Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Computer Science 19 (2013) 1047 – 1052

Procedia Computer Science

The 8th International Symposium on Intelligent Techniques for Ad hoc and Wireless Sensor Networks (IST-AWSN)

Adaptive Energy Aware Cooperation Strategy in Heterogeneous Multi-Domain Sensor Networks

M.J. Shamani[a], Hossein Gharaee[b], Sahba Sadri[c], Fereidoon Rezaei[d] a*

[a]*Kish International Campus, Tehran Univesity, Tehran, Iran*
[b]*Iran Telecomunication Research Center, Tehran, Iran*
[c]*Concordia Institute for Information System Engeneering, Montreal, Canada*
[d]*Kish International Campus, Tehran Univesity, Tehran, Iran*

Abstract

In some applications of sensor networks, multi-domain exists and cooperation among domains could lead to longer lifetime. In this paper, we consider heterogeneous multi-domain sensor networks. It means that different networks belong to different domains and sensors are deployed at the same physical location and their topology is heterogonous. Apparently, domains life time can be increased by means of cooperation in packet forwarding; however selfishness is inevitable from rational perspective. We investigate this problem to find out cooperation of authorities while their sensors are energy aware. When sensors are energy aware, spontaneous cooperation cannot take place. Therefore we presented the Adaptive Energy Aware strategy, a novel algorithm that is based on TIT-FOR-TAT, starts with generosity and ends up with conservative behaviour. Our simulation results showed that this algorithm could prolong its network lifetime in competition with other networks.

Keywords: Wireless sensor network, Cooperation, selfishness, game theory;

1. Introduction

In some application of WSNs, different domains have been deployed in the same field and they are under control of different authorities. The most important advantage of authorities with these situations is to give each other free riding and ask others for free riding in order to prolong their network lifetime.

* Corresponding author. Tel.: +98-919-513-7455 fax: +98-3351-4704.
E-mail address: shamani@ut.ac.ir

doi:10.1016/j.procs.2013.06.147

This behaviour is due to the fact that transmitting a packet is the most energy depleting task in WSNs. If the sensors are able to send their data through multi-hops that are close to them, they will survive more. Would cooperation happen spontaneously? Or each of them would cheat on the other and try to exploit others for its own benefit. This is a critical question and the response to this question is available through game theory because it is the tool to analyze strategies between rational decision makers.

Game theory has been widely applied to solve these problems in adhoc and sensor networks. Two approaches have been formed to deal with them: 1) reputation and punishment 2) pricing and payment techniques [1]. However most mature studies belong to adhoc field and because of major differences between WSN and adhoc most approaches are not applicable on WSNs.

If nodes are not aware of their energy, spontaneous cooperation will happen. As soon as they become energy aware which is realistic assumption these days, they will act defectively because they know there is an end to this cooperation. We propose a novel algorithm which enforces cooperation among authorities and tries to be generous in the beginning of the game. Then it will become more conservative as sensors are close to the end of their life.

As far as we concerned, it is for the first time that cooperation is being evaluated in realistic situations where routing is considered to be hierarchical and topology is heterogeneous. An adaptive energy aware strategy which not only works based on the feedback of other authorities but also tries not to be exploitable facing selfish authorities. Additionally, it makes cooperation more feasible by its generous behaviour.

2. Related work

Cooperation in adhoc networks has been addressed differently. Some of the researchers found out how to deal with it through reputation and punishment based mechanisms like [2-5], while others encourage cooperation with pricing and reputation [6-9]. However in adhoc each node belongs to different authorities which don't have strict limitations of WSNs, moreover their nature is totally different, hence these approaches cannot work well in this area.

Nevertheless, the most similar paper in adhoc to our work could be [5] and the similarity is analysis of cooperation without incentives; also they used GTFT as reputation-punishment mechanism to obtain Nash equilibrium. Finally, while in our model sensors send data to sink stations through cluster heads; they randomly choose sets of nodes to communicate.

In [10], authors demonstrated that cooperation is not evolutionary stable and they proposed a (patient grim trigger) strategy which enforces cooperation by punishment. However they did not consider energy awareness in nodes and they have just studied packet forwarding. Furthermore their strategy is not adaptable and its behaviour changes after permanent iterations. Authors in [11] have proposed dynamic incentive mechanism based on evolutionary game, which seems unnecessary in the case of own interest of sensors and authorities, Although the main problem is that considering selfishness within one authority is an unrealistic situation in WSN, because selfish behaviour within single authority happens only when the node is compromised. Compromised nodes use selfish behaviour as a covering action and the incentive mechanism cannot enforce cooperation with malice.

In [12], which looks to be the extended version of [13], a different study in this area is presented. In both studies, it is stated that cooperation happens spontaneously in WSN and there is no need to enforce cooperation, which is on the contrary of other studies. However [12] showed that how self interests of sensors stimulate cooperation in WSN. Another point is that their study is not applicable in heterogeneous environment because as they have mentioned, increasing the nodes will decrease the percentage of cooperation and in heterogeneous environment we have virtually increased nodes. Furthermore a selfish network can easily prolong its lifetime as they have mentioned by a strategy which they called it smart. Moreover our presented study simulated in more realistic scenario which is cluster routing instead of minimum transmission energy routing which is out of practice.

3. Model assumption

We considered plenty of tiny, limited battery-power devices called sensors. These sensors are two types: normal sensors and advanced sensors. Both are battery powered but advanced sensors battery lifetime is twice more than the normal ones. We assume all sensors can communicate with each other, even if they are under control of different authorities which means that interoperability is guaranteed. We assume there is no packet loss, and any packet drop is based on strategic decisions of sensors facing different authorities.

It is supposed that time is slotted, and all sensors have data to send per round. Another assumption is the similarity of all communication packets in size. Each domain has randomly deployed its sensors in the same filed. We assume there is only one sink in the middle of the field which receives all data.

The routing is supposed to be hierarchical. We used [14] as our routing protocol, which guarantees that energy is distributed by dynamic clustering and clusters heads aggregate reports from sensors and forward them to the sink. However, because of our heterogeneous topology we use SEP [15] as our cluster head election mechanism. Based on our routing, it is supposed that in each round a node can play the role of a sensor which sends data to a cluster head (CH) or the cluster head which receives data from its child and sends aggregated reports to the sink. So if a node becomes a sensor it can ask opponent network CH to send its data and if a node become CH it can accept to receive opponent sensor data to transmit it with aggregated data. It's worthy mention that all requests happen when opponent CH is closer than their own network nearest CH.

Based on these situations each node can have any strategy, like cooperative strategy which asks for others help and gives help, or non-cooperative strategy which doesn't ask for help and neither gives help, or behavioural strategy which takes next step based on the history of opponent movement.

Another assumption is that routing among domains is performed properly which means that sensors advertise correctly and each sensor can join the nearest cluster head. Sensors are supposed to be energy aware and their energy decreases based on their given tasks per round. Finally it is assumed that sensors are pre-programmed.

4. Sensor network prisoner dilemma

Game theory is a tool for modelling strategic decision making situations [16]; while players cannot enforce agreements through third parties and make decisions independently, they may cooperate; however any cooperation must be self-enforcing. Thus our model falls into the category of non-cooperative games [17]. We used iterated prisoners dilemma for modelling our game between parties where betrayal is same as non-cooperation and silence is cooperation. The reason of deploying this model among parties rather than sensors is due to the fact that parties are the ones looking for better payoff which is longer lifetime for their networks, instead of sensors. Sensors are tools for achieving this goal.

In the iterated prisoners dilemma when the game is played exactly N times and both of the players are aware of it, it is always optimal to defect in all rounds. Defection is the only Nash equilibrium. The proof is easy and it is inductive [17].

To enforce cooperation between two players, the number of rounds should be random or one of the players should be unaware of the end of. In this situation defection may no longer be a dominant strategy. Strategy which could stimulate cooperation should be behavioural [17]. Behavioural strategy performs next move based on the last observation. Game theory shows that when the probability of next round is more than a half, cooperation happens by using TFT strategy. To use this strategy in sensor networks we should add following features to the basic strategy: 1-Strategy should not be static and should adapt itself to opponent network. 2-Each node should decide locally without global feedback. 3-Strategy should not to be exploitable and should be able to stop selfishness. 4-Strategy should be scalable. 5-Strategy should stimulate cooperation.6-Strategy should be energy aware.

Based on TFT strategy, number one to four are provided and by generosity number five is reachable. Since we assume (1) the two networks are deployed randomly at the same time, (2) the number of both networks in terms of normal an advanced are the same, (3) and the routing and selection mechanism for cluster head is the same, hence the existence of next round for the two networks is approximately identical, which means if they act cooperatively to the end of the game, the life of their networks is approximately like each other. However each node should ask another network and give help to another network based on existence of next round. We make the existence of next round under conditions, which have been explained below; next round for normal node exists when:

$$(Ec > Etr(\text{to sink}) - \varepsilon) \;\&\&\; (Ec > ((Erc)*(\max \text{child}))+Etr(\max \text{dist})) \quad (1)$$

In the worst case, sensor should transmit its data to a cluster head which is very close to the sink. Because of that if the current energy (Ec) is higher than transmission energy to sink (Etr(to sink))or slightly less, then a sensor has enough energy to pass the next round. Furthermore there should be a cluster head to transmit reported data to the sink. While we don't know where a cluster head is and how many children it has, we consider the worst case which it placed on farthest point (Etr(max dist)) that is radius of rectangle and the number of children is the maximum number, too.
Next round for cluster head exists when:

$$Ec > ((Erc)*(\max \text{child})+Etr(\text{to sink}) \quad (2)$$

The worst case for a cluster head happens when it has the highest number of children to receive their data plus sending the aggregated data to the sink.

5. Adaptive energy aware cooperation algorithm

Each node starts with generosity so each sensor sets its cooperation probability Pc, cooperation rate Rc to max and defection rate Rd to min. When the node is at the end of its life, it will act conservatively in cooperation by dividing the Pc into two and setting Rc to min number and Rd to max.

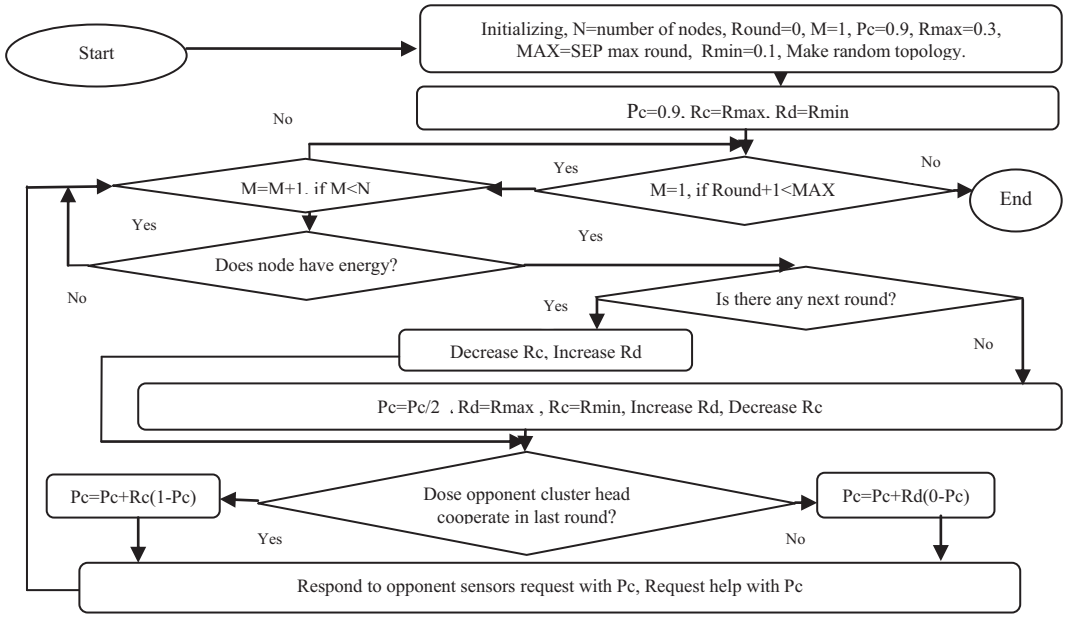

Fig. 1. Algorithm flowchart

5. Simulation

There are two sensor networks with separate operators which are distributed randomly on the ground. The simulation parameters are declared in table 1. Parameters are based on *hierarchical* routing [14] and *SEP* [15]. In order to evaluate this algorithm and strategy we programmed one of the two networks with our adaptive strategy. Then we placed four other networks opposed to ours.

Table1. Simulation parameters

Parameter	Value
Number of nodes per domain	50
Sensors distribution	Uniformly random
Area size	100*100 M
Sink position	50, 50
Normal Sensor Initial battery	0.5 U
Advanced Sensor Initial battery	1 U
Cluster head selection	*SEP*
Receive and send fixed cost	0.00022 U
Routing	Hierarchical
Advanced sensor percentage	10%

This evaluation is done in order to specify longer lifetime between two players. The Benefit of this evaluation is that longer lifetime is the best payoff and each party wants longer lifetime for its own network. For decreasing the impact of random topology we run each simulation twenty times and the results are the average numbers. Network 1: This network operates based on the opposite party feedback (like TFT). Network 2: At the beginning this network starts the game with suspicious and when facing cooperation of the opposite party, goes for feedback play. In this simulation we used *STFT* strategy. Network 3: This network plays irrational and makes decisions irrationally. Network 4: The goal of this network is exploit other network; it applies smart strategy like what [12] has been mentioned, it always asks for help but never gives help. To make this strategy smarter, it starts with cooperation to make reputation and after some random rounds plays defection and waits to see opponent feedback.

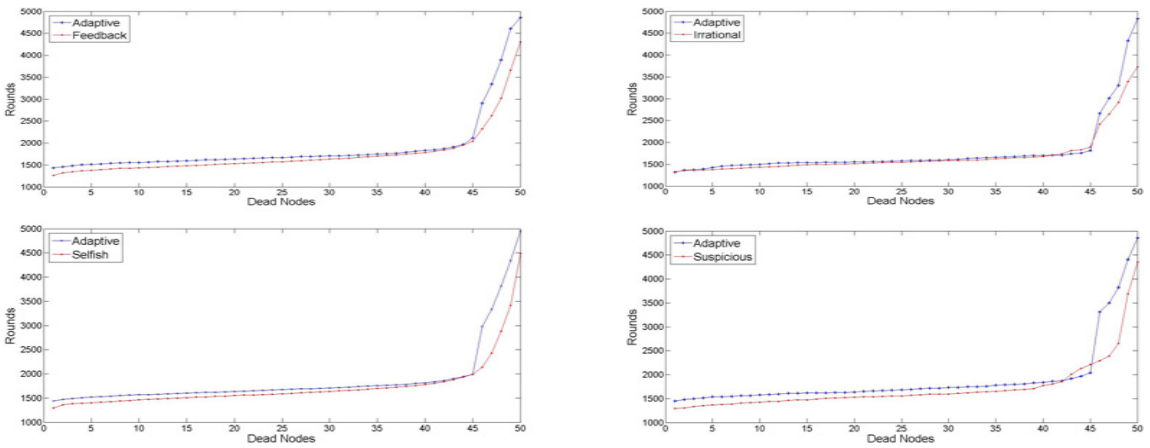

Fig. 2. Adaptive network in competition with other networks

It will change to cooperation after seeing the first defection, then repeats the same algorithm to the end. After the Adaptive network, Suspicious and Selfish networks respectively have the longest lifetime. The reason is that the Suspicious one starts with defection and the Selfish one acts smartly.

7. Conclusion

In this paper, we have addressed the problem of cooperation in packet forwarding between multi-domain networks. We have showed how spontaneous cooperation cannot happen since nodes are energy aware and we have demonstrated that without adapting a strategy, networks are too exploitable in facing selfish network. Furthermore we used TFT as our basic strategy and we added generosity and adaptability to our novel algorithm strategy to have more flexible and scalable strategy. Additionally it is worth mentioning that we used hierarchical routing and heterogeneous topology to have more realistic scenario. The adaptive energy aware strategy enforces cooperation between networks and decreases the generosity gradually after each round. When nodes reach to the end of their life they become conservative in cooperation. The simulation results demonstrate that our strategy can defeat irrational feedback, suspicious strategy and extend its lifetime. In Addition, selfish network which uses smart strategy cannot exploit our network and can only prolong its network lifetime for a short time.

However we used non-cooperative game theoretic model for the game (like some other researchers), but in reality, cooperative game is a possible situation when parties reach to an agreement before starting the game. We will investigate packet forwarding in cooperative games in our future research and we will also work on routing in multi-domain wireless sensor networks.

References

[1] Liu Hua. Cooperation in wireless networks with selfish users. PhD thesis, Southern California Univ; 2010.
[2] Marti S , Giuli T J, Lai K , Baker M. Mitigating routing misbehavior in mobile ad-hoc networks. In: Mobile Computing and Networking; 2000.
[3] Buchegger S, Boudec J L. Performance analysis of the CONFIDANT protocol. In: the 3rd ACM International Symposium on Mobile Ad Hoc Networking & Computing; 2002.
[4] Bansal S, Baker M. Observation-based cooperation enforcement in Ad-hoc networks. Technical Report, Computer Science Department, Stanforn University, Informal publication; 2003.
[5] Srinivasan V, Nuggehalli P, Chiasserini C, Rao R. Cooperation in Wireless Ad-hoc networ. In: IEEE Infocom; 2003.
[6] Buttyan L, Hubaux J P. Stimulating cooperation in self-Organizing mobile Ad Hoc networks. ACM Journal for Mobile Networks (MONET), vol. 8(5); 2003.
[7] DaSilva L, Srivastava V. Node Participation in Ad Hoc and peer-to-peer networks: A Game-Theoretic Formulatio. Workshop on Games and Emergent Behavior in Distributed Computing; 2004.
[8] Crowcroft J, Gibbens R, Kelly F, Ostring S. Modelling incentives for collaboration in mobile Ad-Hoc networks. Performance Evaluation 57; 2004.
[9] Ileri O, Mau S, Mandayam N. Pricing for enabling forwarding in self-configuring Ad Hoc networks. IEEE J. Selected areas in comunications; 2005.
[10] Crosby G V, Pissinou N. Evolution of cooperation in multi-class wireless sensor network. In: 32nd IEEE Conference on Local Computer Networks ;2007.
[11] Chen Z, Qiu Y, Liu J, Xu L. Incentive mechanism for selfish nodes in wireless sensor networks based on evolutionary game. Computers & Mathematics with Applications archive Volume 62 Issue 9, November; 2011.
[12] Buttyán L, Holczer T, Schaffer P. Spontaneous cooperation in multi-domain sensor network. In: Security and Privacy in Ad-hoc and Sensor Networks, Second European Workshop, Hungary; 2005.
[13] Felegyhazi M , Hubaux J P, Buttyan L. Cooperative packet forwarding in multi-domain sensor networks. In: the First International Workshop on Sensor Networks and Systems for Pervasive Computing; 2005.
[14] Heinzelman W R, Chandrakasan A P, Balakrishnan H. An application-specific protocol architecture for wireless microsensor networks. IEEE Transactions on Wireless Communications, vol. 1, no. 4, pp. 660–670; 2002.
[15] Smaragdakis G, Matta I, Bestavros A. SEP: a stable election protocol for clustered heterogeneous wireless sensor networks. In: Second International Workshop on Sensor and Actor Network Protocols and Applications; 2004.
[16] Fudenberg D, Tirole J. Game theory. MIT Press, 1991.
[17] Myerson R B. Game Theory: Analysis of conflict. Harvard University Press: Cambridge, Mass; 1991.