Social Norm Incentives for Secure Network Coding in MANETs

Chuchu Wu, Mario Gerla
Computer Science Department
University of California, Los Angeles
Los Angeles, CA. U.S.A. 90095
Email: {wuchuchu,gerla}@cs.ucla.edu

Mihaela van der Schaar
Electrical Engineering Department
University of California, Los Angeles
Los Angeles, CA. U.S.A. 90095
Email: mihaela@ee.ucla.edu

Abstract—The throughput of mobile ad hoc networks subject to disruption, loss and interference can be significantly improved with the use of network coding. However, network coding implies extra work for forwarders. Selfish forwarders may prefer to simply forward packets without coding them because of the processing overhead introduced by network coding. This is especially true in secure network coding where the coded packets are protected from pollution attacks by processor intense homomorphic signatures. To drive selfish nodes to cooperate and encode the packets, this paper introduces social norm based incentives. The social norm consists of a social strategy and a reputation system with reward and punishment connected with node behavior. Packet coding and forwarding is modeled as a repeated alternate gift-giving game. The interaction between nodes in the repeated game is formalized, the conditions for social strategy sustainability (or compliance) are identified, and a sustainable game that optimizes the social welfare is designed. For this game, the impact of packet loss rate, reputation thresholds and reputation update frequency on performance is evaluated.

Keywords—game theory; network coding; incentive design; reputation scheme;

I. INTRODUCTION

Mobile devices like smart phones are becoming increasingly powerful and capable to function not only as clients, but also as peers in a fully fledged ad hoc network. For instance a mobile may propagate to neighbors in ad hoc mode a stream that it is downloading from the Internet via WiFi or 3G. The mobile devices, however, have energy constraints. Since forwarding other devices’ packets provides no benefit to a mobile that is not an intended destination, rather, it consumes battery resources, a self-interested relay node chooses not to forward the packets. If every relay node drops others’ packets, the video never gets delivered to friends several hops away. This selfish behavior, however, can backfire — when the selfish node transmits its own video file, it will be treated the same way, i.e. its file will be dropped. This behavior is known as ”tit for tat” in cooperative P2P distribution protocols (e.g. bit torrent) and can be corrected with incentives.

A similar situation occurs when the video stream is network coded. Network coding [8], [9], [10] has been shown to improve streaming performance dramatically in disruptive wireless networks with random loss or interference via generating redundant packets to offset the loss. Forwarders don’t retransmit lost packets due to the broadcast MAC used for multicast streaming. Hence network coding improves packet deliver rate and stream quality.

Network coding, however, is susceptible to pollution attacks. Upon receiving corrupted packets, the destination cannot decode and must throw away the entire generation. So network coding streams must be protected by special hash functions or signatures that maintain their properties through linear combinations. One such scheme is the homomorphic hash/signature[13], which however requires heavy processing overhead, up to 100 times the processing of conventional network coding[10]. Due to the high cost of secure network coding, selfish intermediate nodes are more likely to refuse to perform coding in order to save power for their own future transmissions. Hence, an incentive scheme is needed to encourage intermediate nodes to perform secure network coding. Incentive schemes have been proposed for conventional mobile networks before, e.g. [15], [16], [17]. In this paper we extend those schemes to the network coding scenario.

To maintain the model analytically tractable, in this paper we assume a rather simple topology scenario, with unicast from a source to a destination via a single intermediate node. The source node injects a network coded stream. The intermediate node may carry out network coding, simply forward or drop the packets. The social norm based incentive scheme we propose prescribes the action of the intermediate node according to the reputation of the source and destination nodes. If the receiver detects non compliance by the intermediate node (i.e. the intermediate node does not inject redundant coded packets in presence of loss when it should), it will broadcast the deviating action to a scoped neighborhood and the intermediate node’s reputation will be lowered. As a consequence, when a low reputation intermediate node in turn becomes source and sends its own stream, it will be punished; namely, the neighbors will refuse to code its packets according to social strategy. This ”punishment” should be sufficient to persuade the nodes that are frequent video originators or receivers to encode the packets. The above topology is extremely simple. However, careful readers will notice that the same method can be extended to more general and complex topologies with multi-hops, multi-path and multicast scenarios.

In summary, streaming in lossy mobile networks greatly benefits from network coding; network coding must be pro-
In section III, the incentive protocol is analyzed. Section IV cannot decode. “Progressive coding” is used here to overcome full delivery. If less than K linearly independent packets are means the redundancy rate should be set to the expected number of transmissions \( p \) rate denoted as \( 1 - q \) generation size = K packets. The source then injects in the flow network coding is used to increase transmission reliability on lossy wireless channels. The source node S generates a Intra- node D) n random linear coded packets[10]. The ratio n/K (where n >= K) is defined as redundancy rate. If a secure NC scheme such as homomorphic signature is used to protect packets from pollutions, the procedure is no different from regular random linear network coding except for the extra processing overhead. The probability of delivering K packets with n transmissions on a faulty link follows a negative binomial distribution with parameter \( q \), where \( q = 1 - p \) is the packet delivery rate. So the expected number of transmissions \( E(n) = K/q \), which means the redundancy rate should be set to 1/q to achieve full delivery. If less than K linearly independent packets are received, the entire generation is lost because the receiver cannot decode. “Progressive coding” is used here to overcome this problem, where the intermediate node forwards the full generation without coding but only encodes the redundant packets. The advantage of progressive coding is a lower decoding delay and also the ability to receive some packets at the destination even if the full rank is never received.

To simplify the model without loss of generality, we assume that the intermediate node knows a prior loss rate \( p \) and introduces redundancy accordingly, i.e. it injects \( K/(1−p) \) packets, of which K are the original packets and the rest are coded packets.

The nodes in our model are mobiles with the following characteristics: having limited power resources, following selfish algorithms and being randomly matched as session origin, relay and destination. Here selfishness means taking an action to maximize its own utility. The possible actions of an intermediate node includes performing NC, simple forwarding or dropping the packets totally. Relatively high mobility forces the devices to have different neighbors throughout time.

Hence, we use a global reputation system (say, reputation reports are signed and periodically broadcast to a scoped neighborhood) to keep track of the reputation value of each node. This way, each node has a consistent view of the reputations of the other nodes. As discussed later, in practical cases most nodes comply and code. Thus, the rogue minority with bad reputation cannot subvert the election.

The model described above is rather simple (unicast session on a single path), yet it captures the worst damage a node R can cause by being not cooperative. In the more general case, a MANET with multiple paths is deployed from S to D. In this case the non cooperation of a node has a less severe effect than in the single path case because of path redundancy (recall, in our case a malicious node can only drop it cannot pollute). The worst case situation is the unicast session we discussed, with a single non cooperating node in the critical section. The single path model reflects the worst case situation over all possible topologies and routing schemes.

B. Game setting

We model the unicast session in part A as a gift-giving game[4] with two players. Player 1 is the intermediate node R, which has three available actions \( (a_R) \): (1) NC-forward (NC-F) \( K/q \) encoded packets to sink node D; (2) simple-forward (SF) the original K packets to D; (3) totally drop (TD) the packets. Player 2 is the source-destination (S-D) pair of the session, which has no actions. We assume player 2 receives a constant benefit of B for delivering each packet. Player 1 has a constant cost of \( c_1 \) for encoding each packet, and a constant cost of \( c_2 \) for forwarding each packet. Here \( c_1 \) and \( c_2 \) mainly represent the power consumption of coding and forwarding. Then we can obtain the expected utilities of both players as shown in Table I.

<table>
<thead>
<tr>
<th>Action of R in ( a_R )</th>
<th>NC-F</th>
<th>SF</th>
<th>TD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Utility ( v_{R,S-D} )</td>
<td>( -(c_1 + c_2)K/q, BK )</td>
<td>( -c_2K, BKq )</td>
<td>( 0,0 )</td>
</tr>
</tbody>
</table>

Table I: One-shot Gift-Giving Game

As system designers, we encourage nodes to perform NC-F only if the overall utility is maximized when all nodes code.
So the game itself must satisfy the condition in equ.(1), which means that NC-forwarding provides a higher overall utility than simple forwarding, and simple forwarding provides a higher utility than dropping, which is 0. Here B, c_1, and c_2 are all relative values determined by nodes themselves.

\[ BK - (c_1 + c_2) \frac{K}{q} > BK \eta - c_2 K > 0 \]  

(1)

Nodes in the network are assumed to be selfish strategic players who take the action to maximize their own utilities. If it is a one-shot game, there is a dominant action (or best choice) for intermediate node R, i.e. total drop (TD). Therefore the network has zero throughput. Also, one-shot game is not appropriate to model nodes that stay in the network for a relatively long time. So we model it as an infinitely repeated game with discount factor \( \delta \). \( \delta \) represents the probability of playing the game once again in the future. Namely, it reflects the likelihood that a node will stay in the system for the next time period. While some nodes are leaving the network, some new coming nodes arrive in a dynamic balance fashion. \( \delta \) is decided by each node themselves and is not tunable by system designers. The relay node in the current round may become a source or sink node in the future rounds. We assume three nodes in the session are randomly matched and every node in the system is uniform (i.e. all nodes have the same settings of \( B, c_1, c_2, \delta \)). So expectedly, in every three sessions, a certain node in the network will act as relay, source and sink respectively. So the long-term utility of a random node is,

\[ v^\infty = \sum_{t=1}^{\infty} \delta^{t-1}(v^t_R + v^t_{SD}) = v(\theta_{t=1}) + \delta \sum_{\theta'} p_{\tau}(\theta'|\theta)v^\infty(\theta') \]  

(2)

If every node has fixed neighbors and plays the repeated game with the same opponents over time, simply adopting a tit-for-tat strategy will be enough to enforce the nodes to perform network coding. However, mobiles usually change neighbors throughout the experiment, so they do not have knowledge of their new neighbor’s behavior history. Under such circumstance, tagging each node with a reputation value is efficient to record its behavior in the past. By introducing the idea of social norm[14] from economics to wireless networks, we design a novel incentive scheme to encourage nodes to perform network coding despite of the expensive power consumption.

C. Social norm

The social norm, denoted by \( \kappa \), is composed of a social strategy \( \sigma \) and a reputation scheme \( \tau \).

In our reputation system, every node in the network is tagged with a reputation \( \theta \), an integer from \( \Theta = \{0, 1, ..., L\} \) for some L. A high \( \theta \) means that the node performed well (e.g. coding and/or forwarding) in history, otherwise the node did not perform well in the past. The reputation system has the following structure: (1) every node maintains a table that stores all its neighbors’ reputation values; (2) nodes broadcast deviating reports to a scoped neighborhood periodically (3) each node updates the reputations of its neighbors according to the deviating reports received within the period.

\( \sigma \) is a reputation-based behavioral strategy represented by a mapping \( \sigma : \Theta \times \Theta^2 \rightarrow A \), where the first \( \Theta \) is the reputation of the intermediate node R, and \( \Theta^2 \) represents the reputations of the S-D pair. \( A = \{NC-F, SF, TD\} \). So \( \sigma \) specifies the action \( \sigma(\theta_R, \theta_S, \theta_D) \in A \) which node R with reputation \( \theta_R \) should select when faced with a unicast session consisting of a source node with reputation \( \theta_S \) and a sink node with reputation \( \theta_D \).

Generally, the social strategy rewards high reputation nodes by prescribing intermediate nodes to perform coding and forwarding for them; also, it punishes low reputation nodes by prescribing intermediate nodes to drop their packets. We restrict our attention to a set of threshold-based strategies \( \Gamma \). Every strategy \( \sigma \in \Gamma \) can be characterized by a threshold \( k(\sigma) \in \{0, 1, ..., L\} \). Given any threshold \( k \), there are still many choices of \( \sigma \): (3)(4) are two examples. Among all possible strategies, \( \sigma_2 \) is the strictest (i.e. node R performs NC-F only if both source and sink nodes have the maximum reputation \( L \)). In this paper, we mainly use \( \sigma_1 \) as our proposed social strategy, where R performs NC-F if at least one of the source and sink has reputation of \( L \). We will compare \( \sigma_1 \) with other alternatives and analyze the impacts of choosing different strategies in part A of SectionIV.

\[ \sigma_1(\theta_R, \theta_S, \theta_D) = \begin{cases} \text{NC-F} & \text{if } \theta_R = L \cap \max\{\theta_S, \theta_D\} = L \\ \text{TD} & \text{if } \min\{\theta_R, \theta_S, \theta_D\} < k \end{cases} \]  

(3)

\[ \sigma_2(\theta_R, \theta_S, \theta_D) = \begin{cases} \text{NC-F} & \text{if } \theta_R = L \cap \min\{\theta_S, \theta_D\} = L \\ \text{TD} & \text{if } \min\{\theta_R, \theta_S, \theta_D\} < k \end{cases} \]  

(4)

Consistent with our threshold-based social strategy \( \sigma_1 \), we propose a "multi-stage punishment reputation scheme", denoted as \( \tau \), shown in Fig.1, where \( \alpha'_1, \alpha'_2 \) are transition probabilities caused by approved behavior, and \( \varepsilon'_1, \varepsilon'_2, \varepsilon'_3 \) are transition probabilities caused by evil behavior. Specific interpretations can be found in Appendix. Reputations are updated periodically. If an intermediate node always complies with strategy \( \sigma_1 \) during the period, its reputation will increase by 1 until it reaches the maximum \( L \); if it deviates from \( \sigma_1 \) for at least once within the period, its reputation will decrease to either \( k \) or 0, depending on its deviating action—if it drops packet totally when it should not, its reputation will decrease to 0; otherwise, only decreases to \( k \). Here \( \mu_1, \mu_2, \mu_3 \) respectively denote the proportion of nodes with a high \( (\theta > L \) and low \( (0 \leq \theta < k) \) reputation.

III. GAME OPTIMIZATION

A. Metrics

We design social norm based incentives to encourage nodes in the network to cooperate, aiming at maximizing the network throughput. Throughout here is represented by all packets delivered in all sessions within each reputation update period.
Taking the costs (the power consumptions) into account, we use social utility as a metric of the system. Social utility is defined to be the total utility of all nodes in the network after one period.

Besides social utility, another important metric for an incentive scheme is the obedience of the nodes, i.e. sustainability of the social norm. A social norm is sustained when selfish nodes choose to comply with the social strategy instead of deviating from it. Sustainability reflects the probability that a selfish node will choose to cooperate and help others. The more intermediate nodes perform coding, the higher throughput the network will achieve; so the sustainability of the incentive scheme also affects the throughput.

B. System Convergence

Given the social norm with social strategy \( \sigma_1 \) in (3) and reputation scheme \( \tau \) in Fig.1, we can derive the unique corresponding stationary distribution of reputation.

**Proposition 1:** Initially every node is assigned with the maximum reputation value \( L \). When all nodes follow the previously defined social norm, the reputation distribution of nodes in the network converges to a unique point \( \{ \eta(\theta) \} \), as presented as equ.(3) in Appendix.

C. Social utility at steady state

In this subsection we determine the social utility at steady state for social norm \( \kappa = (\sigma, \tau) \) obtained in proposition1. According to the social strategy \( \sigma_1 \), a session containing low reputation nodes (either S, D or R) always has a utility of 0, because low reputation nodes always drop others’ packets and their own packets are also dropped by others as punishment. So we only consider the sessions where all nodes have reputations \( \theta \geq k \). Let \( M \) be the number of sessions where a node acts as a relay node within one reputation update period. We use \( m_1 \) and \( m_2 \) to denote the number of NC and SF sessions for a high reputation intermediate node (an intermediate node with \( \theta_R = L \)). We use \( l \) to denote the number of SF sessions for a medium reputation intermediate node (an intermediate node with \( \theta_R \in [k, L) \)). Since nodes are considered uniform, the social utility, or the expected utility of any node in the network per session, is:

\[
U = \sum \eta(\theta) v(\theta) = \frac{1}{3} \mu_1 \times \left[ \frac{m_1}{M} (B - c_1 + c_2') + \frac{m_2}{M} (Bq - c_2) \right] + \frac{1}{3} \mu_2 \times \left[ \frac{l}{M} (Bq - c_2 - qB) \right]
\]

Where,

\[
m_1 = M (\mu_1^2 + 2\mu_1\mu_2) \\
m_2 = M\mu_2^2 \\
l = M (\mu_1 + \mu_2)^2
\]

We also extend our results to a multihop session in Appendix. We present the expression of the social utility \( U^H \) of a session with \( H \) hops, and a diagram showing the impact of \( H \) on \( U^H \).

D. Sustainability conditions

In this subsection, we determine the sustainability conditions, under which all nodes in the network will rationally choose to comply with the social strategy \( \sigma_1 \) instead of deviating from it. Based on the assumption that all nodes in the network take the action to maximize their own long-term utility, we define sustainability condition of the social norm.

**Definition 1:** Social norm \( \kappa = (\sigma, \tau) \) is sustainable (or has a subgame perfect equilibrium) if when \( \kappa \) is applied, the long-term utility of any node in the network by complying with the social strategy is no smaller than the long-term utility by deviating from the actions prescribed in the social strategy, i.e. for any reputation \( \theta \in \Theta \) and any selfish strategy \( \sigma' \neq \sigma \), we must have \( v^\infty_\sigma(\theta) \geq v^\infty_{\sigma'}(\theta) \), where \( v^\infty(\theta) \) is defined in (2).

**Proposition 2:** Any node in the network will always comply with the social strategy \( \sigma_1 \) and the social norm will be sustained iff. discount factor \( \delta \geq \max \{ \delta_1, \delta_2, \delta_3, \delta_4 \} \), where,

\[
\delta_1 = \frac{c_1 + c_2 - qc_2}{qB(1 - q)}
\]

And \( \delta_2, \delta_3, \delta_4 \) are in implicit form, see Appendix.

If \( \max \{ \delta_1, \delta_2, \delta_3, \delta_4 \} < 1 \), the sustainability conditions can always be satisfied if the actual \( \delta \) of the nodes in the network is close enough to 1, which indicates that the nodes will stay in the system forever. \( \max \{ \delta_1, \delta_2, \delta_3, \delta_4 \} < 1 \) can be guaranteed when benefit \( B \) is big enough comparing with costs \( c_1, c_2 \).

**Proposition 3:** If benefit \( B \) satisfies (8), there always exists a \( \delta = \max \{ \delta_1, \delta_2, \delta_3, \delta_4 \} \in [0, 1] \), s.t. when \( \delta \geq \delta \), the incentive scheme can be sustained by all nodes in the network.

\[
B \geq \frac{c_1 + c_2 - qc_2}{q(1 - q)} \left( \frac{\mu_1}{\mu_2} + 2 \right)
\]

Since \( \delta \) is decided by the system itself and not tunable, smaller \( \delta \) indicates greater chance of sustainability of the social norm. So we use \( 1 - \tilde{\delta} \) as the metric to reflect the sustainability of the scheme. We call it ”Sustainable Interval” (SI), meaning that if the actual \( \delta \) of the system falls into this interval, the social norm will be sustainable. We wish to maximize the SI in order to maximize the probability of sustainability.
E. Optimization problem

We formalize the parameter selection as an optimization problem of maximizing both social utility $U$ in (5) and $SI = 1 - \delta$ for any reputation distribution $\eta(m_1, m_2)$ from the initial state $\eta_0(1,0)$ all the way to the steady state $\{\eta(\theta)\}$.

The parameters can be classified into two categories: one category reflects the nature of the network, and is given (not tunable by designers); the other reflects the characteristics of the social norm based scheme we propose, and can be tuned by the protocol designer.

In summary, network nature parameters include: packet loss rate $p$, benefit-cost ratio $B : c_1 : c_2$, discount factor $\delta$, number of hops $H$; tunable parameters include: social strategy $\sigma$, reputation threshold $k$, number of sessions $M$ within one reputation update period and NC generation size $K$.

IV. PERFORMANCE EVALUATION

In this section, we evaluate the performance of the NC forwarding game using numerical techniques. We compute social utility $U$ and sustainability $SI$ results as a function of system variables and design parameters. In particular we define the optimal selection of reputation thresholds and other design parameters.

A. Selecting the social strategy $\sigma$

In part C of section II, we pointed out that there are many design choices for $\sigma$, and we presented two examples in (3)(4). Here we show that there exists a tradeoff between social utility and sustainability when designing the social strategy. Specifically, a stricter social strategy (e.g. a strategy that requires high reputation of both source and destination for coding at the intermediate node) will lead to a higher sustainability (i.e. higher compliance ratio) at the price of a lower social utility. We discover this tradeoff by comparing the social utility $U$ and the sustainability interval $SI$ of $\sigma_1$ in (3) and $\sigma_2$ in (4), where $\sigma_2$ is stricter than $\sigma_1$. We prove that $U_1 \geq U_2$ and $SI_2 \leq SI_1$. The proof is given in Appendix.

This happens because in $\sigma_2$, the intermediate node performs network coding only when all the nodes in the session have maximum reputation of $L$. Naturally this harms the throughput since it reduces the chance of coding. On the other hand, it enforces the nodes to be more compliant in order to keep a high reputation and avoid severe utility degradation.

B. Selecting the design parameters $L, k$ and $M$

In practice, there are very few nodes with reputation lower than $k$, mainly because the probability that all packets are lost is tiny. Also, malicious nodes that intentionally drop packets will be blacklisted and are avoided during routing. Hence the value of $k$ has almost no effect on network performance. So we only consider the interval between $L$ and $k$. Fig.2 and Fig.3 respectively show the numerical results of stationary social utilities $U$ and SI under different settings of threshold interval $L - k$ and number of sessions in each period $M$.

According to Fig.2 and Fig.3, generally both $U$ and $SI$ are higher when $L - k$ is set small. On the contrary, when $L - k$ is set very large, $U$ approaches the utility value that corresponds to all nodes only performing SF, whereas SI approaches 0. The intuition is that if $L - k$ is very large, medium reputation nodes have to keep performing well for many periods of time in order to reach $L$. During this long journey from $k$ to $L$, they are still medium reputation nodes which only perform (and are only served with) SF, even worse they may leave the system before becoming a high reputation node. Therefore the network has a lower throughput and worse sustainability. Also, we prove mathematically that $U$ is a strictly decreasing function of $L - k$ (see Appendix).

Fig.2 and Fig.3 also show that $U$ and SI increase when $M$ gets smaller. This means that if the system updates or refreshes reputations frequently, i.e. there are fewer sessions in an update period, the network will have a higher throughput and better sustainability. Intuitively, if refreshing rate is higher, the nodes’ reputations more accurately reflect their behavior history. And they will be rewarded or punished in time. We also prove mathematically that $U$ is a strictly decreasing function of $M$ in Appendix.

\begin{figure}[h]
\centering
\includegraphics[width=0.8\textwidth]{fig2.png}
\caption{Social utilities at steady states ($U$) when selecting different threshold intervals ($L - k$) and number of sessions $M$ in one reputation update period}
\end{figure}

\begin{figure}[h]
\centering
\includegraphics[width=0.8\textwidth]{fig3.png}
\caption{Sustainable interval (SI) when selecting different threshold intervals ($L - k$) and number of sessions $M$ in one reputation update period}
\end{figure}

C. Impact of untunable system variables on performance

NC generation size $K$ belongs to tunable parameters, however according to numerical tests, changing $K$ has little impact on system performance. Intuitively, for both NC-F and SF, we
mainly care about the proportion of packets delivered, so the value of $K$ does not affect results.

In part D of section III, we have thoroughly discussed the impacts of discount factor $\delta$ (i.e. the probability of a node staying in the system for the next period) on the sustainability of our scheme. The higher $\delta$, the better sustainability. There exists a threshold $\delta_0$ below which nodes will not comply or perform network coding, above which they will. This indicates that a node that stays in the system for a long time is more likely to help others than the node that will leave the system soon.

Also in part D of section III, we show that there exists a $R_H$ below which the scheme can never be sustained. Benefit $B$ is a relative parameter evaluated by each node itself. If an intermediate node highly values the benefit of its own future transmissions, it has more incentives to serve others and pursue a high reputation. If $\delta$ is too low, a high $B$ is still insufficient to encourage nodes to do network coding, hence the throughput does not increase after $B$.

A low packet loss rate $p$, or a high packet deliver rate $q$, will lead to a higher throughput and social utility as expected. Fig.4 shows how the sustainability of the scheme varies as a function of packet deliver rate. When the packet loss rate is very low, the network condition is good, and nobody does expensive secure NC because the performance of NC is hardly different from SF. When the packet loss rate is very high and the network condition is very bad, nobody does expensive secure NC either, because even if they did, nobody notices and they will be punished anyway due to the severe packet loss. In realistic scenarios, the packet loss rate is generally well below 0.5. With this condition, we may conclude that our incentive scheme is more sustainable (i.e. more nodes are induced to use Network Coding) when packet loss increases, just as NC is beneficial when packet loss is serious.

![Fig. 4. Sustainable interval (SI) of the incentive scheme under different packet deliver rate q](image)

V. CONCLUSION

In this paper, we propose a novel incentive scheme to encourage selfish nodes in MANETs to perform network coding, which leads to higher throughput of the network. Differently from previous schemes, we propose a set of social norm based incentive schemes with parameters that we adjust to optimize the social utility and sustainability. We first prove that reputation distribution converges. Then, we prove the following results: (1) there exists a tradeoff between the social utility/throughput and sustainability — a stricter social strategy will increase the sustainability but decrease the utility; (2) both utility and sustainability will be optimized if the reputation threshold $k$ is set close to the maximum reputation $L$, and reputations are updated or refreshed frequently. Additionally we show how the network condition or the game itself impacts our incentive scheme. However the change of network condition will not change our decisions of parameter selections.

REFERENCES


APPENDIX

- A separated appendix is available with the following link: http://dl.dropbox.com/u/44670797/Appendix.pdf