

# Ranking Terrorists in Networks

Husslage, B.G.M.; Borm, P.E.M.; Burg, T.; Hamers, H.J.M.; Lindelauf, R.

*Publication date:*
2014

*Document Version*
Early version, also known as pre-print

No. 2014-028

# RANKING TERRORISTS IN NETWORKS: A SENSITIVITY ANALYSIS OF AL QAEDA'S 9/11 ATTACK

By

Bart Husslage, Peter Borm, Twan Burg,
Herbert Hamers, Roy Lindelauf

16 April, 2014

ISSN 0924-7815
ISSN 2213-9532

# Ranking terrorists in networks: a sensitivity analysis of Al Qaeda's 9/11 attack

Bart Husslage[1] Peter Borm[2] Twan Burg[2]
Herbert Hamers[2] Roy Lindelauf[3]

**Abstract**

All over the world intelligence services are collecting data concerning possible terrorist threats. This information is usually transformed into network structures in which the nodes represent the individuals in the data set and the links possible connections between these individuals. Unfortunately, it is nearly impossible to keep track of all individuals in the resulting complex network. Therefore, Lindelauf et al. (2013) introduced a methodology that ranks terrorists in a network. The rankings that result from this methodology can be used as a decision support system to efficiently allocate the scarce surveillance means of intelligence agencies. Moreover, usage of these rankings can improve the quality of surveillance which can in turn lead to prevention of attacks or destabilization of the networks under surveillance.

The methodology introduced by Lindelauf et al. (2013) is based on a game theoretic centrality measure, which is innovative in the sense that it takes into account not only the structure of the network but also individual and coalitional characteristics of the members of the network. In this paper we elaborate on this methodology by introducing a new game theoretic centrality measure that better takes into account the operational strength of connected subnetworks.

Moreover, we perform a sensitivity analysis on the rankings derived from this new centrality measure for the case of Al Qaeda's 9/11 attack. In this sensitivity analysis we consider firstly the possible additional information available about members of the network, secondly, variations in relational strength and, finally, the absence or presence of a small percentage of links in the network. We also introduce a case specific method to compare the different rankings that result from the sensitivity analysis and show that the new centrality measure is robust to small changes in the data.

*Keywords*: terrorism; network analysis; centrality measures; cooperative game theory.
*JEL classification*: C71.

[1]Department of Mathematics, Fontys University of Applied Sciences, P.O. Box 90900, 5000 GA Tilburg, The Netherlands.

[2]CentER and Department of Econometrics and Operations Research, Tilburg University, P.O. Box 90153, 5000 LE Tilburg, The Netherlands.

[3]Military Operational Art & Science, Netherlands Defense Academy, P.O. Box 90002, 4800 PA Breda, The Netherlands.

# 1 Introduction

Several instances of (almost succesfull) terrorist attacks in the West have led to relaxations of the restrictions on the retrieval, storage and search of databases that could indicate imminent threats. For instance, think of Umar Farouk Abdulmutallab's attempt at blowing up a Detroit bound airliner (i.e., the 'underwear-bomber') or Quazi Mohammad Rezwanul Ahsan Nafis 2012 attempt at attacking the Federal Reserve Bank of New York. The amount of data that becomes available for the analysis of terrorist related incidents increases. These data contain among others information on both the characteristics of individuals as well as data on the communication between these individuals (cf. Lindelauf et al. (2013)).

Traditionally such data are viewed and analyzed as network data, i.e., members of the network correspond to nodes and their interaction is modeled via links in the network. Standard centrality methods from the field of social network analysis, e.g., degree centrality (cf. Nieminen (1964)), betweenness centrality (cf. Freeman (1977)) and closeness centrality (cf. Borgatti and Everett (2006)), focus on finding key members taking only this network structure into account (cf. Wasserman and Faust (1994)). Recently, Lindelauf et al. (2013) introduced a game theoretic centrality measure that aids in the analysis of databases designed to detect terror threats by taking interactional information into account both on an individual and a coalitional level. This approach is in line with the game theoretic approach of measuring the quality of covert networks in Lindelauf (2011) and Lindelauf et al. (2009). In particular, context specific cooperative coalitional games are defined that reflect the situation at hand taking all available information about the network structure and the individual members and their relations into account. Next, the Shapley value (Shapley (1953)) is computed for the corresponding game to measure the importance of members of the network in order to construct a ranking of these members. A further advantage of using such a cooperative game theoretic centrality measure is that it allows for more flexibility in the sense that for each threat context a specific suitable game can be developed.

In this paper we further elaborate on the existing methodology introduced by Lindelauf et al. (2013). First, to each network we associate a monotonic weighted connectivity game. Here we relax the assumption of Lindelauf et al. (2013) that a coalition is only effective if all members of this coalition are connected in the network. In monotonic weighted connectivity games the effectiveness of a disconnected coalition is determined by the most effective connected subcomponent. This approach resembles reality more closely since partially connected coalitions may still pose a threat to the community. Subsequently, the Shapley value of the newly defined game is used to determine the importance of all members of the network and to construct a corresponding ranking.

Second, we revisit the case of Al Qaeda's 9/11 attack. We define an appropriate monotonic weighted connectivity game suitable to the network underlying the attack. This game incorporates information obtained from Krebs (2002) and Kean et al. (2002). Computing the Shapley value for this game leads to a ranking of the terrorists. Next, a sensitivity analysis is run to investigate the robustness of the ranking obtained. This is accomplished by slightly varying the data available on the members and the structure of the network.

To model individual strength the data on individuals are expressed as weights on the members of the network. In practice these weights are determined by an analyst that measures the importance, skills, or (financial) means available to a terrorist. Obviously, the determination

of such weights may differ from one analyst to another. Therefore, we want to see how robust the derived ranking is with respect to small variations in the weights. Concerning the network structure itself, obviously not all interactional data between members may be completely known, i.e., some links may be missing or may be obsolete. Therefore we perform a second type of sensitivity analysis to see how robust our ranking is with respect to the addition or deletion of a small percentage of the links in the network. Finally, some of the interactions between members may be considered more important than others, i.e., the relational strength may differ for each interaction (e.g., email communication, exchanging explosive materials). Therefore we also perform a third type of sensitivity analysis to see how robust our ranking is with respect to changes in the weights assigned to interactions.

The sensitivity analysis compares the rankings obtained by slightly perturbing the data to the ranking found for the unperturbed data using a tailor-made comparison method on rankings. For an overview on general comparison methods on rankings we refer to Su and Dong (1998) and Fagin et al. (2003). We find that the ranking based on the new game theoretic centrality measure is robust to small changes in the data.

The structure of this paper is as follows. Section 2 formally associates a monotonic weighted connectivity game to each network on the basis of data on characteristics of individuals and interactions. Subsequently, using the Shapley value, a game theoretic centrality measure and a corresponding ranking is defined. In Section 3 we perform a sensitivity analysis of this centrality measure using data of Al Qaeda's 9/11 attack. In Section 4 we summarize the main conclusions of the sensitivity analysis.

## 2 A new game theoretic centrality measure

A network can mathematically be represented by a graph $G = (N, E)$, where the node set $N$ represents the set of members of the network and the set of links $E$ consists of all relationships that exist between these members. The existence of a relationship between member $i$ and $j$ is denoted by $ij \in E$. For a coalition $S \subseteq N$, the subnetwork $G_S$ consists of the members of $S$ and its links in $E$, i.e., $G_S = (S, E_S)$ where $E_S = \{ij \in E | i, j \in S\}$.

A cooperative game in coalitional form is a pair $(N, v)$, where $N$ denotes the finite set of players and $v$ is a function that assigns to each coalition $S \subseteq N$ a value $v(S)$, which can be interpreted as the effectiveness of the coalition. By definition $v(\emptyset) = 0$. The central issue is how to adequately allocate $v(N)$, the effectiveness of the grand coalition, over all players. Thus, implicitly measuring to what extent each player is responsible for the total effectiveness of the grand coalition. The Shapley value (Shapley (1953)) of a cooperative game $(N, v)$ allocates $v(N)$ by averaging marginal contributions of a player to the different coalitions[1].

Following Lindelauf et al. (2013) the idea is to create a game that takes into account the structure of the network $G = (N, E)$, individual strengths (e.g., special skills) of the members of the network, summarized by $\mathcal{I} = \{w_i\}_{i \in N}$ with $w_i \geq 0$, as well as the relational strength (e.g., communication) between members of the network, summarized by $\mathcal{R} = \{k_{ij}\}_{ij \in E}$ with $k_{ij} \geq 0$.

[1]Let $\sigma = \sigma_1 \sigma_2 \cdots \sigma_N \in \Pi$ be an ordering of the players in the grand coalition $N$. If player $i$ is at position $k$, i.e., $\sigma_k = i$, then its marginal contribution $m^\sigma(i)$ is defined as $m^\sigma(i) = v(\{\sigma_1, \ldots, \sigma_k\}) - v(\{\sigma_1, \ldots, \sigma_{k-1}\})$, i.e., the extra value that player $i$ contributes to the already established coalition $\{\sigma_1, \ldots, \sigma_{k-1}\}$. Since the marginal contribution depends on the ordering $\sigma$, we average over the set of all possible orderings $\Pi$, resulting in the Shapley value of player $i$: $\varphi_i(v) = \frac{1}{n!} \sum_{\sigma \in \Pi} m^\sigma(i)$.

A coalition $S \subseteq N$ is called a connected coalition if the network $G_S$ is connected, otherwise $S$ is called disconnected. We define a *monotonic weighted connectivity game* $(N, v^{\text{mwconn}})$ with respect to network $G = (N, E)$ based on $\mathcal{I}$ and $\mathcal{R}$ in the following way. For a connected coalition $S$ we define

$$v^{\text{mwconn}}(S) = \begin{cases} f(S, \mathcal{I}, \mathcal{R}) & \text{if } |S| > 1 \\ 0 & \text{otherwise,} \end{cases} \tag{1}$$

where $f$ is a context specific and tailor-made non-negative function depending on $S$, $\mathcal{I}$ and $\mathcal{R}$ which measures the effectiveness of coalitions in the network. It can be chosen to best reflect the situation and information at hand. For a coalition $S$ that is disconnected we define

$$v^{\text{mwconn}}(S) = \max_{T \subset S,\ T \text{connected}} v^{\text{mwconn}}(T). \tag{2}$$

Observe, that the value of each disconnected coalition is based on the most effective connected component of this coalition. For the purpose of this paper we define $f(S, \mathcal{I}, \mathcal{R})$ by

$$f(S, \mathcal{I}, \mathcal{R}) = \left( \sum_{i \in S} w_i \right) \cdot \max_{ij \in E_S} k_{ij}. \tag{3}$$

This specific choice can be motivated for terrorist cells in which we need to focus on the total operational strength of the cell as well as the most prominent line of communication between members.

Subsequently, the game theoretic centrality measure $C^{\text{m}}$ of member $i$ in network $G = (N, E)$ based on $\mathcal{I}$ and $\mathcal{R}$ is defined by

$$C^{\text{m}}(i) = \varphi_i(v^{\text{mwconn}}),$$

where $\varphi_i(v^{\text{mwconn}})$ is the Shapley value of member $i$ in the game $v^{\text{mwconn}}$. The corresponding ranking of all members of $N$ will be denoted by $R^{\text{m}}$. The centrality measure $C^{\text{m}}$ is illustrated in the following example.

### Example: the centrality measure $C^{\text{m}}$

Consider the network in Figure 1 in which the five members are denoted by the letters $A$ to $E$ and the six links represent the relationships between these five members. This defines $G = (N, E)$.

Suppose that individual information is available only for member $E$. He was involved in a previous attack and has financial means to support a potential new attack. Counterterrorism analysts will take this observation into account when assigning weights to the members. Here we assume that member $E$ is assigned a weight of 4 and all other members are assigned a weight of 1, see Figure 2. This defines $\mathcal{I}$.

Additionally, suppose it is observed that member $A$ and $B$ communicate more frequently than the other members of the network. Here we assume that link $AB$ is assigned a weight of 3 and all other links are assigned a weight of 1, see Figure 2. This defines $\mathcal{R}$.

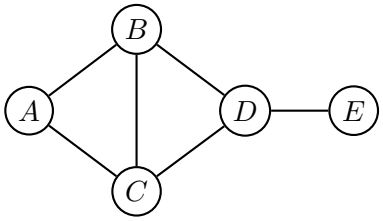


**Figure 1:** Example of a network.

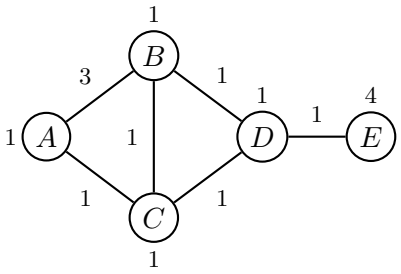


**Figure 2:** Example of a network with information on individual and relational strengths.

Using (3) the values $v^{\text{mwconn}}(S)$ as defined in (1) and (2) can be computed for each coalition $S$. Table 1 provides these values[1] for each of the 32 coalitions in $N = \{A, B, C, D, E\}$. The resulting centrality measure $C^{\text{m}}$ of each member is presented in Table 2. The corresponding ranking $R^{\text{m}}$ is given by $(BADEC)$. As expected, the additional information used ensures that member $A$ and $B$ attain a high ranking, identifying $A$ as the key player in this network. Note that the peripheral position of $E$ in the network does decrease its importance, whereas the weight of $E$ does increase the importance of $D$ since the latter establishes a connection between member $B$ and $E$.

| Coalitions | $\emptyset$ | $\{C\}$ | $\{D\}$ | $\{E\}$ | $\{C,D\}$ | $\{C,E\}$ | $\{D,E\}$ | $\{C,D,E\}$ |
|---|---|---|---|---|---|---|---|---|
| $\emptyset$ | 0 | 0 | 0 | 0 | 2 | 0 | 5 | 6 |
| $\{A\}$ | 0 | 2 | 0 | 0 | 3 | 2 | 5 | 7 |
| $\{B\}$ | 0 | 2 | 2 | 0 | 3 | 2 | 6 | 7 |
| $\{A,B\}$ | 6 | 9 | 9 | 0 | 12 | 9 | 21 | 24 |

**Table 1:** The value $v^{\text{mwconn}}(S)$ for each coalition in the example in Figure 2.

| Member | Centrality measure $C^{\text{m}}$ |
|---|---|
| $A$ | 6.1667 |
| $B$ | 6.4167 |
| $C$ | 1.7500 |
| $D$ | 5.5833 |
| $E$ | 4.0833 |

**Table 2:** The centrality measure $C^{\text{m}}$ for the example in Figure 2.

□

[1] In this compact (but non-standard) notation, e.g., the cell corresponding to row $\{B\}$ and column $\{D, E\}$ represents that $v^{\text{mwconn}}(\{B, D, E\}) = 6$.

## 3 Sensitivity analysis of Al Qaeda's 9/11 attack

On September 11th, 2001, four commercial airplanes were hijacked by members of Al Qaeda. Two of these planes were directed to fly into the Twin Towers of the World Trade Center in New York, a third plane flew into the Pentagon and a fourth plane crashed somewhere in Pennsylvania. The network $G = (N, E)$ of the 19 hijackers directly responsible for this attack is depicted in Figure 3 (see Krebs (2002)). The colors in the network refer to the different flights of American Airlines (AA) and United Airlines (UA); i.e., AA-77 (white), AA-11 (lightgray), UA-93 (gray) and UA-175 (darkgray).

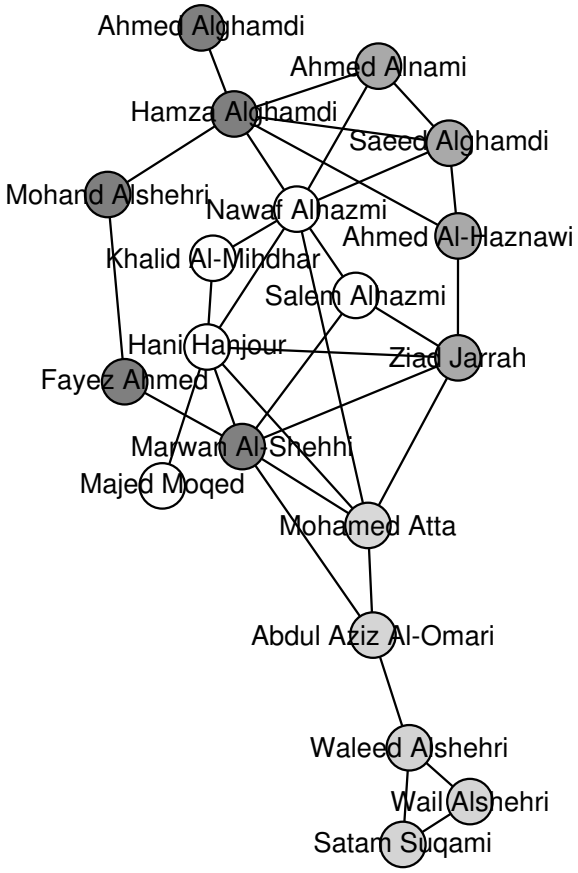


**Figure 3:** Operational network of hijackers of Al Qaeda's 9/11 attack. AA-77 (white), AA-11 (lightgray), UA-93 (gray) and UA-175 (darkgray).

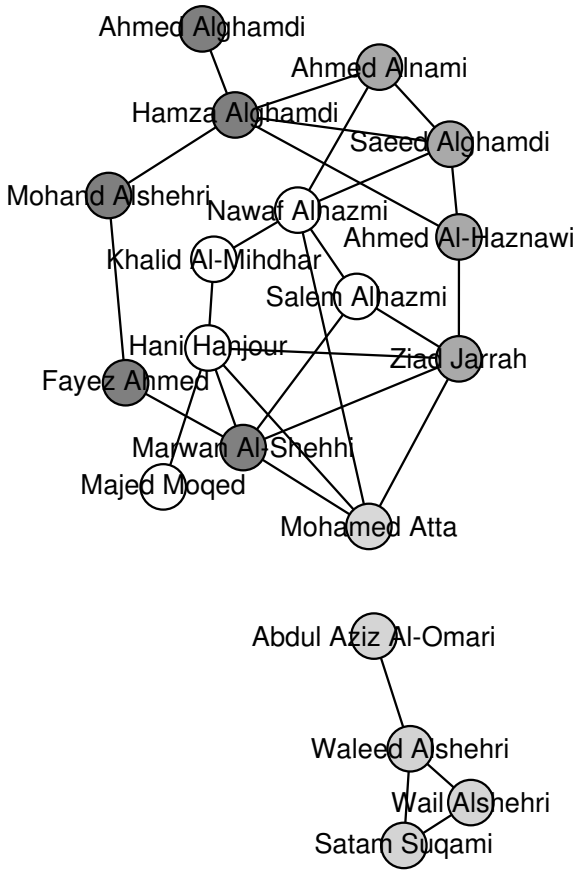


**Figure 4:** Operational network of hijackers of Al Qaeda's 9/11 attack with four (random) links removed. AA-77 (white), AA-11 (lightgray), UA-93 (gray) and UA-175 (darkgray).

Table 3 presents the weight assigned to each hijacker based on additional data, like affiliation and attending terrorist training camps, extracted from the 9/11 commission report (Kean et al. (2002)). This table provides $\mathcal{I} = \{w_i\}_{i \in N}$. No additional information on relational strength is given, so for $\mathcal{R} = \{k_{ij}\}_{ij \in E}$ we propose $k_{ij} = 1$ for all $ij \in E$.

| Hijacker | Weight | Hijacker | Weight |
|---|---|---|---|
| Ahmed Alghamdi | 1 | Nawaf Alhazmi | 2 |
| Hamza Alghamdi | 1 | Khalid Al-Mihdhar | 3 |
| Mohand Alshehri | 1 | Hani Hanjour | 1 |
| Fayez Ahmed | 1 | Majed Moqed | 1 |
| Marwan Al-Shehhi | 3 | Mohamed Atta | 4 |
| Ahmed Alnami | 1 | Abdul Aziz Al-Omari | 1 |
| Saeed Alghamdi | 1 | Waleed Alshehri | 1 |
| Ahmed Al-Haznawi | 1 | Satam Suqami | 1 |
| Ziad Jarrah | 4 | Wail Alshehri | 1 |
| Salem Alhazmi | 1 | | |

**Table 3:** Weight assigned to each hijacker of Al Qaeda's 9/11 attack.

We use the function $f(S, \mathcal{I}, \mathcal{R})$ of (3) to determine the game $v^{\text{mwconn}}$, the centrality measure $C^{\text{m}}$ and the corresponding ranking $R^{\text{m}}$. The resulting ranking $R^{\text{m}}$ is provided in Table 4. Since surveillance and observation capacity is almost always a limiting factor, it is valuable to identify the key players in the network to optimally allocate these scarce resources. We therefore focus on the top-5 of the ranking.

To perform a sensitivity analysis on the ranking $R^{\text{m}}$ for this operational network we need to be able to compare different rankings with one another. For example, consider the situation where not all lines of communication in the operational network have been discovered, resulting in the network in Figure 4 in which 4 (random) links have been removed. Note that the network in Figure 4 is disconnected. Ranking $R_1$ in Table 5 presents the ranking of the hijackers corresponding to the network in Figure 4. The difference between the rankings $R^{\text{m}}$ and $R_1$ is represented by the number $\rho(R^{\text{m}}, R_1) \geq 0$, which is computed as follows. First, each hijacker in the original ranking $R^{\text{m}}$ is assigned a value based on its position in the ranking, see Table 6. Then the sum of the values of all hijackers that leave the top-5 in $R^{\text{m}}$ and enter the top-5 in $R_1$ is taken. The values assigned to the positions are chosen in such a way that highly ranked hijackers that leave the top-5 in $R^{\text{m}}$ and lowly ranked hijackers that enter the top-5 in $R_1$ result in a large value of $\rho$. This value of $\rho$ will be relatively low when two rankings do not differ too much. Note that $\rho(R^{\text{m}}, R_1) = \frac{1}{5} + \frac{1}{14} = \frac{19}{70} \approx 0.2714$ in our example since Hani Hanjour, with a value of $\frac{1}{5}$, leaves the top-5 in $R^{\text{m}}$ and Khalid Al-Midhar, with a value of $\frac{1}{14}$, enters the top-5 in $R_1$.

In our sensitivity analysis we will first focus on network structure and vary the number of links present in the network. We will not only investigate scenarios in which a percentage of the links is removed from the network, but also scenarios in which a percentage of the links is added to the network. Hence, we consider the situation when an intelligence agency has gathered information about the structure of some network but does not know for sure whether all lines of communication are discovered or play a role in the network. Second, we will focus on individual and relational strength and investigate scenarios in which different weights on individuals and links are used. In practice field experts have to decide on the exact heights of the weights assigned to individuals and links. The magnitude of such weights should reflect individual characteristics (e.g., financial means, skills to create an explosive) or the importance

| Ranking $R^{\mathrm{m}}$ |
|---|
| Mohamed Atta |
| Ziad Jarrah |
| Marwan Al-Shehhi |
| Nawaf Alhazmi |
| Hani Hanjour |
| Khalid Al-Midhar |
| Abdul Aziz Al-Omari |
| Hamza Alghamdi |
| Waleed Alshehri |
| Ahmed Al-Haznawi |
| Salem Alhazmi |
| Fayez Ahmed |
| Saeed Alghamdi |
| Mohand Alshehri |
| Ahmed Alnami |
| Majed Moqed |
| Ahmed Alghamdi |
| Satam Suqami |
| Wail Alshehri |

**Table 4:** Ranking for the network in Figure 3 based on $C^{\mathrm{m}}$.

| Ranking $R_1$ |
|---|
| Ziad Jarrah |
| Mohamed Atta |
| Marwan Al-Shehhi |
| Nawaf Alhazmi |
| Khalid Al-Midhar |
| Hani Hanjour |
| Hamza Alghamdi |
| Ahmed Al-Haznawi |
| Salem Alhazmi |
| Fayez Ahmed |
| Saeed Alghamdi |
| Mohand Alshehri |
| Ahmed Alnami |
| Majed Moqed |
| Ahmed Alghamdi |
| Waleed Alshehri |
| Satam Suqami |
| Wail Alshehri |
| Abdul Aziz Al-Omari |

**Table 5:** Ranking for the network in Figure 4 based on $C^{\mathrm{m}}$.

| Position | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| Value | 1 | 4/5 | 3/5 | 2/5 | 1/5 | 1/14 | 2/14 | 3/14 | 4/14 | 5/14 |
| Position | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | |
| Value | 6/14 | 7/14 | 8/14 | 9/14 | 10/14 | 11/14 | 12/14 | 13/14 | 1 | |

**Table 6:** Value assigned to each position in ranking $R^{\mathrm{m}}$.

of a specific type of communication (e.g., email communication, exchanging explosive materials). Obviously, it is difficult to quantify these numbers accurately. Therefore, we also want to check what impact minor changes in the assigned weights have on the ranking of the hijackers.

With respect to network structure, we have run 1000 simulations in which we randomly added or deleted up to 4 links and computed the resulting values of $\rho$. With respect to individual strength, we have run 1000 simulations in which we set the weight for each of 4 randomly selected individuals randomly equal to 1, 2, 3 or 4. To investigate the effect of relational strength, we have increased the weight of a single link to 4, with the rest of the weights kept to 1. Since the network contains only 33 links, we computed the value of $\rho$ for each scenario, i.e., for this part no simulations were needed. The results of this sensitivity analysis are depicted in Figure 5. Note that (another) simulation shows that the expected value of $\rho$ is approximately 4.18 when $R_1$ would be a random ranking of the 19 members which does not use network structure, individual strength and relational strength.

From Figure 5 it follows that the ranking resulting from the monotonic weighted connectivity game is robust to small changes in the network structure and the weighing of links and members. In all but one case, the value of $\rho$ is significantly less than the value $\rho = 4.18$ obtained by a random ranking. Note that $\rho \geq \frac{1}{5} + \frac{1}{14} \approx 0.27$ in case one hijacker is replaced in the original

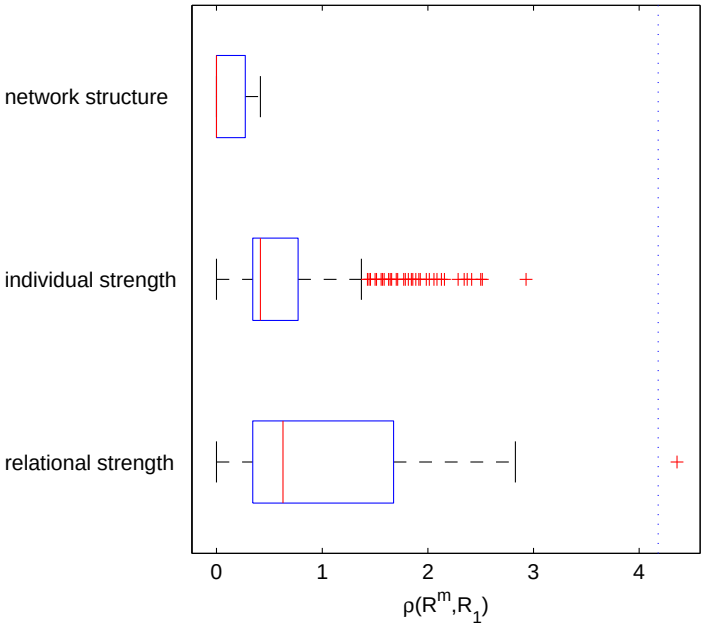


**Figure 5:** Boxplots of $\rho$-values for the sensitivity analysis of Al Qaeda's 9/11 network on network structure, individual strength and relational strength.

top-5 by a hijacker not yet present in the top-5. Two hijackers leaving the original top-5 will yield a value of $\rho$ of at least $\frac{1}{5} + \frac{2}{5} + \frac{1}{14} + \frac{2}{14} \approx 0.81$. For three hijackers this value is at least 1.63.

When varying the number of links present in the network the top-5 of the original ranking is seen to remain virtually unchanged. In 50% of the cases the ranking remains unchanged and in another 25% of the cases only one hijacker leaves the top-5. When varying the weights assigned to individuals in the network the top-5 differs slightly from the original ranking. In almost 75% of the cases only one hijacker in the top-5 is replaced. In most other cases at most two hijackers are replaced. Even the (relatively few) outliers are seen to differ significantly from the value of $\rho$ when using a random ranking. The original ranking is seen to be more sensitive to varying the weight of a single link. Although at most one hijacker in the top-5 is replaced in 50% of the cases, the remaining cases show more variability in the value of $\rho$. In one case the value of $\rho$ is even larger than the value of a random ranking. In this particular case the link between the lowest ranked hijackers Satam Suqami and Wail Alshehri is assigned a weight of 4, catapulting them into the top-5 and resulting in an extremely large value of $\rho$. The remaining rankings, however, all still outperform a random ranking.

We can conclude that $R^{\mathrm{m}}$ provides a ranking for the 9/11 network that is globally robust against link-changes as well as weight-changes. It will be clear that the methodology behind $R^{\mathrm{m}}$ can be applied to other data sets as well. These data sets need not be restricted to terrorist networks but could also apply to e.g. criminal networks. Moreover, variations in our choice of $f(S, \mathcal{I}, \mathcal{R})$ in (3) should be studied to better fit specific settings.

# 4 Conclusions

In this paper we propose a new type of ranking of terrorists in order to identify key players in terrorist networks. In particular, we use game theoretic centrality measures to construct such a ranking. These centrality measures do not only take the network structure into account, i.e., who communicates with whom, but also incorporate individual and coalitional characteristics, such as special skills, and relational characteristics, like frequency of communication. In particular, our new game theoretical centrality measure is based on monotonic weighted connectivity games that take into account the strength of connected subnetworks of terrorists, thus providing a more suitable model of real-life networks.

We tested the robustness of the rankings obtained using our new centrality measure by performing a sensitivity analysis on the ranking of the terrorists in Al Qaeda's 9/11 attack. In this analysis we run several types of simulations in which we either vary the network structure, i.e., the links present, or vary individual strength or relational strength. In each simulation a new ranking is constructed and this ranking is compared to the original ranking of the terrorists. To facilitate the comparison of rankings we use a tailor-made comparison method. It follows that the new game theoretic centrality measure is robust to small changes in the network structure, as well as to small perturbations in individual and relational strength.

Hence, the new game theoretic centrality measure takes all available information about the members of the network and their relations into account, incorporates the strength of connected subnetworks, and is robust to small changes in the available data, which makes it a promising measure to construct rankings of terrorists in real-life networks.

# References


Borgatti, S.P. and M.G. Everett (2006). A graph-theoretic framework for classifying centrality measures. *Social Networks*, **28**, 466–484.

Fagin, R., R. Kumar, and D. Sivakumar (2003). Comparing top k-lists. *SIAM Journal on Discrete Mathematics*, **17(1)**, 134–160.

Freeman, L.C. (1977). A set of measures of centrality based on betweenness. *Sociometry*, **40**, 35–41.

Kean, T.H., L.H. Hamilton, and R. Ben-Veniste (2002). *The 9/11 commission report, final report of the national commission on terrorist attacks upon the United States.* W.W. Norton and Company, Inc., New York.

Krebs, V.E. (2002). Uncloaking terrorist networks. *First Monday*, **7**.

Lindelauf, R.H.A. (2011). *Design and analysis of covert networks, affiliations and projects.* Ph. D. thesis, Tilburg University, Tilburg.

Lindelauf, R.H.A., P. Borm, and H. Hamers (2009). The influence of secrecy on the communication structure of covert networks. *Social Networks*, **31**, 126–137.

Lindelauf, R., H.J.M. Hamers, and B.G.M. Husslage (2013). Game theoretic centrality analysis of terrorist networks: the cases of Jemaah Islamiyah and Al Qaeda. *European Journal of Operational Research*, **229(1)**, 230–238.

Nieminen, J. (1964). On centrality in a graph. *Scandinavian Journal of Psychology*, **15**, 322–336.

Shapley, L. (1953). A value for n-person games. *Annals of Mathematics Studies*, **28**, 307–317.

Su, L.T., Chen H.L. and X.Y. Dong (1998). Evaluation of Web-based search engines from the end-user's perspective: A pilot study. *Proceedings of the ASIS Annual Meeting*, **35**, 348–361.

Wasserman, S. and K. Faust (1994). *Social network analysis, methods and applications.* Cambridge: Cambridge University Press.