Quantifying Anonymity Trade-Off Using Nash Equilibrium Approach

J. Darwin & R. Anantha Kumar, Kalasalingam Institute of Technology, Krishnankoil

Abstract:

In this paper proposed the Quantifying anonymity using conditional entropy of the routes given the adversary's observation, the problem of optimizing anonymity is posed as a two-player zero-sum game between the network designer and the adversary. Game theory applied to study the optimal performance tradeoffs and equilibrium strategies. Using independent schedule however, requires dummy transmissions by the relays. The results are applied to study the relationships between anonymity, the fraction of monitored relays and the fraction of hidden relays in large networks.

Keywords: Quantifying anonymity, Nash Equilibrium Approach

I **Introduction**

The packet transmission times1 of nodes in a network can reveal significant information about the source–destination pairs and routes of traffic flow in the network. The typical design of anonymous networking protocols models adversaries a omniscient and capable of monitoring every single transmission in the network perfectly. From a practical standpoint, this is far too conservative, and such universal information would be available only to the network owner or a centralized controller. In this paper, our goal is to study the problem of anonymity in networks under a more general adversary model, where an *unknown* subset of the nodes is monitored by the adversary. The subset of monitore nodes could depend on the physical location of the adversary or partial knowledge of network transmission protocols. It is also possible that in some public wireless networks, certain node may have weaker physical protection than others and are hence more vulnerable to transmission monitoring. From a network design perspective, the goal is to design transmission and relaying strategies such that the desire level of network performance is guaranteed with maximum *anonymity of network routes*. Providing anonymity to the routes of data flow in a network requires modification of packet transmission schedules and additional transmissions of dummy packets to confuse an external observer. These modifications, however, reduce the achievable network performance, particularly in ad hoc wireless networks, where the scheduling needs to satisfy medium access constraints on the shared channel. Therefore, depending on the desired quality of service (QoS), it is necessary to pick the optimal set of nodes to modify transmission schedules so that anonymity is maximized without violating QoS requirements [1].

II Game Theory in Networking

Game theory is a formal theory of interactive decision making, used to model any decision involving two or more decision makers, called *players*, each with two or more ways of acting, called *strategies*, and well define preferences among the possible outcomes, represented by numerical *payoffs*.

In conventional decision theory, rational choice is defined in terms of maximizing expected utility (EU), or subjective expected utility (SEU), where the objective probabilities of outcomes are unknown. But this approach is problematic in games because each player has only partial control over the outcomes, and it is generally unclear how a player should choose in order to maximize EU or SEU without knowing how the other player(s) will act. Game theory, therefore, incorporates not only rationality assumptions in the form of expected utility theory, but also common knowledge assumptions, enabling players to anticipate one another's strategies to some extent, at least. The standard common knowledge and rationality (CKR) assumptions are as follows:

CKR1 (common knowledge): The specification of the game, including the players' strategy sets and payoff functions, is *common knowledge* in the game, together with everything that can be deduced logically from it and from the rationality assumption CKR2.

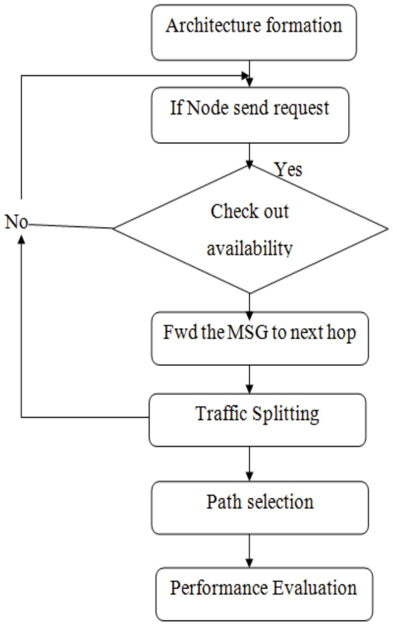
CKR2 (rationality): The players are rational in the sense of expected utility theory – they always choose strategies that maximize their individual expected payoffs, relative to their knowledge and beliefs – and this is *common knowledge* in the game. A proposition is common knowledge if every player knows it to be true, knows that every other player knows it to be true, knows that every other player knows that every other player knows it to be true, and so on. This is an everyday phenomenon that occurs, for example, whenever a public announcement is made, so that everyone present not only knows it, but knows that others know it, and so on.[2]

III Nash Equilibrium Approach

The most important "solution concept" of game theory flows directly from best replies. A *Nash equilibrium* (or *equilibrium point* or simply *equilibrium* is an outcome in which the players' strategies are best replies to each other. In the Prisoner's Dilemma game, joint defection is a Nash equilibrium, because *D* is a best reply to *D* for both players, and it is a unique equilibrium, because no other outcome has this property. A Nash equilibrium has strategic stability, because neither player could obtain a better payoff by choosing differently, given the coplayer's choice, and the players, therefore, have no reason to regret their own choices when the outcome is revealed. The fundamental theoretical importance of Nash equilibrium rests on the fact that if a game has a uniquely rational solution, then it must be a Nash equilibrium. Von Neumann and Morgenstern [31, pp. 146–148] established this important result vi a celebrated *indirect argument*, the most frequently cited version of which was presented later by Luce and Raiffa [18, pp. 63–65]. Informally, by CKR2, the players are expected utility maximizers, and by CKR1, any rational deduction about the game is common knowledge. Taken together, these premises imply that, in a two-person game, if it is uniquel rational for the players to choose particular strategies, then those strategies must be best replies to each other. Each player can anticipate the coplayer's rationally chosen strategy (by CKR1) and necessarily chooses a best reply to it (by CKR2); and because th strategies are best replies to each other, they are I Nash equilibrium by definition. A uniquely rational solution must, therefore, be a Nash equilibrium.

The indirect argument also provides a proof that a player cannot solve a game with the techniques of standard (individual) decision theory (*see* strategies of decision making) by assigning subjective probabilities to the coplayer's strategies as if they were states of nature and then simply maximizing SEU. The proof is by *reductio ad absurdum*. Suppose that a player were to assign subjective probabilities and maximize SEU in the Prisoner's Dilemma game. Thespecific probabilities are immaterial, so let us suppose that Player I, for whatever reason, believed that Player II was equally likely to choose *C* or *D*. Then, Player I could compute the SEU of choosing *C* as 1/2*(3)* + 1/2*(0)* = 1.5, and the SEU of choosing *D* as 1/2*(5)* + 1/2*(1)* = 3; therefore, to maximize SEU, Player I would choose *D*. But if that were a rational conclusion, then by CKR1, Player II would anticipate it, and by CKR2, would choose (with certainty) a best reply to *D*, namely *D*. This leads immediately to a contradiction, because it proves that Player II was no equally likely to choose *C* or *D*, as assumed from the outset. The only belief about Player II's choice that escapes contradiction is that Player II will choose *D* with certainty, because joint defection is the game's unique Nash equilibrium.

III System Flow Graph



We proposed the Nash equilibrium for implementing more number of players instead of two player zero sum game. Performance Metrics: Anonymity and Throughput. Parallel relay networks to demonstrate the applicability of the game-theoretic approach.

IV Results

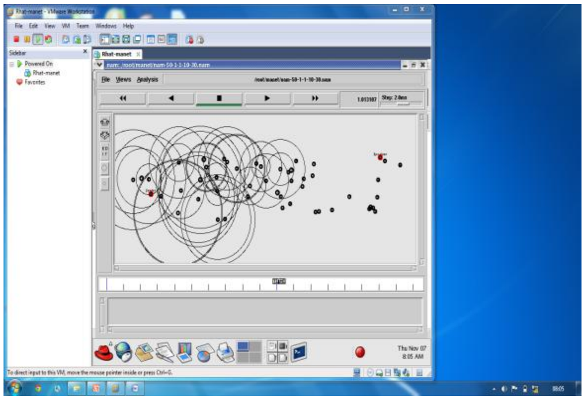


Figure.1 Packet Transmission

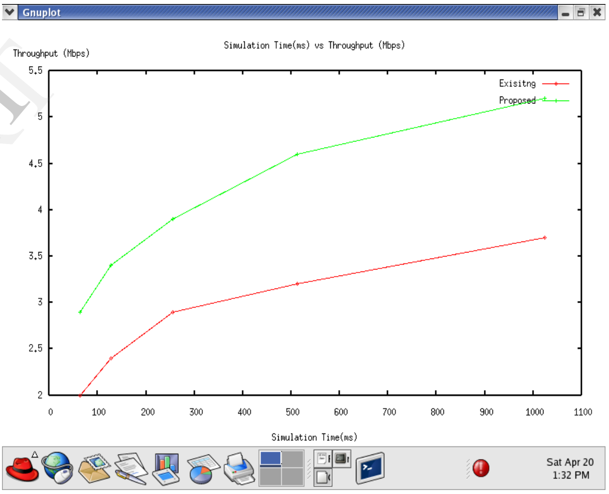


Figure 2 Comparison of throughout

V Conclusion

In this paper, we considered the problem of providing anonymity to network communication when adversaries monitor or compromise an unknown subset of nodes in the network. We presented a game-theoretic formulation and proved the existence of saddle-point equilibria. Using the class of parallel relay networks, we demonstrated that this approach can be used to obtain optimal strategies for the network designer and the adversary, as well as provide insights into anonymity–throughput tradeoffs in large networks. The problem of computing the equilibria has not been dealt with in this paper, but efficient algorithms for this purpose would fortify the results here and are part of ongoing research. In this paper, we have used specific classes of networks and assumed knowledge of topology and sessions. A similar approach for random networkswith random connections could shed valuable insights into scaling behavior of anonymous networking.

VI References

1] Parv Venkadasubramanian, " A game theoretic approach to Anonymous Networking" IEEE Transaction on Networking, Vol 20, No 3, June 2012., pp 892-905.

2] Andrew M. Colman, " Game Theory " Encyclopedia of Statistics in Behavioral Science, Vol 2 , pp 688-694, 2005.

3] T. He and L. Tong, "Detecting information flows: Fundamental limits and optimal algorithms," IEEE Trans. Inf. Theory, 2007, submitted for publication

4] A. Kashyap, T. Basar, and R. Srikant, "Mutual information games in multiuser channels with correlated jamming," IEEE Trans. Inf.Theory,vol. 55, no. 10, pp. 4598–4607, Oct. 2009

5] S. Sarkar, E. Altman, R. El-Azouzi, and Y. Hayel, "Information concealing games in communication networks," in Proc. IEEE INFOCOM, Phoenix, AZ, Apr. 2008, pp. 2119–2127

6] J. F. Nash, "Equilibrium points in -person games," in Proc. Nat. Acad.Sci., Jan. 1950, vol. 36, pp. 48–49.

AUTHOURS PROFILE:

J.DARWIN doing his M.E degree in Computer Science Engineering at kalasalingam Institute of Technology, Tamilnadu. He received his B.E degree in Computer Science Engineering at Anna University of Technology, Madurai, Taminadu. His research interests include Networking, Cloud Computing and Software Engineering.

R.ANANTHA KUMAR working as a Assistant Professor in kalasalingam Institute of Technology, Tamilnadu. He received his M.E degree in Software Engineering at Rajalakshm Engineering College, Tamilnadu. He received his B.E degree in Computer Science Engineering at Arulmigu Kalasalingam College of Engineering, Taminadu. His research interests include Networking, Cloud Computing and Software Engineering.