfy the following conditions: $1 \ge RF > PF \ge 0$, $RF + PF = 1$. Δt is the period between the current time and the time of last interaction and between node *i* and node *j* $(\Delta t \ge 0)$. *s* and *f* denote the amount of successful or failed interactions during the time period Δt, respectively. *S* and *F* are the forwarding successful probability or failed probability respectively. Furthermore, $S = s/(s+1)$, $F = f/(f+1)$. Δt, *RF* and *PF* can be determined according to the practical requirement.

Definition 2 Similarity is referred to the level of similar judging and recommendation ability between node *i* and node *k* to some neighbor node for their trust relationship.

When node *i* and *k* show the higher similarity, they will have the same opinion towards a node, that is, the two nodes have the same recommendation ability for computation of trust degree Here, let *s*(*i*, *k*) denote the similarity of node *i* and *k*, its formula is as follows:

$$s(i,k) = \frac{\sum_{u\in CN(i,k)}\left(T^{d}(i,u)-\overline{T_i}\right)*\left(T^{d}(k,u)-\overline{T_k}\right)}{\sqrt{\sum_{u\in CN(i,k)}\left(T^{d}(i,u)-\overline{T_i}\right)^{2}}*\sqrt{\sum_{u\in CN(i,k)}\left(T^{d}(k,u)-\overline{T_k}\right)^{2}}} \tag{2}$$

Obviously, $0 \le s(i,k) \le 1$. Where *CN*(*i*, *k*) denotes the number of common neighbor nodes for nodes *i* and *k*. $T^d(k, u)$ and $T^d(i, u)$ denote the direct trust degree of node *i*, *k* to *u* respectively. $\overline{T_i}$ and $\overline{T_k}$ denote the average direct trust degree of node *i* and node *k* that are put on their common neighbor nodes in *CN*(*i*, *k*) respectively.

From Formula (2), we can calculate the similarity between node *i* and its neighbor nodes. According to all the similarities between node *i* and its neighbor nodes, we select the most similar nearest-neighbors (the similarity between two nodes should satisfy a certain threshold *τ*, we can choose appropriate *τ* according to the practical application scenario, such as $\tau \ge 0.6$). The *m* most similar nearest-neighbors are sorted in descending order by similarity. The higher of the similarity of neighbors, the more reliable and trusted they give the recommendation information. So, the trust degree between node *i* and *j* can be computed indirectly by node *i* and the m most similar nearest-neighbors. That is, we can calculate indirect trust degree by the nodes' similarity as below.

Definition 3 Indirect trust degree is used to represent the recommendation trust degree by most similar nearest-neighbors. Combining the direct trust degree of most similar nearest-neighbors, we can describe the recommendation trust level more reliably, truthfully and precisely.

We can achieve the formula of $T^r(i, j)$ as:

$$T^{r}(i,j) = \frac{\sum_{k\in m} T^{d}(k,j)*s(i,k)}{\sum_{k\in m} s(i,k)} \tag{3}$$

So, Formula (3) should satisfy the condition obviously: $0 \le T^{r}(i,j) \le 1$.

The neighbor nodes' recommendations improve the trust evaluation process for nodes that do not succeed in observing their neighbors due to resource constraints or link outages. The ability of assessing the trust degree of each node using indirect trust degree by recommendations brings several advantages. Firstly, a node can detect and isolate malicious behaviors, avoiding to relay packets to malicious behaviors. Secondly, cooperation is stimulated by selecting the neighbors with higher trust levels to relay packets.

Considering the above mentioned direct trust degree and indirect trust degree, we put the whole trust degree definition as follows.

Definition 4 Trust degree denotes the sum of direct and indirect trust degree between nodes. It is computed as follows:

$$T(i,j) = \alpha \times T^{d}(i,j) + \beta \times T^{r}(i,j) \tag{4}$$

where *T*(*i*, *j*) denotes the trust degree between node *i* and *j* $(0 \le T(i,j) \le 1)$. *α* and *β* denote the corresponding weighting factors for $T^d(i, j)$ (direct trust degree) and $T^r(i, j)$ (indirect trust degree), they can be determined by practical situation ($\alpha + \beta = 1$). If the current situation of network is prone to estimate the direct trust, we can set up the condition: $1 > \alpha > \beta > 0$. The interactions between nodes are not frequent and every node may not be familiar with each other during the initializing phase of network. The indirect trust degree is not the key point to be evaluated, so the network only considers the direct trust degree for trust degree ($\alpha = 1$, $\beta = 0$). As the network performs consistently in some periods, the trust relationship will be formed from direct trust along with indirect trust. The detailed algorithm is proposed in Section 4.

3.2. Cost of Opportunistic Routing

Definition 5 The cost of a single routing is referred to as an existing feasible opportunistic routing. Let *R* denote all existing opportunistic routing from node *s* to *d*, and $r = (s, n_1, n_2, \cdots, n_k, d)$ is a route in *R*.

$L = \{n_1, n_2, \cdots, n_k, d\}$ denote the trust forwarding list. The cost of *r* relative to *R* denoted by C_r, the sum of the fore link costs in *r*.

$$C_r = \sum\nolimits_{i\in r} d_{i,J(i)} = d_{s,J(s)} + d_{n_1,J(n_1)} + \cdots + d_{n_k,J(n_k)} \qquad (5)$$

where $J(i)$ denotes trust neighbor forwarding list of node $i \in r$. It is important to emphasize that the cost of a single routing depends on the R (that it traverses) because each consecutive fore link cost $d_{i,J(i)}$ depends on the entire trust neighbor forwarding list $J(i)$ rather than on the effective forwarder in $J(i)$ that is used.

Because the single route r may suffer from some influences such as interference of wireless channel, dynamic topology and remaining energy consumption of each node, etc. The r emerges with a certain probability, denoted by $p(r)$. The broadcast nature of wireless network can generate the $|R|$ size of opportunistic routing. So, the cost of opportunistic routing can be calculated by $COR(R)$.

Definition 6 The cost of opportunistic routing $COR(R)$ is the sum of all existing feasible routing cost with an emerging probability across the opportunistic routing. Thus $COR(R)$ is expressed as:

$$COR(R) = \sum\nolimits_{r\in R} p(r) \times C_r \qquad (6)$$

$COR(R)$ denote the cost of opportunistic routing in network. $p(r)$ can be estimated by a number of factors such as the non-deterministic outcome of link layer transmissions, network layer protocol mechanisms and the topology of the network. These depend on the practical conditions of the network (congestion situation, packet sending rate and interference of channels and so on).

3.3. Trust Opportunity Forwarding Mechanism

From the above mentioned definitions, we can derive the minimum cost opportunistic routing by choosing the optimal forwarder and prioritize each node in its trust forwarding list by calculating its cost distance to destination. It can ensure that there is a trust minimum cost routing in all potential routes, and it can also avoid the malicious nodes joining the forwarding list and making malicious attacks. We express the trust opportunistic forwarding mechanism as:

$$\mathrm{Min}_{\forall R} COR(R)$$

where the whole trust nodes is comprised of the trust neighbor forwarding list $J_r \in R(i)$ of each node i in an existing route r. Let $T(i, k)$ denote the trust degree of between node i and k, k in $J_r \in R(i)$, $T(i, k) \geq T_{\text{threshold}}$. $T_{\text{threshold}}$ represents the trust threshold of network. Furthermore, the node that has the higher trust degree and the lowest cost to reach the destination in the $J_r \in R(i)$ is selected as the actual forwarder. As the $COR(R)$ achieves the minimum gradually, trust forwarding list can be formed by selecting the forwarding nodes from the trust neighbor forwarding list of each node in this minimal cost routing.

4. Unicast Routing Protocol TMCOR

We describe the algorithm of Calculating Trust Degree and Updating Direct Trust Degree. We assume that all link delivery probabilities can be evaluated by sending probe packets in the period T. The two algorithms can compute and update the trust degree among nodes in a distributed way. The detailed process is showed in **Algorithms 1** and **2**.

The basis of protocol TMCOR is Trusted Minimum-cost OR, which is depicted in **Algorithm 3**. A Filtering NeighborMNodes algorithm (see **Algorithm 4**) is planned by preventing the malicious nodes or links from being added in trust neighbor forwarding list of node i. The algorithm of Minimum-cost OR (G, d) can obtain the minimum cost route of each node from itself to d in G.

Algorithm 1. Calculating trust degree (*i, j*).

```
Input: node $i$ and its neighbor $j$
Output: T($i, j$)
//Initialize and compute the trust degree between node $i$ and its neighbor $j$.
Node $i$ collects related information to construct the local topology;
Calculate the direct trust degree based on the neighbor table and historical interactive event with neighbor of node $i$;
if there is no interaction between $i$ and its neighbor $j$ then
{
    trust degree of node $i$ and $j$ is initialized by the direct trust degree as $T(i,j) \leftarrow T^d(i,j) \leftarrow 0.5$;
    store the direct trust degree and the current time in the local information table;
}
Else if there is interaction between $i$ and its neighbor $j$ then
{
    Updating DirectTrustDegree ($i, j$);
    Store the direct trust degree and the current time in the local information table ;
    Node $i$ calculates the similar direct trust degree of its neighbors to $j$ by formula (2), the similarity $\tau$ satisfies the condition, $\tau \geq 0.6$;
    Node $i$ calculate the indirect trust degree with its neighbor $j$ by formula (3);
    Calculate the total trust degree of node $i$ and $j$ by formula (4);
}
else
    $T(i,j) \leftarrow 0$;
end if
```

Algorithm 2. Updating direct trust degree (*i, j*).

```
Input: node $i$ and its neighbor $j$.
Output: $T^d_{new}(i,j)$.
//Updating the direct trust degree between node $i$ and its neighbor $j$.
if( (Node $i$ and $j$ are connected) and $T^d_{old}(i,j) > 0$) then
    $T^d_{new}(i,j)$ is updated by formula (1);
else
if ((Node $i$ and $j$ are not connected ) and $T^d_{old}(i,j) \le 0$) then
        $T^d_{new}(i,j) \leftarrow 0$;
else
  Node $i$ collects its neighbors' information by sending HELLO packets during period $T$;
end if
```

Algorithm 3. Trusted minimum-cost OR (*G, d*).

```
Input: graph $G$ and node $d$.
Output: $S$
for each node $i$ in $V$
      do Filtering NeighborMNodes ($G$,$i$)
            $D_i \leftarrow \infty$;
            $F_i \leftarrow \Phi$;
end for
$D_d \leftarrow 0$;
$S \leftarrow 0$;
$Q \leftarrow V$;
while $Q \ne \Phi$       do
     $j \leftarrow$EXTRACT-LEAST-COST($Q$);
        $S \leftarrow S \cup \{j\}$;
          for each edge $(i,j)$ in $E$
               do $J \leftarrow F_i \cup \{j\}$;
               if $D_i > D_j$ then $D_i \leftarrow d_{i,j} + D_j$;
                      $F_i \leftarrow i$;
               end if
          end for
end while
```

Algorithm 4. Filtering NeighborMNodes (*G, i*).

```
Input: graph $G$ and node $i$.
Output: the new graph G($E$,$V$).
for each edge $(i,j)$ in $E$
      if Calculating TrustDegree($i$,$j$) <$T_{threshold}$ then
            $E \leftarrow E$-edge($i$,$j$);
            $V \leftarrow V$-$\{j\}$;
      end if
end for
```

The function EXTRACT-LEAST-COST in Minimum-cost OR (*G*, *d*) indicates that a node having minimal cost to *d* can be selected from the current node sets. In addition, we also keep a trust forwarding list for each node, which stores the nodes as the candidates for the next hops to *d*. Let *S* denote the set of nodes that have a shortest opportunistic routing. *Q* is a priority queue, which stores the nodes that have a shortest opportunistic routing and is keyed by their D_i .The algorithm is described in detail in **Algorithm 3**.

5. Multicast Routing Protocol TMCOM

The purpose of the multicast routing protocol is to efficiently disseminate the message to all appointed vehicles in a timely manner. The problem of finding the routing paths resulting in minimum total required transmissions area while ensuring timely delivery, can be defined as a delay-constrained minimum Steiner tree problem [27]. We can use the **Algorithms 1** and **2** to calculate Trust Degree and Updating Direct Trust Degree in TMCOM. We can also apply the **Algorithm 3** to prevent the malicious nodes or links from being added in trust neighbor forwarding list of node *i*. The algorithm of TMCOM is depicted in **Algorithm 5**. The algorithm of Minimum-cost OR (*G*, *d*) can obtain the minimum cost route of each multicast node from itself to *d* in *G*. The delay constraint function for a pair of vehicles then can be defined as:

$$f_\Delta(i,j)=\left[d_a(i,j)+d_b(i)-d_b(j)\right]/v_j \quad (7)$$

where $d_a(i, j)$ is the actual distance between vehicles *i* and *j*, which can be calculated using Cartesian coordinate that get from GPS, d_b is the braking distance of each vehicle, $d_b = v \cdot t_R + v^2/2 \cdot \alpha$, *v* is the speed of the vehicle, t_R is the reaction time of the driver, and *α* is the maximum deceleration. Let *P*(*s*, *r*) be the set of all possible paths in *G* from node *s* to node *r*. The delay constraint for node *r* for the path *p* is the minimum of the sum of the delay constraint for each pair $\langle i,j\rangle \in p$ [27]:

$$\Delta_r = \min_{p\in\mathcal{P}(s,r)} \left\{ \sum_{\langle i,j\rangle \in p} f_\Delta(i,j) \right\} \quad (8)$$

The core of the multicast protocol is to calculate the multicast tree. The algorithm is depicted in **Algorithm 5**.

6. Simulation and Analysis

6.1. Simulation Environment

Our simulations are based on the IEEE 802.11b of MAC layer, which is included in the NS2. The vehicles move from a random starting point to a random destination along the road (the speed is uniformly distributed between 0 - 20 m/s). The transport protocol is User Datagram Protocol (UDP). Traffic sources are Constant-Bit-Rate (CBR). The source and destination pairs are randomly spread over the entire network. The packet generating rate is 4 CBR. The number of sources is 10 in the network. These scenario files are generated by the scene generator of the simulator. The mobility model is a random way point model in a rectangular field. Each simulation is done in the presence of 1 ~ 20 malicious nodes. The other related parameters are listed in **Table 1**.

6.2. Adversary Model

We simulate the following two types of malicious attacks:

1) Black Hole Attack. The malicious node dumps all data packets that are supposed to forward in this attack. It participates in the process of establishing routes, which is initiated by other nodes to maintain the links connectivity;

2) Gray Hole Attack. The gray hole attack is similar to the black hole attack. The malicious node selectively forwards data packets at random interval. In this paper, we assume that the malicious nodes can randomly drop data packets with a dropping ratio in the range of 0.4 - 0.8.

6.3. Result Analysis

6.3.1. Performance Metrics

We will evaluate the performance of our TMCOR scheme comparing with the classic ExOR protocol in terms of throughput, average end-to-end delay, and security-gains. 1) Throughput: the number of packets transmitted per unit time from the source node to the destination; 2) Average end-to-end delay: the total average delay caused by all the packets that are successfully transmitted; 3) Security-gains: in the aspect of resisting the malicious attacks, the increment of security performance caused by adopting the way.

6.3.2. Results and Analysis

In the following paragraphs we evaluate the performance of TMCOR scheme comparing with ExOR in terms of three metrics: throughput, average end-to-end delay, security-gains.

Figure 1 shows the throughput of the two protocols with different number of malicious nodes. The results show that throughputs of the two protocols are progressively reducing with the number of malicious nodes increasing. However, the throughput of TMCOR scheme (from 176 KB/s to 60 KB/s) is a little higher than ExOR protocol (from 160 KB/s to 40 KB/s). This is because the TMCOR scheme reduces the attack of the malicious node by judging and comparing its trust degree value to prohibit it to join the network.

Algorithm 5. Trusted minimum-cost OR multicast (*G*, *d*).

```
Input : $G(V, E)$ - the interaction graph
        $s$ - the sender
Output: $R$ - the set of receiver nodes
        $\Delta r,\ \forall r \in R$ - TMCOM for every receiver nodes
for each node $i$ in $V$
  do Filtering NeighborMNodes ($G$,$i$);
  unmark all nodes in $V$ ;
$R \leftarrow \varnothing$;
$\Delta s \leftarrow 0$;
$\Delta r \leftarrow \infty,\ \forall r \in R$ ;
create an empty queue $Q$ ;
mark $s$ ;
enqueue ($Q$, $s$) // enqueue $s$ into $Q$;
while $Q$ is not empty do
    $i \leftarrow$dequeue ($Q$) ;
    for $<i, j> \in E$ do
        if   $\Delta j > (f\Delta(i, j)+\Delta i)$ then
         $\Delta j = f\Delta(i, j)+\Delta i$;
              if $j$ is unmarked then
             mark $j$ ;
           $R \leftarrow R \cup \{j\}$ ;
           enqueue ($Q$, $j$); // enqueue $j$ into $Q$ ;
        end if
    end for
end while
```

Table 1. Simulation parameters.

Parameter	Meaning	Value
Area	Road area	1000 m × 80 m
N	Number of nodes	**50**
$\boldsymbol{r}$	Transmission radius of each node	250 m
$\boldsymbol{s}$	Maximum node speed	20 m/s
P	Data packet size	512 bytes
α	Weighting factor of $Td(i, j)$	0.6
β	Weighting factor of $Tr(i, j)$	0.4
Δt	Time interval of trust update	0.5 s
T	Simulation times	200 s
M	Number of malicious nodes	1 ~ 20
Threshold	Threshold of trust degree value	0.5

Figure 2 shows that the security-gains of the TMCOR are increasing with the number of malicious nodes increasing. We measure the security-gains as (TMCOR-TExOR)/TExOR where TMCOR and TExOR denote the network lifetime of the two protocols respectively. The network lifetime is also referred to the longest running time interval as the network suffering from the malicious attacks. The simulation results are shown in **Figure 2**. When the number of malicious nodes is 20, the security-gains attain the maximum 0.85. Because the effective trust mechanism can identify the malicious nodes and prohibits it to be the actual forwarder. Therefore, the connectivity of network can be further enhanced and the process of delivery packets can be effectively performed.

In **Figure 3**, we evaluate the average delay of the two protocols as a function of the speed of nodes. As shown in **Figure 3**, TMCOR scheme achieves a higher average delay than ExOR by 21.9%. This is because TMCOR cost additional delay overhead of ExOR such as collecing information of trust degree, updating the trust degree *et al*.

Figure 4 is the each data point continuous simulation run 10 times after the average results, can see, TMCOM, MORE, ODMRP three protocols with multicast membership increase its throughput decreased gradually, this is because the increase in the number of multicast members with the average successful transmission time is on the increase, and that the throughput of the three protocols slightly reduce. The throughput of TMCOM scheme decreases slowly, because TMCOM is a trusted opportunistic routing multicast protocol, so basically no packet loss. As can be seen in the system throughput of TMCOM scheme is much better than the MORE and ODMRP protocol. The throughput of MORE protocol than ODMRP, because it is not only the network coding and the opportunistic routing thought. Due to MORE on each coded packet transmission, not like TMCOM to make optimal transmission decision, so the throughput of TMCOM scheme is more highly than the MORE protocol.

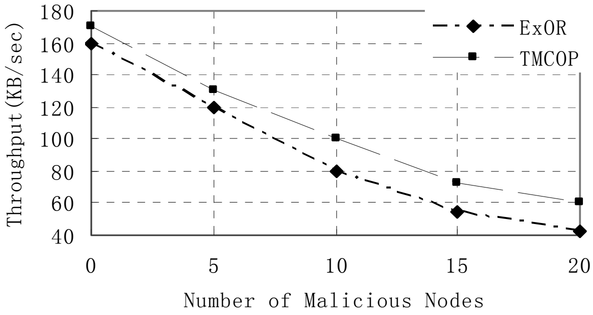

Figure 1. Throughput vs. # of malicious nodes.

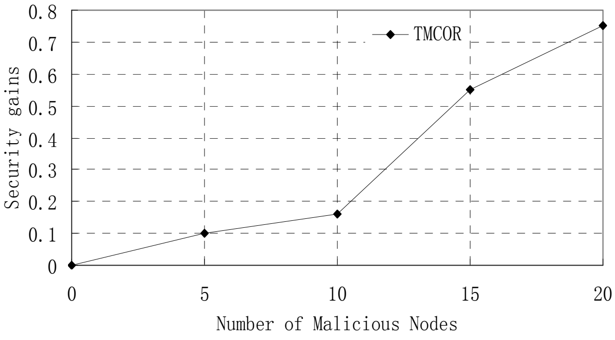

Figure 2. Security-gains vs. # of malicious nodes.

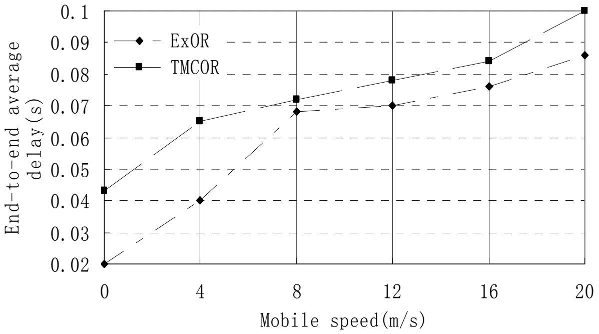

Figure 3. Average delay vs. speed of nodes.

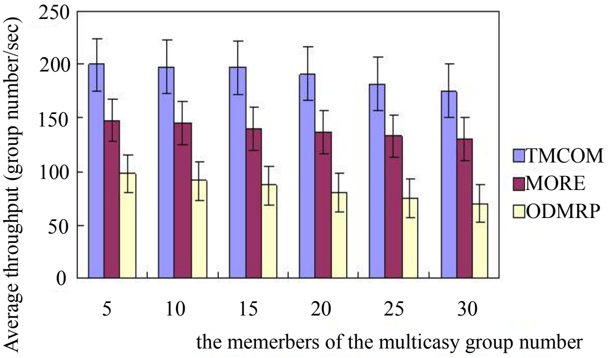

Figure 4. The system throughput contrast.

7. Conclusions

In this paper, we build a trust opportunistic forwarding model based on selecting the optimal forwarder in trust neighbor forwarding list and devise a trusted unicast (TMCOR) and a multicast routing protocol (TMCOM). We also validate the effectiveness of the proposed protocols by nsclick simulator. Simulation results show that TMCOR and TMCOM outperform existing protocol in terms of resisting malicious attacks, cost of routing and throughput.

In our future work, we will conduct extensively simulation and rigorous analysis to verify the performance of TMCOR and TMCOM under real environment. In addition, we will integrate this idea with network coding and QoS assurance for further study.

8. Acknowledgements

The work is supported by National Natural Science Foundation of China (Project No. 60970117, 61173137), Key Project of Natural Science Foundation of Hubei Province (Project No. 2010CDA004) the Ph.D. Programs Foundation of Ministry of Education of China (No. 20120141-110073), Fundamental Research Founds for National University, Wuhan University (Project No. 3104002, 2011211-02020007).

REFERENCES

[1] M. Li, K. Zeng and W. J. Lou, "Opportunistic Broadcast of Event-Driven Warning Messages in Vehicular *Ad Hoc* Networks with Lossy Links," *Computer Networks*, Vol. 55, No. 10, 2011, pp. 2443-2464. doi:10.1016/j.comnet.2011.04.005

[2] X. Yu, H. Q. Guo and W.-C. Wong, "A Reliable Routing Protocol for VANET Communications," 7*th International Wireless Communications and Mobile Computing Conference* (*IWCMC*), Istanbul, 4-8 July 2011, pp. 1748-1753.

[3] M. L. Zhang and R. S. Wolff, "A Border Node Based Routing Protocol for Partially Connected Vehicular *Ad Hoc* Networks," *Journal of Communications*, Vol. 5, No. 2, 2010, pp. 130-143.

[4] S. Biswas and R. Morris, "ExOR: Opportunistic Multi-Hop Routing for Wireless Networks," *ACM SIGCOMM*, Vol. 35, No. 4, 2005, pp. 133-144.

[5] Z. Zhong, J. Wang and S. Nelakuditi, "Opportunistic Any-Path Forwarding in Multi-Hop Wireless Mesh Networks," Technical Report TR-2006-015, 2006.

[6] H. Dubois-Ferriere, M. Grossglauser and M. Vetterli, "Least-Cost Opportunistic Routing," *Proceedings of* 2007 *Allerton Conference on Communication*, *Control*, *and Computing*.

[7] K. Zeng, W. J. Lou, J. Yang and D. R. Brown III, "On Throughput Efficiency of Geographic Opportunistic Routing in Multihop Wireless Networks," *Mobile Networks and Applications*, Vol. 12, No. 5, 2007, pp. 347-357.

[8] E. Rozner, J. Seshadri, Y. A. Mehta and L. L. Qiu, "SOAR: Simple Opportunistic Adaptive Routing Protocol for Wireless Mesh Networks," *IEEE Transactions on Mobile Computing*, Vol. 8, No. 12, 2009, pp. 1622-1635.

[9] M. M. Lu, F. Li and J. Wu, "Efficient Opportunistic Routing in Utility-Based *Ad Hoc* Networks," *IEEE Transactions on Reliability*, Vol. 58, No. 3, 2009, pp. 485-495.

[10] M. M. Lu and J. Wu, "Opportunistic Routing Algebra and its Applications," *Proceedings of INFOCOM*, 2009, pp. 2374-2382.

[11] K. Zeng, W. Luo and H. Zhai, "On End-to-End Throughput of Opportunistic Routing in Multirate and Multihop Wireless Networks," *IEEE INFOCOM*'08, Phoenix, 13-18 April 2008, pp. 816-824.

[12] K. Zeng, W. Lou and Y. Zhang, "Multi-Rate Geographic Opportunistic Routing in Wireless *Ad Hoc* Networks," *IEEE Milcom*, Orlando, October 2007.

[13] Z. Zhong and S. Nelakuditi, "On the Efficacy of Opportunistic Routing," *Proceedings of SECON* '07, San Diego, 18-21 June 2007, pp. 441-450.

[14] K. Zeng, Z. Y. Yang and W. J. Lou, "Opportunistic Routing in Multi-Radio Multi-Channel Multi-Hop Wireless Networks," *IEEE Transactions on Wireless Communications*, Vol. 9, No. 11, 2010, pp. 3512-3521.

[15] S. Chachulski, M. Jennings, S. Katti and D. Katabi, "Trading Structure for Randomness in Wireless Opportunistic Routing," *ACM SIGCOMM Computer Communication Review*, Vol. 37, No. 4, 2007, pp. 169-180.

[16] T. Cui, L. Chen, T. Ho and S. Low, "Opportunistic Source Coding for Data Gathering in Wireless Sensor Networks," *Proceedings of MASS*, ACM, New York, 2007, p. 26.

[17] Y. Sun, W. Yu, Z. Han and K. J. R. Liu, "Information Theoretic Framework of Trust Modeling and Evaluation for *Ad Hoc* Networks," *IEEE Journal on Selected Areas in Communications*, Vol. 24, No. 2, 2006, pp. 305-317. doi:10.1109/JSAC.2005.861389

[18] G. Theodorakopoulos and J. S. Baras, "On Trust Models and Trust Evaluation Metrics for *Ad Hoc* Networks," *IEEE Journal on Selected Areas in Communications*, Vol. 24, No. 2, 2006, pp. 318-328. doi:10.1109/JSAC.2005.861390

[19] S. Peng, W. Jia and G. Wang, "Voting-Based Clustering Algorithm with Subjective Trust and Stability in Mobile *Ad-Hoc* Networks," *Proceedings of the IEEE/IFIP International Conference on Embedded and Ubiquitous Computing* (*EUC* 2008), Shanghai, 17-20 December 2008, pp. 3-9. doi:10.1109/EUC.2008.93

[20] J. Luo, X. Liu, Y. Zhang and D. Ye, "Fuzzy Trust Recommendation Based on Collaborative Filtering for Mobile *Ad-Hoc* Networks," *Proceedings of the* 33*rd IEEE Conference on Local Computer Networks* (*LCN* 2008), Montreal, 14-17 October 2008, pp. 305-311.

[21] J. Li, R. Li and J. Kato, "Future Trust Management Framework for Mobile *Ad Hoc* Networks," *IEEE Communications Magazine*, Vol. 46, No. 4, 2008, pp. 108-114.

[22] S. Marti, *et al.*, "Mitigating Routing Misbehavior in Mobile *Ad Hoc* Networks," *Proceedings of MobiCom*'00. ACM, New York, 2000, pp. 255-265.

[23] S. Buchegger and B. J. Le, "Performance Analysis of the CONFIDANT Protocol: Cooperation of Nodes, Fairness in Dynamic *Ad Hoc* Networks," *Proceedings of the IEEE ACM Symposium on Mobile Ad Hoc Networking and Computing*, ACM, New York, 2002, pp. 226-236.

[24] A. Hassan, M. H. Ahmed and M. A. Rahman, "Performance Evaluation for Multicast Transmissions in Vanet," *IEEE CCECE*, Niagara Falls, 8-11 May 2011, pp. 001105-001108.

[25] X. D. Hu, T. Shuai, X. H. Jia and M. H. Zhang, "Multicast Routing and Wavelength Assignment in WDM Networks with Limited Drop-Offs," *IEEE INFOCOM*'04, 7-11 March 2004.

[26] H. Y. Wu and X. H. Jia, "QoS Multicast Routing by Using Multiple Paths/Trees in Wireless *Ad Hoc* Networks," *Ad Hoc Networks*, Vol. 5, No. 5, 2007, pp. 600-612.

doi:10.1016/j.adhoc.2006.04.001

[27] A. Sebastian, M. L. Tang, Y. M. Feng and M. Looi, "A Multicast Routing Scheme for Efficient Safety Message Dissemination in VANET," *IEEE Wireless Communications and Networking Conference*, Sydney, 18-21 April 2010, pp. 1-6.