International Symposium on Computer Science and its Applications

Truthful and Secure Routing in Ad Hoc Networks

Mehdi Kargar
Department of Computer Engineering
Sharif University of Technology, Tehran, Iran
Mohammad Ghodsi
Department of Computer Engineering
Sharif University of Technology, Tehran, Iran
School of Computer Science
Institute for Research in Fundamental Sciences (IPM), P.O. Box: 19395-5746, Tehran, Iran

***Abstract*—Cooperation among nodes is vital in wireless networks since in such networks nodes depend on each other for routing packets. However, cooperation in such operations consumes nodes recourses such as battery and bandwidth. Therefore, it is necessary to design incentive mechanisms to enforce nodes to forward packets when the source and destination of the packet are other nodes. We study routing in wireless networks from a game theoretic view point. Based on this view, the network consists of greedy and selfish nodes who accept payments for forwarding data for other nodes if the payments cover their individual costs incurred by forwarding data. Also, route falsification attacks are easy to launch by malicious nodes in wireless networks. These nodes falsify data and routes in the network. Thus, mitigating this attack is vital for the performance of the whole network. Previous routing protocols in wireless networks inspired by game theory just consider that network consists of selfish nodes. In this work, we consider that the network consists of malicious nodes too. Here we present a secure and truthful mechanism for routing in wireless networks that cope selfish and malicious nodes.**

I. Introduction

During the last few years we have all witnessed persistently increasing growth in the deployment of wireless networks. A mobile ad hoc network is a infrastructure-less and autonomous network where a set of nodes are connected by wireless links. Each node works as both a router and an end system. Due to the limited transmission range of wireless network interfaces, multiple nodes may be needed for one node to exchange data with another one across the network. Routing is a key issue in wireless networks and it has been the topic of extensive research in the last few years.

Most of the routing protocols assume that all the nodes that make up the wireless network are cooperative, specially they are willing to act as intermediate nodes in a routing path by forwarding data for other nodes in the network as in AODV [1] and DSR [2]. The willingness to cooperate assumption is not reasonable in a general wireless setting because forwarding data for other nodes can exhaust the battery of a node without this node being the source or the destination of the data that it forwards. If the network nodes are owned by a multiple entities and are independent agents, they are indeed selfish. In wireless networks, nodes have limited resources and battery, and forwarding data is resource consuming. Thus, a node may not be spend its resources to forward data for other nodes. Some of other protocols assume that nodes are malicious and they will destroy the network and damage other nodes as in Ariadne [3] and SAR [4]. Malicious nodes falsify packets of other nodes. With these selfish and malicious behavior the wireless network would not work properly [5].

For solving this selfish behavior problem, nodes are given some incentive for data forwarding. Selfish nodes are rational agents since they make decisions consistently to maximize their payoff. By repayment for their cost and some extra money, nodes will be willing to forward data and participate in routing. However, different nodes spend different cost and energy for the same amount of data because they may use different emitting power. Thus they will have different cost for emitting unit power. In addition, the cost of a node could vary over time. This is because the node's battery status. However, for maximizing the payoff, selfish nodes may not reveal their true cost. Thus, we need truthful protocols and strategies for preventing this scenario. For motivating nodes to act truthfully, we should offer some incentives to nodes according to their cost. On the other hand, the sender nodes prefer the lowest routes. Therefore, the sender chooses this path for routing their packets. Detection of malicious nodes is very important for the performance of the network and routing properly. The source node wants a route that does not have any malicious node that falsifies its packets and data. Thus, routes consist only non malicious nodes and pay for intermediate nodes for forwarding data and cooperation in routing.

A protocol is called truthful or strategy-proof if it maximizes the payoff to the nodes only when they reveal their true costs. Thus, selfish nodes have no incentive for cheating about their cost. There exist some truthful routing protocols for wireless networks in the literature [5], [6]. They usually use a model based on the least cost path (LCP). It is known that LCP routing can be implemented in a truthful manner. Also the VCG mechanism is used to calculate the payment to the nodes which is attractive enough for nodes so that they do not have incentive to cheat on their cost [7]. However, these schemes can not handle the existence of malicious nodes in the network. They assume that network only contains selfish nodes which may drop packets to save battery and/or bandwidth but they will not falsify packets. We detect malicious nodes based on a modification of SORI [8], [9] which is a fair reputation

978-0-7695-3428-2/08 $25.00 © 2008 IEEE
DOI 10.1109/CSA.2008.42

mechanism. After detecting malicious nodes, truthful routes will be constructed using non malicious nodes.

The remainder of the paper is organized as follows. Section II reviews the related work. In section III formal statement of the problem is presented. Section IV introduce our mechanism and protocol for secure and truthful routing. The analysis of truthfulness and correctness are discussed in section V. Simulation results is presented in section VI. section VII concludes the paper.

II. Related Work

The problem of nodes cooperation in the wireless networks has been an intense research area in the last few years [6], [10], [11], [12]. Buchegger and Le-Boudec presented CONFIDANT protocol to isolate and detect misbehavior and selfish nodes [13], [14]. Based on own observation and neighborss observation, CONFIDANT monitors nodes behavior, reports warning messages to neighbors and estimate nodes reputation. Michiardi and Molva proposed an algorithm, CORE, to evaluate and validate reputations [15]. CORE uses a combination of three reputation: subjective, indirect and functional reputation for measuring a nodes contribution to the wireless network.

Marti et al. presented watchdog and pathrater for mitigating routing misbehavior and selfish nodes in ad hoc networks [16]. Watchdog is used to recognize selfish and malicious nodes and pathrater is used to choose a route that does not contain them. Security extensions to DSR by relying on neighbors monitoring routing packets context to recognize the malicious nodes is presented in [17]. Miranda and Rodrigues suggested that nodes are allowed to openly announce that they do not forward messages for some nodes [18]. A distributed algorithm for providing fairness to nodes, specially to solve the location privilege the counting retransmission problems is presented by Wang et al. in [19].

The use of virtual money which is called nuglet or credit for stimulating nodes cooperation has been suggested in [20]. A node earns nuglet or credit by providing routing packets to others and has to pay to get services from other nodes. To protect the nuglets or credit value from attacks and modification some security modules independent of nodes are used. Ben Salem et al. presented a rewarding and charging scenario in wireless networks. Using base stations, the scenario combines symmetric cryptography with nuglet [21]. Thus, it can prevent some attacks and refusal to pay and dishonest rewards. Fratkin et al. propose a method that uses a trusted banker node to assure the payment solidification [20]. Also, it assures integrity for virtual money scenario. Crowcroft et al. presented a pricing model where nodes update their cost based on power usage and bandwidth [22]. Sprite system for motivating cooperation among nodes is proposed in [11]. Every node sends a receipt which is the digest of received or forwarded packets, to a central service that is called Credit Clearance Service (CCS). Then, the CCS identifies the charge and credit to each node involved in the forwarding phase.

Mechanism design was introduced to solve the selfish nodes problem. Anderegg and Eidenbenz presented the ad hoc-VCG routing protocol for ad hoc networks with selfish nodes [6]. This is a truthful and cost-efficient protocol for data transmissions. It uses the VCG mechanism and it needs $O(n^3)$ control messages for a route discovery. Recently Wang and Singhal proposed LOTTO protocol that finds a least cost path for data forwarding with a lower routing overhead of $O(n^2)$ [5].

Zhong et al. provided CORSAC, a truthful routing protocol which combines the cryptography and the VCG mechanism [23]. The message overhead of this protocol is $O(\rho \times E \times n)$, where n the number of nodes, E the number of edges or links and ρ is the number of power levels. Chen and Nahrstedt presented iPass [24]. iPass is an auction system where nodes get forwarding services by bidding in the intermediate nodes. Cai and Pooch provided another method that is called TEAM [12]. It is a truthful method but the payment to the intermediate nodes may not cover their cost and nodes may have no incentive to forward packets. Also, the sender saves nothing and gets worse service due to more hops used. Eidenbenz et al. presented a VCG protocol named COMMIT [25]. It allows a source to set a reserve price for its data transmission to a destination. COMMIT incurs an overhead of $O(n^2 \times \log n)$ using underlying topology control protocols. It assumes that a node incurs the same cost to send packets to different neighbor nodes.

Many secure on-demand routing protocols, such as ARAN [26] , SAODV [27], SRP [28], Ariadne [3], SDSR [29] and SORI [8], are proposed for mobile ad hoc networks in the literature. ARAN and SAODV are are based on AODV, while SRP, Ariadne, and endairA, and SDSR are are based on DSR. Here we discuss some of them.

In ARAN protocol, source node signs the request packets before broadcasting it. Each node in the path verifies the signature of the previous node. Then, it replaces the signature of the previous node with its signature of the packet, and rebroadcast the new packet. At the end, the destination node verifies the signatures of its previous node and the source node. The security mechanisms used for reply packets are similar.

SAODV uses two security mechanisms. First digital signatures to authenticate the non mutable fields of request packet and request reply packet. Second it uses hash chains to secure the mutable information. Because of the shortcoming of one way hash chain mechanism, SAODV can not prevent a malicious node from forwarding a route reply with the same hop count as in the route reply it receives.

The SRP requires security verification only between source and destination of a route using MAC for route request and route reply packets. Because SRP does not use any authentication of the intermediate nodes in both route request and route reply process, it makes the protocol more light-weight, but more vulnerable to attacks by malicious nodes.

The secure and objective reputation-based incentive scheme for ad-hoc networks (SORI), introduced in [8] focuses in the packet forwarding function. SORI consists of three main components: Neighbor Monitoring, Reputation Propagation and Punishment. Every node monitors the behavior of its neighbors and maintains a local record based on this observation. With reputation propagation component, local and global reputation information is combined and non-cooperative nodes will be punished by punishment component. We use a modification of SORI for detection of malicious nodes.

III. Formal Statement of the Problem

We design a protocol that routes packets along a path which is Least Cost Path (LCP) and it does not contain malicious nodes. Also, our protocol is truthful. The setting and scenario that explained above is very well suited for analysis by means of game theory, more specifically by mechanism design. The purpose of a mechanism design problem is to define and explain a game. This game should be played in such a way that the outcome of the game played by independent agents according to the rules set by the mechanism designer will be the preferred outcome. This outcome is called the social optimum. The game should be designed based on the dominant strategy and results in the social optimum. The dominant means that no player has no incentive to lie and deviate from the strategy. The final state is called dominant-strategy equilibrium if all players playing dominant strategies in the game. The purpose of a mechanism designer is to define rules that results in a dominant-strategy equilibrium [30]. Then, we define a mechanism design problem, a mechanism, truthful mechanism and VCG mechanism according to Nisan [30].

Mechanism Design Problem

- There are n agents. Each agent i, $i \in \{1, \ldots, n\}$, has some private information t_i , called type. Other values and information are openly known.
- There is an output specification that maps to each type vector $t = (t_1, \ldots, t_n)$ to a set of allowed output o.
- Each agents i has its own preference over all outputs. The preference is given by a function $v_i(t_i, o)$. This is called its valuation function and is a real number from output o when its type is t_i . If the mechanisms output is o and the payment to agent i is p_i , agent is utility is $u_i = p_i + v_i(t_i, o)$. Every agent seeks to maximize this utility.

Mechanism

- A mechanism defines a set of strategies A_i for each agent i. Each agent selects a strategy a_i from A_i . For each input vector $(a_1, \ldots, a_n)$, the mechanism calculates an output $o = o(a_1, \ldots, a_n)$ and a payment vector $p = p_i(a_1, \ldots, a_n)$ for each agent.

Truthful Mechanism

- A mechanism is called truthful or strategy-proof if an agent i maximizes its utility $u_i = v_i(t_i, o) + p_i$ by giving its true private type t_i regardless of what other agents do. On the other hand, truth-telling is a dominant strategy.

VCG Mechanism

- A mechanism $m = (o(t), p(t))$ is a VCG mechanism if the following statements hold. The output $o = o(a_1, \ldots, a_n)$ maximize the total welfare $\sum_{i=1}^{n} v_i(t_i, o)$ and the payment is calculated according to VCG formula $p_i(t) = \sum_{i \neq j} v_j(t_i, o(t)) + h_i(t_{-i})$. t_{-i} identifies the vector of types of all agents except i and h_i is an arbitrary function of t_{-i}.

Given a set of cost, the least cost path can be computed using the Bellman-Ford or Dijkstra algorithm. However, for preventing nodes from lying about their cost, a truthful mechanism should be used The problem can be described as what follows. A network is a biconnected graph $G = (V, E)$. Each edge or link e of the graph is an agent and has type $t_e \geq 0$. This type is the agents cost for sending a single packet along this edge. The mechanism design goal is to find an output LCP between source , s, and destination , d, nodes. Nisan and Ronen proved that the following mechanism is truthful. The payment p_e given to agent e is 0 if e is not on the LCP and $p_e = d_{G|e=\infty} - d_{G|e=0}$ if it is on the LCP. In this context $d_{G|e=\infty}$ is the length of the LCP which does not contain e and $d_{G|e=0}$ is the length of the LCP when the cost of e is assumed to be zero. Later Feigenbaum et al. [7] proved that this is applicable when nodes are agents.

We consider a wireless network as a directed weighted graph $G = (V, E, W)$. V is the set of nodes in the network, or agents in the mechanism design. E is the set of wireless links (edges) between nodes. W is the set of weights for each link, determining the cost to forward a packet along that link. Each link might have different weight since a node has different cost to forward a packet to different neighbor nodes. On removing any node and its incident links, the graph is still connected. Thus, the wireless network is biconnected. A node v_j within radio range of node v_i is presented as link (v_i, v_j). The power consumption is used as a basis for evaluating the cost of links. The weight w_{ij} of link (v_i, v_j) is assumed as the product of v_is emitting power P_i^{emit} and its cost of unit power c_i. On the other hand, $w_{ij} = P_i^{emit} \times c_i$. It should be noted that control messages are sent with maximum emitting power. Thus, they will reach more nodes. For data transmissions, the sender sends packets using the least power with which the receiver can receive the packets. A sender can choose its emitting power P^{emit}. This power identifies the radio range. According to the wireless propagation system, the signal strength received by the receiver j is $P_{i,j}^{rec} = (K \times P_i^{emit})/(d^{\alpha})$, where K is a constant and $\alpha \in [1, 6]$ is the distance-power gradient depending on the environment condition. If $P_{i,j}^{rec}$ exceeds a threshold P_{min}^{rec}, then j can receive the data properly. A receiver j can estimate the minimum emitting power needed for the sender i to forward data to it using the transmitting power P_i^{emit}. Thus, the minimum emitting power would be $P_{i,j}^{rec} = (P_i^{emit} \times P_{min}^{rec})/(P_{i,j}^{rec})$.

For stimulating the cooperation among nodes, the protocol will use virtual money. If a node forward data for other nodes, it will earn money. The source node will pay the cost of the route. The payment includes the cost of data transmissions, control messages and some extra money as bonus. The cost for data transmissions is the sum of links cost along the LCP. Nodes of the network are selfish and rational. They want to maximize their utility and payoff. Thus, they may declare their cost untruly. It should be mentioned that some of the nodes destroy the network or attack other nodes. In other words, they are malicious. Thus, one of other tasks of this work would be finding them and preventing routing from them. In this paper, we focus on designing a truthful routing protocol. We will assume that there is no collusion between nodes. Other issues such as transferring money, securely crediting and the bootstrap of the virtual money are out of scope of this work. We assume a payment scenario [11] that handles the accounting and transferring of payment between nodes. Also, a tamper-proof hardware can be used to prevent virtual money from attacks and modification [20].

IV. Secure and Truthful Routing Protocol

In this section we present our secure and truthful routing protocol for ad hoc networks. The proposed routing protocol is a reactive routing protocol. It only takes action and starts computing routing paths when a network node starts a session. After detecting and removing malicious nodes, the proposed protocol computes the LCP and then routes the data packets from source to destination along the LCP. Thus, the protocol consists of four phases. These are detecting malicious nodes, route discovery, data transmission and route recovery. In the next sections, each phase is presented in detail.

A. detecting malicious nodes

For detecting malicious nodes, a modification of SORI is used [8]. It is assumed that nodes are in promiscuous mode. It means that they listen to every packet transmitted by their neighbors even if the packet is not intended for them. Also, a packet can be received by all nodes that lie in the transmission range of the sender. Each node N maintains two local records based on forwarding operation of its neighbor G. The $R(G)$ (request for forwarding) indicates the number of packets node N has transmitted to node G to forward. $H(G)$ is the number of packets node G has correctly forwarded. Each node N creates a record $L(G)$ which contains node N's opinion about node G's reputation. It is indeed the proportion of packets correctly forwarded by node G, $L(G) = H(G)/R(G)$. Thus, each node maintains the reputation of its neighbors. If $L(G)$ is less than a threshold, then node G is considered as a malicious node and nodes will avoid sending data from this node. In this paper the threshold is equal to 0.8.

B. Route Discovery

In the route discovery phase, the LCP is computed from source to destination. It is basically based on [6]. Whenever a source node v_0 wants to communicate with a destination node v_n, it initiates the route discovery phase by broadcasting a RR (Route Request) packet to the network. This packet contains the following data. The unique identifier 0 of the source node, the unique identifier n of the destination node, a sequence number $s_{0,n}$, the cost of energy c_0 and the emission power P_0^{emit}. Every node v_j except source and destination that receives the RR packet from a node v_i performs the following process.

- If this is a fresh packet and it is not received previously based on its sequence number, the next step is preformed, otherwise drop it.
- If node v_i is a malicious node, based on $L(v_i)$ the packet is dropped, otherwise the next step is preformed.
- Determine power $P_{i,j}^{rec}$ at which the packet was received to the node. Then, compute minimum power required for node v_i to transmit to node v_j as $P_{i,j}^{min} = (P_i^{emit} \times P_{min}^{rec})/(P_{i,j}^{rec})$.
- The emission power P_i^{emit} is replaced by $P_{i,j}^{min}$ in the RR packet. Then the unique identifier j, the emission power P_j^{emit} and the cost of energy c_j is appended to RR packet and the packet is rebroadcasted by node v_j.

Destination v_n collects the arriving packets. It should be noted that destination v_n removes the packets that received from malicious nodes. After creation of the network as the graph $G = (V, E, W)$, v_n computes the LCP from v_0 to v_n, as $v_0, v_1, \ldots, v_{n-1}, v_n$. On the existence of more than one shortest path, the destination would select one of them randomly. Because the malicious nodes are removed in the route discovery phase, the network and related graph would not have any malicious node.

Let $|LCP|$ identifies the total cost of the LCP. For computing the VCG payments to the intermediate nodes, the destination also calculates for each intermediate node i the least cost path LCP^i from v_0 to v_n that does not contain node v_i as an intermediate node. The VCG payment to intermediate node v_i is indicated as p_i. It is computed as $p_i = |LCP^i| - |LCP| + (c_i \times P_{i,i+1}^{min})$. Indeed, p_i is the difference of the cost of the LCP from v_0 to v_n, if node v_i did not exist, and the cost of the LCP from v_0 to v_n without the cost incurred by v_i. It should be noted that $c_i \times P_{i,i+1}^{min}$ is the cost that incurred by node v_i and the difference $|LCP^i| - |LCP|$ is the bonus that v_i receives to reveals its cost truthfully.

For clarifying the process of computing the payments, an example is presented in Figure 1. This network consists of 8 nodes (agents). Node $Source$ wants to communicate with node $Destination$. Node Z are detected as malicious node by node $Destination$ based on $L(v_z)$ of node $Destination$. It should be mentioned that the value of $L(v_z)$ of node C does not have any effect on the routing process. It is because that node C receives the packet with sequence number $s_{0,n}$ from node $Source$. Thus, it just removes the packet form node Z with sequence number equal to $s_{0,n}$ in the first step of route discovery and it would not consider that whether node Z is malicious or not. Also node X are detected as malicious node by node D in the same way. Thus, nodes X and Z can not participate in the process of route discovery. Node $Destination$ collects the arriving packets and creates the network and computes the LCP from $Source$ to $Destination$. The LCP is $LCP = Source, A, B, Destination$ and the cost of this path is $|LCP| = 4 + 1 + 2 = 7$. The LCP without nodes A and B are $LCP^A = Source, C, D, Destination$ and $LCP^B = Source, A, D, Destination$ respectively. The

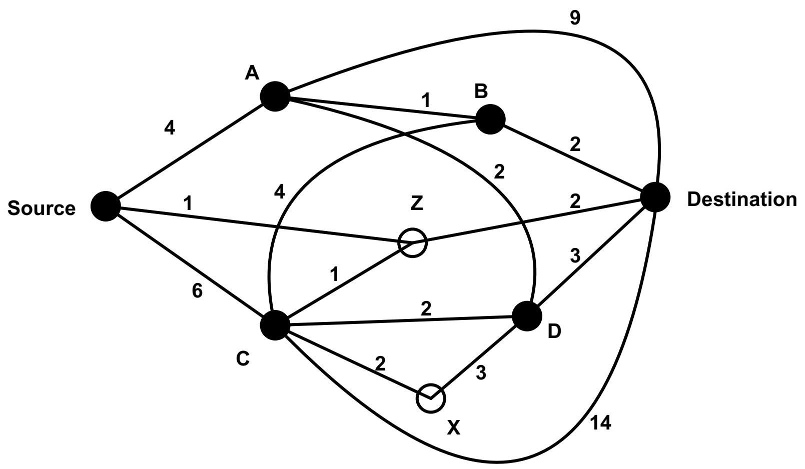

Fig. 1. The network consists of 8 nodes. Nodes X and Z are malicious nodes. node $Source$ wants to send data to node $Destination$. The LCP from $Source$ to $Destination$ is $LCP = Source, A, B, Destination$ and the cost of this path is $|LCP| = 4 + 1 + 2 = 7$.

costs of these paths are $|LCP^A| = 6 + 2 + 3 = 11$ and $|LCP^B| = 4 + 2 + 3 = 9$. Thus, the VCG payments to intermediate nodes A and B are $p_A = 11 - 7 + 1 = 5$ and $p_B = 9 - 7 + 2 = 4$.

After computing the LCP and payments, destination node creates a RP (route reply) packet and sends it back along the reverse LCP to the source node. It contains the unique identifier of the nodes in the LCP, VCG payments and minimum required transmitted power. It should be noted that destination node signs the packet to prevent it from modification. Each of n nodes in the network might broadcast $O(n^2)$ RR packet and it results in $O(n^3)$ packets in total. This is similar to what is stated in [6]. However, using the techniques in [5], the number of packets can be reduced to $O(n^2)$ and the performance of the network is improved.

C. Data Transmission

In the phase of data transmission phase, packets are sent along the LCP form source to destination. Also, all nodes send packets using the minimum power required to forward the packages to the next node. In addition, source node adds the payments to the intermediate nodes to the packets. There are several solutions for making these payments. One of them provides this service using a tamper proof hardware item that is included in the communication device and the money is stored in there [6]. Another solution requires a a universally accepted financial institution. This institution provides digital money that can be transferred from one node to another node. Other issues are out of the scope of this paper.

D. Route Recovery

Link breakage might happen during data transmission. It is because of the node mobility or failure of the nodes. In addition the cost of a node may increase or decrease over the time. Thus, the previous payments is not valid any more. In such cases, the corresponding node sends a RE (route error) packet to the source. After receiving the RE packet, the source starts a new route discovery to find a new LCP to the destination.

V. Truthfulness and Correctness

In this section we will show that the proposed mechanism is truthful and works properly. It should be mentioned that there is no collusion between nodes. The weight of an edge or link (v_i, v_j) is computed by the sender node v_i and the receiver node v_j. We will prove that truthfulness and revealing the true costs and emission power is the dominant strategy. It should be noted that the malicious nodes are removed from consideration in the route discovery phase. Malicious nodes might falsify packets and destroy the network. After removing these malicious nodes, we can focus on non malicious nodes. Thus, in the remaining parts of the analysis, it is assumed that malicious nodes are detected and removed and we just have selfish and non malicious nodes in the network. Selfish nodes want to maximize their utility. We will show that over declaration or under declaration for both nodes v_i and v_j does not increase their utility.

Receiver node v_j should declare the estimated of minimum emitting power $P_{i,j}^{min}$. We will show that declare the true value of this parameter will be the best strategy for node v_j. If v_j under declares $P_{i,j}^{min}$, the LCP might pass through it. But the v_i uses a lower power to send data and packets to v_j. Therefore, v_j will be out of the radio range of v_i and v_j will not be able to forward packets and it will get payment.

If receiver node v_j over declares $P_{i,j}^{min}$, the path through v_j is made more expensive. Thus, the LCP might not go through edge (v_i, v_j). If (v_i, v_j) is still on the LCP, v_js over-declaration increases the cost of the path $|LCP|$. However, based on the equation for computing the payment to the intermediate nodes, since w_{ij} and $|LCP^j|$ do not change while $|LCP|$ is increased, v_j will get less payment than it gets when it tells the true value of $P_{i,j}^{min}$. Thus, receiver node v_j has no incentive to lie about $P_{i,j}^{min}$.

We show that the payment that the sender node v_i gets, will not increase if it lies about its cost c_i or emission power P_i^{emit}. There are two cases. First node v_i under declares its emission power or its cost. It mights claim that its emission power is P_i^{*emit} while it is actually P_i^{emit} ($P_i^{*emit} > P_i^{emit}$), or it mights claim that its cost is c_i^* while it is actually c_i ($c_i^* > c_i$). By under declaring these values, (v_i, v_j) appears cheaper. Because the payments to the intermediate nodes are computed according to above equation, this does not increase the utility of v_i. If v_i is on the LCP with P_i^{emit} and c_i, then it still is on it with either under declaration of P_i^{*emit} and c_i^* and v_i receives the same utility in both cases and has the same cost. If v_i is not on the LCP with P_i^{emit} and c_i and moves itself onto the LCP by under declaration of these values, the utility of v_i becomes negative as it will incur costs that are higher than the payment it gets.

Also, v_i can over declare the emission power or or its cost-of-energy, ($P_i^{*emit} < P_i^{emit}$) and ($c_i^* < c_i$). These makes (v_i, v_j) to appear more expensive. If v_i is not on the LCP by declaring the truth, then it will not move by over declaration. If v_i is on the LCP when declaring the true values, it might either no longer be on it by over declaring or it might still be on the LCP, but the payment that it gets does not change according to the above equation.

VI. Simulation Results

In this section the results of our simulation is presented. The protocol is not compared with generic routing protocols such as DSR and AODV because their models are different. They assume that all nodes are obedient and they do not act selfishly. However, our protocol is based on the assumption that nodes may act selfishly and maliciously. Also, we can not compare with game theoretic based protocols such as Ad hoc-VCG because we assume that some nodes are malicious. In the simulation study, we consider that following parameters.

- **Overhead** Overhead is defined as the total protocol control messages exchanged by nodes in the wireless network. These are RR, RP and other control messages.
- **Delay** Delay is the average source to destination delay of data packets.
- **Packet delivery ratio** This is the percentage of the total number of packets received by destination to the total number of packets broadcasted by all nodes.
- **Energy consumption** This is the total energy or power consumed for broadcasting all packets in the wireless network.
- **Overpayment ratio** This is the ratio of total payment to the intermediate nodes paid by all source nodes in the network plus the cost of the source nodes to total cost all nodes incurred for transmission of packets.

Glomosim is used as our simulation environment [31]. Number of nodes are varies between 50 and 70 nodes. They placed uniformly in a square area of $500m \times 500m$. We used 802.11 protocol with default values for different parameters. Four levels of power emission is used. They are $1, 3, 5, 7dBm$, corresponding to the radio range of $125, 158, 198 and 250m$, respectively. It should be noted that the routing messages were always sent with the highest power level. All nodes in the network have same cost of unit power and followed the Random Way point mobility model. The speed range is set to $010m/s$ with the pause time equal to $30s$. The duration of each simulation is set to $1100s$. it starts at $50s$ and ending at $1000s$. Percentage of malicious nodes is set to 10%.

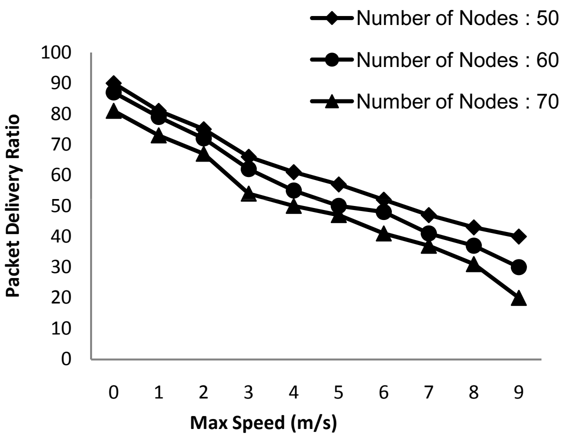

Fig. 2. Performance Under Different Malicious Strategies

A. Packet delivery ratio

Figure 2 shows the packet delivery ratio for different number of nodes and maximum speed. It suggests that when the number of nodes increases, the packet delivery ratio decreases. Also when maximum speed increases, the packet delivery ratio decreases. It is because that when the network mobility increases the possibility that a path established and makes available decreases. Thus, the packet delivery ratio decreases.

B. Overhead

Figure 3 shows the overhead for different number of nodes and maximum speed. This simulation suggests that as the maximum speed increases, the overhead increases too.

C. Delay

Figure 4 shows the delay for different number of nodes and maximum speed. The measurement of delay is second. This figure shows that as the maximum speed increases, the delay increases too. Also, the delay of networks with more nodes are larger than networks with fewer number of nodes.

D. Energy Consumption

Figure 5 shows the energy consumption for different number of nodes and maximum speed. This simulation shows that as the maximum speed increases, the energy consumption increases too.

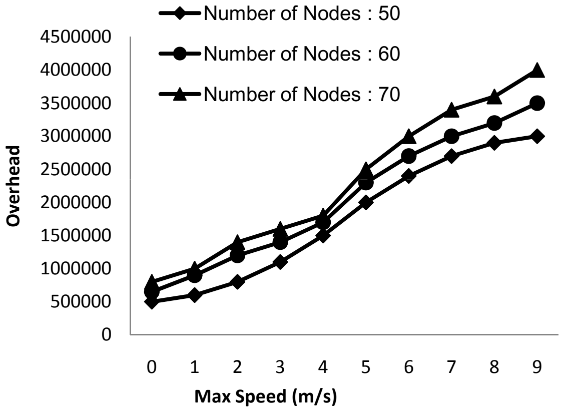

Fig. 3. Performance Under Different Malicious Strategies

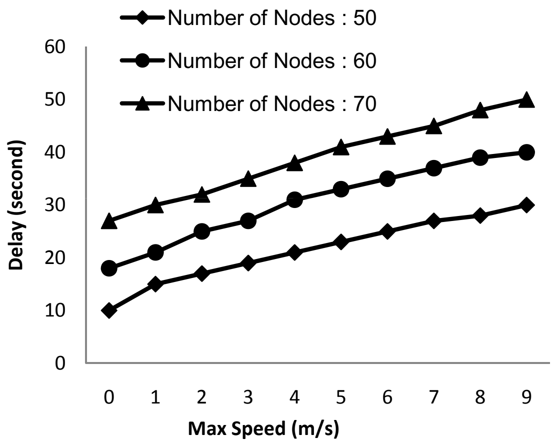

Fig. 4. Performance Under Different Malicious Strategies

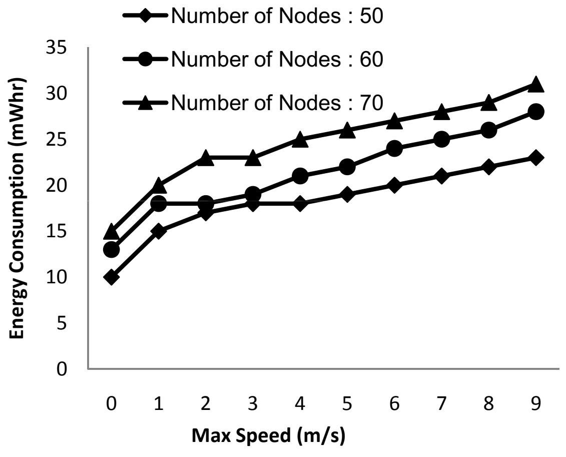

Fig. 5. Performance Under Different Malicious Strategies

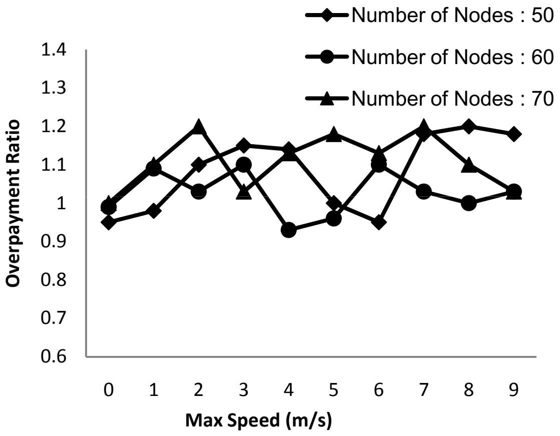

Fig. 6. Performance Under Different Malicious Strategies

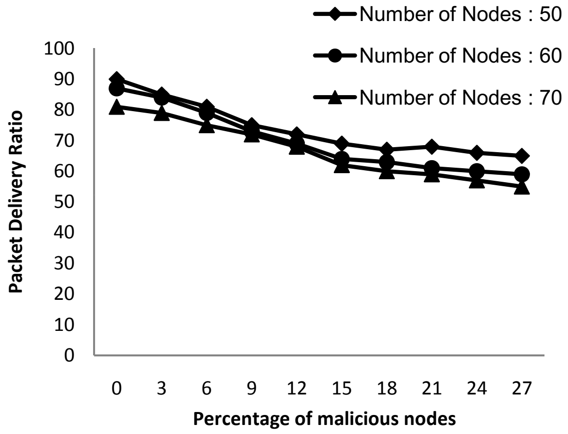

Fig. 7. Performance Under Different Malicious Strategies

E. Overpayment

Figure 6 shows the overpayment for different number of nodes and maximum speed. The overpayment ratio is approximately constant for different settings. It varies between 0.9 and 1.2.

F. Percentage of malicious nodes

In the previous simulations, the percentage of malicious nodes was constant. It was set to 10%. Figure 7 shows the effect of different number of malicious nodes. As the percentage of malicious node increases, the packet delivery ratio decreases and the performance of the whole network decrease. It is because of the bad effect of malicious nodes. They will consume other node's resources and other nodes should find a larger path that does not include malicious nodes.

VII. Conclusion

In this paper a secure and truthful routing mechanism for wireless network is presented. It is assumed that the network consists of malicious and selfish nodes. Malicious nodes falsifies information and packets. Selfish nodes do not contribute in the process of routing unless they have some incentives. Based on this assumptions, a new protocol is presented based on game theory and mechanism design. After detecting malicious nodes, our protocol finds the least cost path for routing through it. The payments as the incentive to intermediate nodes are based on VCG payments. It is believed that VCG is a truthful mechanism. Thus, every nodes in the network reveal their true costs.

REFERENCES

[1] C. Perkins, "Ad-hoc on-demand distance vector routing," *Internet draft RFC*, 1997.

[2] B. Johnson and D. Maltz, "Dynamic source routing in ad hoc wireless networks," *Mobile Computing*, 1996.

[3] Y.-C. Hu, A. Perrig, and D. Johnson, "Ariadne: A secure on-demand routing protocol for ad hocnetworks," in *Proceedings of MobiCom02*, 2002.

[4] S. Yi and R. Kravets, "Security-aware ad hoc routing for wireless networks," in *Proceedings of MobiHOC01*, 2001.

[5] Y. Wang and M. Singhal, "On improving the efficiency of truthful routing in manets with selfish nodes," *Pervasive and Mobile Computing*, vol. 3, p. 537559, 2007.

[6] L. Anderegg and S. Eidenbenz, "Ad hoc-vcg: A truthful and cost-efficient routing protocol for mobile ad hoc networks with selfish agents," in *Proceedings of MobiCom03*, 2003.

[7] J. Feigenbaum, C. Papadimitriou, R. Sami, and S. Shenker, "A bgp-based mechanism for lowest-cost routing," in *proceedings of the 2002 ACM Symposium on Principles of Distributed Computing*, 2002.

[8] Y. Wang, V. C. Giruka, and M. Singhal, "A fair distributed solution for selfish nodes problem in wireless ad hoc networks," in *Proceedings of Ad-Hoc, Mobile, and Wireless Networks: Third International Conference, ADHOC-NOW 2004*, Vancouver, Canada, July 2004.

[9] H. Q, W. D, and K. P, "Sori: a secure and objective reputation-based incentive scheme for ad-hoc networks," in *Proceedings of IEEE WCNC2004*, March 2004.

[10] V. Srinivasan, P. Nuggehalli, F. Chiasserini, and R. Rao, "Cooperation in wireless ad hoc networks," in *Proceedings of Infocom'03*, 2003.

[11] S. Zhong, Y. Yang, and J. Chen, "Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks," in *Proceedings of Infocom'03*, 2003.

[12] J. Cai and U. Pooch, "Play alone or together-truthful and efficient routing in wireless ad hoc networks with selfish nodes," in *Proceedings of MASS04*, 2004.

[13] S. Buchegger and J. Le-Boudec, "Nodes bearing grudges: Towards routing security, fairness, and robustness in mobile ad hoc networks," in *Proceedings of EUROMICRO-PDP*, 2002.

[14] ——, "Performance analysis of the confidant protocol (cooperation of nodes: Fairness in dynamic ad-hoc networks)," in *Proceedings of MobiHOC02*, 2002.

[15] P. Michiardi and R. Molva, "Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in *proceedings of Communication and Multimedia Security Conference 2002*, 2002.

[16] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *proceedings of MobiCom00*, 2000.

[17] K. Paul and D. Westhoff, "Context aware detection of selfish nodes in dsr based ad-hoc networks," in *proceedings of IEEE Vehicular Technology Conference02*, 2002.

[18] H. Miranda and L. Rodrigues, "Preventing selfishness in open mobile ad hoc networks," in *proceedings of 7th CaberNet Radicals Workshop*, 2002.

[19] Y. Wang, V. Giruka, and M. Singhal, "A fair distributed solution for selfish node problem in mobile ad hoc networks," in *proceedings of ADHOCNOW04*, 2004.

[20] L. Buttyan and J.-P. Hubaux, "Enforce service availability in mobile ad-hocwans," in *proceedings of MobiHOC00*, 2000.

[21] N. B. Salem, L. Buttyan, J. Hubaux, and M. Jakobsson, "A charging and rewarding scheme for packet forwarding in multi-hop cellular networks," in *proceedings of MobiHoc03*, 2003.

[22] J. Crowcroft, R. Gibbens, F. Kelly, and S. Ostring, "Modelling incentives for collaboration in mobile ad hoc networks," in *proceedings of WiOpt03*, 2003.

[23] S. Zhong, L. Li, Y. Liu, and Y. Yang, "On designing incentive-compatible routing and forwarding protocols in wireless ad-hoc networksan integrated approach using game theoretical and cryptographic techniques," in *Proceedings of MobiCom05*, 2005.

[24] K. Chen and K. Nahrstedt, "ipass: and incentive compatible auction scheme to enable packet forwarding service in manet," in *proceedings of ICDCS04*, 2004.

[25] S. Eidenbenz, G. Resta, and P. Santi, "Commit: A sender-centric truthful and energy-efficient routing ptotocol for ad hoc networks with selfish nodes," in *proceedings of IPDPS05*, 2005.

[26] K. Sanzgiri, B. Dahill, B. Levine, and E. Belding-Royer, "A secure routing protocol for ad hoc networks," in *proceedings of IEEE ICNP*, 2002.

[27] G. Zapata, "Secure ad hoc on-demand distance vector (saodv) routing," in *In IETF Internet Draft. http://www.ietf.org/internet-drafts/draft-guerrero-manet-saodv-00.txt*, 2001.

[28] P. Papadimitratos and Z. Haas, "Secure routing for mobile ad hoc networks," in *proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference(CNDS)*, 2002.

[29] F. Kargl, A. Gei, S. Schlott, and M. Weber, "Secure dynamic source routing," in *proceedings of the 38th Annual Hawaii International Conference on System Sciences (HICSS)*, 2005.

[30] N. Nisan and A. Ronen, "Algorithmic mechanism design," *Games and Economic Behavior*, vol. 35, pp. 166–196, 2001.

[31] "Glomosim simulator," in *http://pcl.cs.ucla.edu/projects/glomosim/*.