Game-Theoretic Approach to Mitigate Packet Dropping in Wireless Ad-hoc Networks

Diman Zad Tootaghaj, Farshid Farhat, Mohammad-Reza Pakravan, Mohammad-Reza Aref

Department of Electrical Engineering, Sharif University of Technology, Tehran , Iran

{diman_zad, farhat}@ee.sharif.edu
{pakravan, aref}@sharif.edu

Abstract—**One of the problems that cause severe degradation in system performance of ad-hoc network is dropping packets by misbehaving nodes. In this paper, we propose a security mechanism for detection of selfish or malicious nodes which try to drop information packets in routing phase also defending against collaborative attacks in which mobile nodes try to disrupt communication or save their power. Our proposed algorithm outranks previous schemes because it is resilient against colluding attacks and can be used in networks which wireless nodes use directional antennas. We also propose a game theoretic strategy, ERTFT for nodes to promote cooperation. In comparison with other proposed strategies like TFT, ours is resilient to systematic errors in detection of selfish nodes and does not lead to an unending death spiral.**

Keywords- Game theory, Ad-hoc Wireless Networks Security, Resilience to Selfishness, Promoting cooperation.

I. Introduction

Open and dynamic nature of network topology, shared wireless medium, limited resource constraints and lack of centralized control gives rise to many challenges in designing a security mechanism to promote nodes to cooperate in routing process. Each node in the network acts as an independent router to send data from source to destination. As a result, each node in the network can be a threat for security of system. In this paper we propose a security routing protocol based on DSR to detect selfishness of nodes and promote cooperation among them. First we introduce routing misbehavior of the nodes in section 2. In section 3 we present our protocol which is done in two steps, detecting selfish nodes and punishing selfish nodes, and simulation results of our own simulator, Game Theoretic Network Simulator (GTNS) are given in section 4.

II. Routing Misbehavior in ad-hoc networks

Non-cooperative actions of nodes are usually called selfishness; selfish nodes try to benefit from other nodes but refuse to forward packets of other nodes. In [1] Selfishness of nodes has been categorized into three types In this paper we consider all types of selfishness; we try to detect selfishness and not to forward data packets of selfish nodes.

III. Solutions to deal with Selfishness

There have been various techniques to prevent selfishness in literature. Most schemes try to detect and prevent misbehavior of individual nodes, therefore they are vulnerable when adversaries work together to form a collaborative attack. Furthermore, most schemes use overhearing mechanism introduced in [2] and [3] for detection. In this technique each node monitors its one-hop neighbors' transmissions by overhearing the wireless medium. Overhearing detection mechanism may fail because of collision, data loss and power restriction. Also this technique assumes that every node uses Omni-directional. Furthermore in this technique there is a possibility of applying a collaborative attack in which two or more colluding nodes want to disconnect network. In [4], the authors propose a mechanism to detect Byzantine failures in MANETs. Using this method both individual and collusive Byzantine can be detected, but this method would fail if there are malicious nodes in network which lie about receiving data packets. Dealing with selfishness in our DSR-like routing protocol is done in two steps: 1) detection of selfish nodes in the network. 2) Punishing the selfish nodes and promoting cooperation in the network. Next we explain each step.

A. ERTFT Detection mechanism

We assume that each node could generate its private/public keys and public keys of nodes are spread over the network by an independent public-key infrastructure (PKI). We also assume that after receiving packets, every node should send a confirmation packet to the previous hop neighbor. The confirmation from node i+1 to node i is

$$(16\ \mathrm{bytes\ of\ Data}, \mathrm{n}'_{\mathrm{i+1}}\mathrm{sID})_{\mathrm{n}'_{\mathrm{i+1}}\mathrm{sPrivate\ key}} \quad (1)$$

No other nodes in the network expect node $\mathrm{n_{i+1}}$can send this confirmation packet; also concatenating 16 bytes of data prevents replay attacks. If node $\mathrm{n_i}$ has not received this confirmation packet from $\mathrm{n_{i+1}}$ within a timeout it should mark $\mathrm{n_{i+1}}$ as a selfish node, find another route to the destination and mark the action of $\mathrm{n_{i+1}}$ as a non-cooperative action. Changing route by intermediate nodes is based on Locally Multipath Adaptive Routing protocol [5] that could finally find proper route without any selfish nodes to the destination. If it does not find another route it should send a Route Search packet to the previous hop, so the previous hop should find another path to the destination. In this case if we don't get acknowledgement (ACK) from the source node we are sure that every intermediate node has received confirmation packets, and we can start binary search algorithm to detect colluding attack. In order to reduce additional routing overhead caused by ERTFT detection scheme, we assume that the selfish nodes of types 1,2 or 3 do not show a lot of time-varying behaviors and only for a fraction of the data packets intermediate nodes should send back confirmation packets.

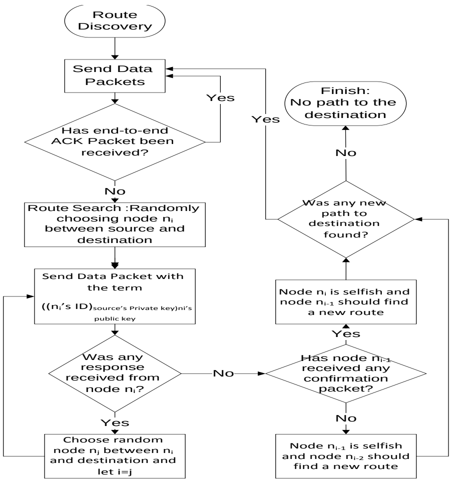
Route Discovery
Send Data Packets
Yes
Has end-to-end ACK Packet been received?
No
Route Search :Randomly choosing node n_i between source and destination
Send Data Packet with the term
$((n_i$'s ID$)_{\text{source's Private key}})_{n_i\text{'s public key}}$
Was any response received from node n_i?
Yes
Choose random node n_j between n_i and destination and let i=j
No
Has node n_{i-1} received any confirmation packet?
No
Node n_{i-1} is selfish and node n_{i-2} should find a new route
Yes
Node n_i is selfish and node n_{i-1} should find a new route
Was any new path to destination found?
Yes
No
Finish: No path to the destination

Figure 1. Flowchart of different steps for detection of selfishness by source node

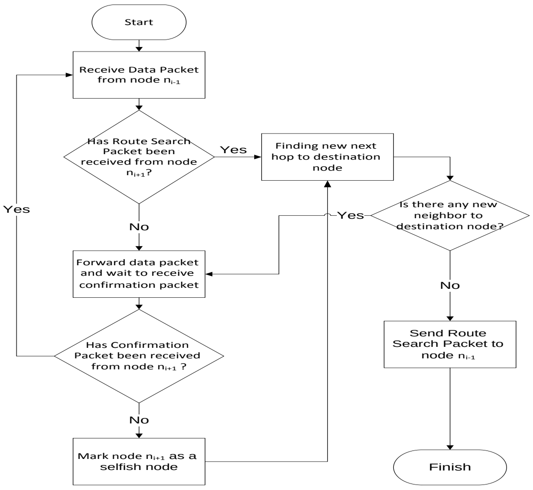
Start
Receive Data Packet from node n_{i-1}
Has Route Search Packet been received from node n_{i+1}?
Yes
Finding new next hop to destination node
Is there any new neighbor to destination node?
Yes
No
Send Route Search Packet to node n_{i-1}
Finish
No
Forward data packet and wait to receive confirmation packet
Has Confirmation Packet been received from node n_{i+1} ?
Yes
No
Mark node n_{i+1} as a selfish node

Figure 2. Flowchart of different steps for detection of selfishness by intermediate node

Fig. 1 and Fig. 2 show flowchart of different steps that source node and intermediate nodes should take to detect selfishness.

B. Cooperation enforcement under game theoretic model

We consider that every two neighbor nodes in the network are involved in a packet forwarding game, which can be modeled by repeated prisoner's dilemma. As we don't know when the game will finish, we can assume that every two nodes in network are playing infinitely repeated prisoner's dilemma.

1) ERTFT Strategy for repeated prisoner's dilemma

Tit for tat, is a highly effective strategy for repeated prisoner's dilemma [6]. While it has been shown that the strategy is optimal, but in an ad-hoc network if two nodes play tit for tat, and one of them mistakenly detects its opponent's action defective, both player will choose defection in every game cycle. To solve this problem, the error resilient tit for tat ERTFT strategy is proposed. In ERTFT, in addition to every neighbor's previous action, every node saves its own previous action too. So it can avoid punishing other nodes because of its own action. ERTFT strategy for player p_i can be represented as

$$p_{\mathrm{i}}\colon \begin{cases} \text{at t} = 1 & \text{plays C} \\ \mathrm{t} > 1 \;\; plays\ D\ if \begin{cases} h_c^{t-1} = \{D, C\} \\ \text{or} \\ h_c^{t-1} = \{D, D\}\ \ and\ h_c^{t-2} = \{\mathrm{D}, \mathrm{C}\} \end{cases} \\ \mathrm{t} > 1 & plays\ C\ otherwise \end{cases}$$

Where in h_c^{t-1} the first argument shows the component of the player's action, and the second argument shows the player's own action. Next we will find the thresholds for nodes that have best effect in term of power consumption to play cooperative or selfish.

Proposition [6]: In an infinitely repeated game with $\delta < 1$ if a player can not increase its payoff at some history by a one-step deviation; it cannot increase its payoff by n-step deviation. It means: $\mathrm{U}^{1\mathrm{SD}} \leq \mathrm{U}^{\mathrm{c}} \rightarrow \mathrm{U}^{\mathrm{nSD}} \leq \mathrm{U}^{\mathrm{c}}$. So it is sufficient to investigate if one step deviation would give more payoff than following the ERTFT strategy or not. Assume prisoner's dilemma with payoffs shown in table 1:

TABLE I. ERTFT STRATEGY PAYOFFS

	C	D
C	$\alpha_1 - \alpha_2, \alpha_1 - \alpha_2$	$-\alpha_2, \alpha_1$
D	$\alpha_1, -\alpha_2$	0,0

Where α_1 is the payoff of own forwarded-packets by the neighbors and α_2 is the payoff of the neighbors' packets forwarding. Assume that traffic of nodes has uniform distribution. If the game is played infinitely, each player values the sequence $(\mathrm{w}_1, \mathrm{w}_2, \ldots.)$ by

$$\mathrm{U} = \sum_{\mathrm{t}=1}^{\infty} \delta_{\mathrm{i}}^{\mathrm{t}-1} \mathrm{w}_{\mathrm{t}} \qquad 0 < \delta < 1 \tag{2}$$

In which w_{t} is the action of player in time t, and $\delta_{\,i}$ is discount factor between 0 and 1. In this paper we assume that δ_i is every node's power ratio defined by

$$Power\ ratio = \frac{\text{Instantaneous}\ power\ of\ node\ i}{Maximum\ power} \tag{3}$$

In other words, based on energy levels, nodes will evaluate their future payoffs. If their energy level is low they don't care about their future payoff. But when their energy level is max, long time payoff has the same value as short term payoff.

If both players play ERTFT payoff of one step deviation is defined as

$$\mathrm{U}^{\mathrm{D}} = \alpha_1 + (-\alpha_2)\delta + \delta^2 + \delta^3 + \cdots \tag{4}$$

But if players play ERTFT their payoff is

$$\mathrm{U} = 1 + \delta + \delta^2 + \delta^3 + \cdots \tag{5}$$

Players have motivation to deviate from ERTFT strategy when

$$\alpha_1 + (-\alpha_2)\delta > 1 + \delta \rightarrow \;\; \delta < \frac{\alpha_1 - 1}{\alpha_2 + 1} \tag{6}$$

I. SIMULATIONS

To investigate ERTFT behavior, the algorithm is implemented in GTNS: game theoretic network simulator. To compare the performance of the strategies, we have considered packet delivery ratio, total power of network at the end of simulation, number of selfish nodes of type1 and 2 and number of ad-hoc nodes at the end of simulation.

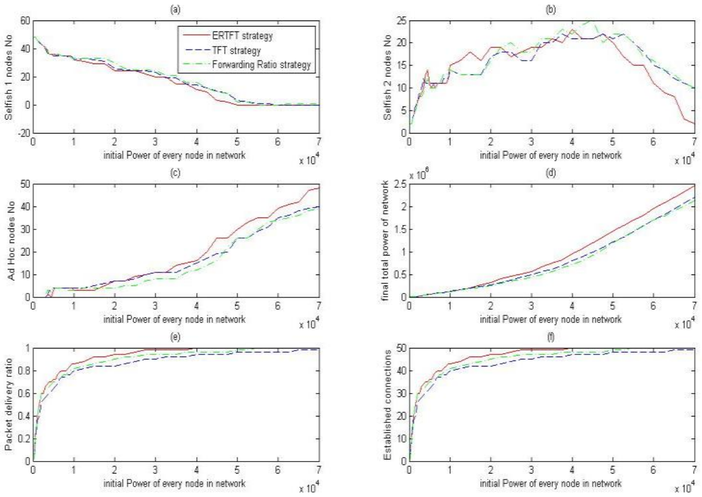

Figure 3. a) Number of selfish nodes of type1 b) Number of selfish nodes of type2 c) Number of ad-hoc nodes d) Final total power of network e) Packet delivery ratio f) Established Connections in the end of simulation in three strategies: ERTFT, TFT and Forwarding Ratio in scenario1.

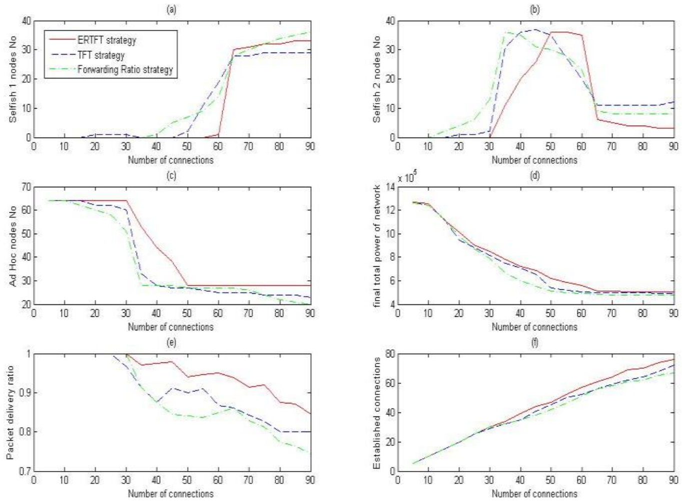

Figure 4. a) Number of selfish nodes of type1 b) Number of selfish nodes of type2 c) Number of ad-hoc nodes d) Final total power of network e) Packet delivery ratio f) Established Connections in the end of simulation in three strategies: ERTFT, TFT and Forwarding Ratio in scenario2.

Three game theoretic strategies have been employed: The TFT, the Packet forwarding ratio strategy [7], and the ERTFT strategy. We have added 1 percent error in detection of selfish nodes in the network. Furthermore we have simulated two scenarios to compare the performance of these three strategies: The reported results are the average of ten random traffic runs.

Scenario1: In the first scenario, a sample network of 50 nodes randomly placed over a 1000*500 m^2 area with coverage area of 200 meters have been used and 50 traffics are initiated randomly between 50 randomly selected pairs. At the start of simulation none of nodes are selfish, but as simulation starts and power of nodes decrease some nodes become SN1 and some of them become SN2. We assume that the thresholds are $Th1 = MaxPower/2$ and $Th2 = MaxPower/4$. You can see packet delivery ratio, final total power of network, number of selfish nodes of type 1 and 2 and number of ad-hoc nodes in three strategies in Fig. 3(a-f) respectively. As you can see from figures when initial energy level of nodes is very low, nodes become selfish very soon and as a result ERTFT doesn't show better performance as this strategy does not punish nodes strictly, but when the initial power of nodes increases less nodes in network become selfish and ERTFT shows better performance.

Scenario2: In this scenario we used a sample grid network consisted of 64 nodes placed over a 350*350 m^2 area. The coverage area of each node is 98 meters. We have changed number of connections in network from 5 to 90 connections randomly Fig. 4(a-f) shows the simulation results for three strategies. When more than half of nodes in network become selfish ERTFT doesn't punish selfish nodes strictly and as a result ad-hoc nodes should consume more power and more ad-hoc nodes become selfish because their energy level decreases to the threshold of selfishness. In this case TFT strategy performs nearly the same as ours. But when number of selfish nodes is less than half nodes in network ERTFT performs better than the other two presented strategies.

II. Conclusion

This paper introduces a new game theoretic approach to detect selfishness and promote cooperation called ERTFT. Compared with other approaches our proposed scheme is resilient against collision and can defend against colluding attacks where nodes try to disrupt communication. After detecting selfish nodes in network we have proposed a game theoretic strategy ERTFT, for neighbor nodes which are participating in a packet forwarding game. The proposed strategy is resilient to systematic error in detection of selfish nodes and unlike other previous strategies like TFT won't go to an unending loop of noncooperation. ERTFT outperforms TFT or FR strategy specially when the initial power of nodes in network is high or number of selfishness in network is low.

References

[1] P. Michiardi, R. Molva, "Simulation-based Analysis of Security Exposure in Mobile Ad-hoc Networks", in Proc. of European Wireless Conference, 2002.

[2] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks", in Proc. Int. Conf. Mobile Computing and Networking, Boston, MA, Aug. 2000, pp. 255-265.

[3] S. Buchegger, and J. Y. Le Boudec, "Performance analysis of the CONFIDANT protocol: Cooperation of nodes-Fairness in distributed ad hoc networks", in Proc. IEEE/ACM Workshop Mobile Ad Hoc Networks, Lausanne, Switzerland, June 2002, pp. 226-236.

[4] F. Farhat, M. R. Pakravan, M. Salmasizadeh, M. R. Aref, "Locally Multipath Adaptive Routing Protocol Resilient to Selfishness and Wormholes", ISPEC 2010, LNCS Volume 6047/2010, 187-200, 2010.

[5] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens, "ODSBR: An on-demand secure Byzantine resilient routing protocol for wireless ad-hoc networks", ACM Trans. Inf. Syst. Secur., 1-35, 2008.

[6] M. J. Osborne, "An Introduction to Game Theory", Oxford University Press, 2003.

[7] K. Komathy, P. Narayanasamy, "Study of Co-Operation among Selfish Neighbors in MANET under Evolutionary Game Theoretic Model", Signal Processing, Proceedings of ICSCN '07. International Conference on Digital Object Identifier, Page(s): 133 – 138, 2007.