On the Rationality and Optimality of Transportation Networks Defense — a Network Centrality Approach

Yaniv Altshuler, Rami Puzis, Yuval Elovici, Shlomo Bekhor, and Alex (Sandy) Pentland

Abstract Transportation infrastructures have recently gained increasing attention in the context of homeland security. Being both a main target for attacks as well as a method for carrying out such attacks, much effort is being allocated these days towards increasing our understanding regarding transportation networks [18]. Specifically, measuring and predicting human mobility patterns along the links of a transportation network has been of great importance to researchers in the field, as it contains the basic information needed in order to cope with transportation related threats more efficiently. Such threats can take for example the form of a group of terrorists trying to reach their target by car, or a truck filled with chemical or radioactive material. These threats require homeland security agencies to rapidly deploy monitoring or surveillance units in key junctions, dispatch air units to central locations etc. Clearly, carrying out this mission relies on the knowledge of what are those key traffic junctions, and how to deploy the existing (and always on shortage) resources most efficiently. Hitherto, producing the transportation data required for answering these questions was done off-line and relied heavily on expensive and time consuming surveying and on-field observational methods. Network Betweenness is known to be highly correlated with network load in communication and transportation networks. In this work we show how a specially designed Be-
tweenness Centrality measure that can be useful for optimizing locations of static or mobile monitoring equipment. Furthermore, we show that the accuracy of the estimations produced using this approach can be further enhanced when additional (pre-defined and known) properties of the network are taken into account, generating an augmented Mobility Oriented Betweenness Centrality measure. We demonstrate the efficiency of the proposed method both analytically and experimentally, using real world transportation network constructed using cellular phones data, that contains a high resolution network of the Israeli transportation system. We show that the traffic flow level that were measured using this expensive and complicated method can be accurately estimated using our proposed Augmented Betweenness technique. As a result, we can generate an efficient deployment scheme of monitoring units for this specific network, and calculate the percentage of traffic it monitors.

1 Introduction

Since the days of the Roman empire transportation networks have been one of the cornerstones for the strength and stability of states. Maintaining the availability of roads and the safety of travelers was always an important challenge for rulers and governments. Transportation systems in most of modern countries are considered nowadays relatively safe. However, maintaining their safety requires constant monitoring and law enforcement. With the increase in the complexity of transportation systems, combining various types of land, air and marine vehicles, both private and public, the challenge of monitoring them becomes both increasingly difficult and important. In fact, attackers and disturbing factors that threaten transportation networks usually get to their destination using this network as well. For example, a group of terrorists that are planning to carry out an attack (such as hijacking an airplane or exploding a subway station) will most likely get to their destination using some means of transportation. When it comes to their security profile, transportation networks, therefore, have a unique feature, being both a potential target for an attack and the mean to carry it.

Ideally, each transportation network (global, national and urban) should have been built while incorporating a monitoring station alongside each of its routes and intersections. This, however, is not feasible due to privacy reasons and financial and operational considerations. It is hence crucial to find deployment schemes for monitoring stations, that would analytically guarantee the maximization of traffic monitoring, using a limited number of monitoring units. Such a scheme could be used to calculate either a static deployment of large scale monitoring units, or a dynamic on-demand deployment that could be implemented as an urgent response for a specific threat. Ultimately, this system would provide the maximal detection probability of threat agents for a specific budget, or alternatively — minimal number of monitoring units for a pre-defined requested detection probability. These monitoring stations may be either police patrols, automatic units for detecting biologic, chemical or radiologic hazards, or any other monitoring units.
In order to produce efficient deployment schemes, the traffic pattern of the users of the transportation system must be thoroughly studied. The analysis of mobility trends and demands forecasting in transportation networks relies nowadays heavily on household survey data that provides the required input for calibrating the mathematical models that represent decisions people make related to travel [42]. However, a well known problem common to all interview-type surveys is non-response. Complex methods to correct for non-response have been developed, however, these alleviate the problem only partially [39].

As mentioned in [12], another limitation of household surveys is the need for active cooperation from the respondents, relying on their memory and patience. The need for active participation reduces the ability to capture complex travel and activity patterns, and the ability to collect data over a long period of time. The problems mentioned above, coupled with budget constraints, explain the fact that typical household surveys collect data regarding a period of merely one or two days for each household. As a result, there exists a strong need for finding an alternative mechanism of assessing mobility and traffic demand in transportation networks, one that could be used without the necessary, tedious and inaccurate process of surveying.

Combining this with the need for fast deployment optimization solutions, it is clear that in order to find an efficient optimization scheme that would satisfy all aspects of transportation related homeland security deployment problem we must resort to methods that rely on the analysis of the transportation network itself. Such a method can produce dynamic solutions to a variety of optimization systems, and do so in close to real time (using efficient heuristic search methods).

*Betweenness Centrality* (BC) stands for the ability of an individual node to control the communication flow in the networks [8,26]. Formally, for a node \( v \) it denoted the total portion of shortest-paths between every pair of nodes in the network that pass through \( v \) (see more details in Section 4). In recent years Betweenness was extensively applied for the analysis of various complex networks [10, 43] including among others social networks [40,46], computer communication networks [25,49], and protein interaction networks [16]. Holme [28] have shown that Betweenness is highly correlated with congestion in particle hopping systems. Extensions of the original definition of BC are applicable for directed and weighted networks [17,47] as well as for multilayer networks where the underlying infrastructure and the origin-destination overlay are explicitly defined [36].

In this work we discuss the applicability of BC and certain augmented types of it for the prediction of mobility patterns in transportation networks, and subsequent deployment optimization of monitoring units in the network. Specifically, we show that there is a strong positive correlation between the traffic that flows through a node in a transportation network and its BC measures. This in turn directly implies a positive correlation between a solution to the Betweenness optimization problem and the “collaborative monitoring units deployment problem”. In other words, this duality means that deployment schemes that obtain high Betweenness value are also guaranteed to better approximate the maximal monitoring probability deployment.

We define an optimization problem where the cost of deploying a set of monitoring units depends on the properties of routes and intersections they are deployed on.
(e.g. load, number of lanes, length). In contrast to the cost, effectiveness of monitoring units’ deployment can be measured as the net number of suspected agents (e.g. cars, trucks, ...) that have been inspected. We show that given a characterization of a potential attack (namely — the weighted graph that represents possible transportation measures the attacking agents may use) we can provide an efficient deployment scheme for the locations of monitoring units. Furthermore, we can also estimate the percentage of traffic this deployment would achieve. These two numbers put together and combined with the overall cost of a potential attack, yield a “rationality criterion” for investments in monitoring infrastructures, namely — measure of the benefit of the system compared to the expected damage it prevents (see Equations 4 and 6).

The rest of the chapter is organized as follows: Section 2 contains an overview of the related work in regards to homeland security and transportation. Section 3 describes the transportation dataset that was used in this study. Section 4 contains a technical discussion concerning the correlation between Betweenness Centrality and traffic flow. Our proposed approach for generating efficient deployment schemes is discussed in Section 5, containing first a theoretical basis, followed by a thorough empirical validation using our real-world transportation network dataset — a comprehensive transportation network of the Israeli roads and highways system, containing over 15,000 directed links. Two heuristic methods are presented, and their performance in terms of solution efficiency and computation time is discussed. A short discussion regarding the implications of our proposed method is presented in Section 6. A case study of various attack scenarios using the Israeli transportation network is discussed in Section 7 and concluding remarks appear in Section 8.

2 Related Work

Homeland security has become one of the dominant aspects with respect to Intelligence Transportation research since September 11. The importance of Transportation Systems and Technology with respect to homeland security and counterterrorism is discussed in details in official publications of the U.S. National Research Council [1, 2]. A survey of the homeland security threats and risks regarding transportation infrastructure can be found in [18].

For example, infectious disease outbreaks pose a critical threat to public health and national security [14, 19]. Utilizing today’s expanded trade and travel, infectious agents can be distributed easily within and across country borders as part of a biological terror attack, resulting in potentially significant loss of life, major economic crises, and political instability. Such threats stress even more the importance of a reliable and efficient transportation monitoring infrastructure. An example for mitigating this risk can be found in [33], where an attempt to create a “smart” and safer border is made.

With respect to land transportation, the main focus thus far had been on monitoring the transportation of hazardous materials. It is important to note that the vast
majority of works on these topics did not focus on the security oriented threats (such as preventing terrorists from hijacking these materials and using them in weapons) but rather, on efficient routing. Efficient routing of hazardous vehicles transportation involves determining what paths vehicles should take to minimize population exposure in the event of an accident. As pointed out in [48] many authors have developed algorithms and heuristics for solving various cases of the routing problem [11, 13, 15, 22, 51]. In addition, there exist a multitude of works that concern the problem of treating and analyzing the risk that stems from conveying hazardous materials using the national transportation infrastructure [23, 29, 38].

This work is the first attempt to address this issue from a different angle — trying to predict the traffic patterns of network users of an existing (and optionally dynamic) transportation infrastructure, and finding an approximation for the optimal deployment of monitoring units for it. In this sense, this work somewhat resembles the line of work that deals with risk assessment, albeit it is also accompanied with constructive recommendations for policy makers regarding the appropriate positions (and quantities) of monitoring units that are deployed in order to cope with this risk.

3 Transportation Network Dataset

The widespread use of cellular phones in Israel enables the collection of accurate transportation data. Given the small size of the country, all cellular companies provide national wide coverage. As shown in [12], the penetration of cellular phones to the Israeli market is very high, even to lower income households, and specially among individuals in the ages of 10 to 70 (the main focus of travel behavior studies). Such penetration enables a comprehensive study of travel behavior that is based on the mobility patterns of randomly selected mobile phones in the Israeli transportation system. This data was shown in [12] and [27] to provide a high quality coverage of the network, tracking 94% of the trips (defined as at least 2km in urban areas, and at least 10km in rural areas). The resulting data contained a wealth of traffic properties for a network of over 6,000 nodes, and 15,000 directed links. In addition, the network was accompanied with an Origin Destination (OD) matrix, specifying start and end points of trips.

The network was created for the National Israeli Transportation Planning Model. In urban areas the network contains arterial streets that connect the interurban roads. For each link of the network, there is information about the length (km), hierarchical type, free-flow travel time (min), capacity (vehicles per hour), toll (min), hourly flow (vehicles per hour), and congested travel time (min). The hourly flows and congested travel times were obtained from a traffic assignment model that loads the OD matrix on the network links.
3.1 Network Structure

Based on the dataset described above we have created a network structure, assigning running indices from 1 to 6716 to the nodes (junctions). We have examined the directed variant of the network where each road segment between two junctions was represented as either one or two directed links between the respective nodes.

In order to get a basic understanding of the network we first extracted and studied several of its structural properties (see Table 1). We have partitioned the network into structural equivalence classes of the nodes and bi-connected components and computed the Betweenness Centrality indices of the nodes \[26, 31, 32\]. Structurally equivalent vertices have exactly the same neighbors and the set of these vertices is called a structural equivalence class. As can be seen from Table 1 the number of structural equivalence classes is roughly the number of vertices in the network and the size of the largest class is three. This means that there are no “star-like” structures in the network and alternative paths between any two vertices are either longer than two hops or have other links emanating from the intermediate vertices.

On the other hand the number of biconnected components in the network is low compared to the number of nodes, meaning that there are significant regions of the network that can be cut out by merely disconnecting a single node.

<table>
<thead>
<tr>
<th>Table 1 Structural properties (Israeli transportation network).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nodes</td>
</tr>
<tr>
<td>Edges (undirected representation)</td>
</tr>
<tr>
<td>Edges (directed representation)</td>
</tr>
<tr>
<td>Number of structural equivalence classes</td>
</tr>
<tr>
<td>Largest equivalence class</td>
</tr>
<tr>
<td>Number of bi-connected components (BCC)</td>
</tr>
<tr>
<td>Avg BCC size</td>
</tr>
<tr>
<td>Largest BCC</td>
</tr>
</tbody>
</table>

3.2 Congestions

In this chapter we define the impact of congestion as the difference between the time to travel through a congested link and the free-flow time to travel. Congestion of a junction can be either inbound or outbound. Inbound congestion is the sum of all congestions on inbound links of some junction. Figure 1 presents the distribution of congestion on network nodes (junctions). Power law nature of this distribution means that vast majority of nodes are not congested but there are a few nodes whose congestion can be arbitrarily large. Based on the Wardrop’s User Equilibrium [45] this also implies a low number of yet significant deviations between the routes chosen by travelers during free-flow and during congestions. In Section 4.3 we use this fact to merge between two routing strategies.
3.3 Flow

The analyzed dataset contains traffic flow through links provided as the number of vehicles per hour. In the next section we will compare the flow through nodes estimated using Betweenness Centrality to the measured flow. We compute the total inbound flow through a node by summing flows on all of its inbound links, where outbound flow is computed symmetrically. Unless a specific junction is a source or a destination of traffic we expect the inbound flow to be equal to the outbound flow. Figure 2 demonstrates the correlation between inbound and outbound flow. We see that vast majority of the nodes are located on the main diagonal, however, there are some deviations, caused by the fact that the data represents average measurements that were carried out along a substantial period of time.

Figure 3 presents the distribution of inbound flow on network nodes. This distribution is exponential, meaning that a vast majority of nodes have little flow through them. However, in contrast to network congestion, there are no “unbounded fluctuations”, i.e. the flow through the most “busy” junctions is not as high as can be expected from the power law distribution of betweenness and congestions (Figures 1 and 4). In fact, congestions significantly limit the flow through the busiest junctions, which subsequently is the reason we do not see the long tail in flow distribution.
Fig. 2 Incoming vs. outgoing flow for each node.

Fig. 3 Exponential distribution of traffic flow through nodes.

4 Betweenness Centrality vs. Traffic Flow

Betweenness Centrality is defined as the total fraction of shortest paths between each pair of vertices that pass through a given vertex [26]. Let $G = (V, E)$ be a directed transportation network where $V$ is the set of junctions and $E$ is the set of directed
Rationality and Optimality of Transportation Networks Defense

Let \( \sigma_{st} \) be the number of shortest paths between the origin vertex \( s \in V \) and the destination vertex \( t \in V \) (in some applications the shortest path constraint can be relieved to allow some deviations from the minimal distance between the two vertices). In the rest of this chapter we will refer to the shortest or “almost” shortest paths between two vertices as routes. Let \( \sigma_{st}(v) \) be the number of routes from \( s \) to \( t \) that pass through the vertex \( v \). The Betweenness Centrality can hence be expressed by the following equation:

\[
BC(v) = \sum_{s,t \in V} \frac{\sigma_{st}(v)}{\sigma_{st}}
\]  

(1)

Note that in this definition we include the end vertices (\( s \) and \( t \)) in the computation of Betweenness since we assume that vehicles can be inspected also at their origin and at the point of their destination.

After computing the Betweenness Centrality for the given transportation network, we can easily see that the distribution of Betweenness Centrality follows a power law (Figure 4). Long tail distributions such as the power law suggest that there is a non negligible probability for existence of vertices whose Betweenness Centrality can be arbitrarily high. This is in contrast to the exponential flow distribution depicted in Figure 3. The different nature of these two distributions suggests that BC as defined above will overestimate the actual traffic flow through nodes especially for the most central vertices.

![Fig. 4 Power law distribution of Betweenness Centrality](image)

Next we would like to check the correlation between BC and traffic flow. Although the correlation is significant the square error is very low \( (R^2 = 0.2021) \) as
shown in Figure 5 (a). Every point in this Figure represents a vertex with the x-axis corresponding to the measured traffic flow and y-axis corresponding to the computed BC.

![Correlation of flow through nodes and Betweenness Centrality](image)

**Fig. 5** Correlation of flow through nodes and Betweenness Centrality

We now discuss augmented variants of the Betweenness Centrality measure that significantly improve the correlation with the traffic flow.

### 4.1 Origin-Destination based Betweenness Centrality

BC definition according to Equation 1 BC assumes equal weights of routes between every pair of vertices in the network. In other words, every vertex acts as an origin and as a destination of traffic. We would like to utilize the measured origin-destination (OD) flow matrix in order to prioritize network regions by their actual use. For this, we shall use the following altered definition for Betweenness, as suggested in [36]:

$$BC(v) = \sum_{s,t \in V} \frac{\sigma_{s,t}(v)}{\sigma_{s,t}} \cdot OD_{s,t}$$  \hspace{1cm} (2)

where $OD$ is the actual measured origin-destination matrix. This method produces a better correlation ($R^2 = 0.4916$) between the theoretic (BC) and the measured traffic flow (see Figure 5 (b)).
4.2 Shortest Routes based on Time to Travel

In order to further improve our ability to estimate the predicted network flow using the network’s topology, we note that both BC calculation methods (Equations 1 and 2 above) assume that routes are chosen according to shortest path strategy based on hop counting. In this section, we retain the shortest path assumption but use weighted links for calculating the Betweenness score. One option is to use the length of the road segments as their weights for the shortest path calculations (based on the well justified assumption that people prefer short routes over the long ones). However, the road capacity, congestions, and the number of segments also play significant roles when choosing the route to destination. People would prefer highways over sideways when the distance difference is not high.

Shortest path algorithms (such as Dijkstra’s or Bellman-Ford’s) are able to consider only one distance weight on links when computing the shortest path to a destination. We shall therefore assume that the primary heuristic guiding people when they chose a route is the time required to reach their destination. Using this assumption, we recompute the BC on the directed transportation, weighting links by their free-flow travel time.

Let $BC_{ft}(v)$ denote the Betweenness of a node $v$ computed w.r.t. the free-flow travel time. Figure 5 (c) shows significant improvements in the correlation between the measured traffic flow and the theoretical $BC_{ft}$ values computed w.r.t the OD matrix and free-flow travel time link weights ($R^2 = 0.6123$). We can see that there are few nodes whose flow was significantly underestimated by the BC measure. Notice that there are also several nodes whose flow was actually overestimated. This can be explained by the fact that people do not travel strictly via shortest paths, but may have various deviations. In particular the deviations form shortest paths are affected by the day time and the day of week.

4.3 Peak-Hours Aware Betweenness Centrality

It is a reasonable assumption that during peak hours travelers will choose to avoid the congested roads and choose their routes based on the congested travel time rather than on the free-flow travel times. Let $BC_{ct}(v)$ denote the Betweenness of a node $v$ computed w.r.t. the congested time. Computing Betweenness using only the congested travel time weights results in $R^2 = 0.7096$. Although peak hours are relatively small fraction of the day, most vehicles travel at these hours. This is the reason for higher correlation of $BC_{ct}$ with the measured traffic flow.

We shall now combine both the Betweenness Centrality computed w.r.t. the free-flow travel time and the congested time by taking a weighted average, namely:

$$BC(v) = \alpha \cdot BC_{ft}(v) + (1 - \alpha) \cdot BC_{ct}(v)$$
where $\alpha$ denotes the relative fraction of vehicles traveling during the free-flow periods. The resulting centrality index can achieve higher correlation with the measured average traffic flow. The maximal correlation of $R^2 = 0.7285$ is obtained for $\alpha = 0.25$ as shown in the Figure 6.

![Figure 6](image-url)  
**Fig. 6** Squared error ($R^2$) as the function of the free flow traffic fraction ($\alpha$).

### 4.4 Separating Stubs Nodes from Transit Nodes

Carefully looking at the various nodes we can see that they can be divided into two groups: *stub nodes* and *transit nodes*.

A Stub node is a node that is an origin or a destination of the traffic (as seen in the Origin-Destination matrix). These nodes account for approximately 10% of the network's nodes. All other nodes (namely, nodes that generate insignificant or no outgoing or incoming routes) are called Transit nodes, as they only forward traffic and do not generate or consume it.

Figure 5 (d) presents the correlation that is received when the two groups of nodes are being processed separately. Specifically, the results show a $R^2 = 0.7068$ for the Transit nodes and a $R^2 = 0.7429$ for the Stub nodes.
4.5 Mobility Oriented Betweenness Centrality

As previously mentioned, the transportation network dataset we use contains a “type” attribute for each link, representing the domain-specific “role” of the link in the overall network. For example, links of types 13 and 14 correspond to internal neighborhood roads, whereas links of type 12 correspond to “collectors” — roads that are in charge of aggregating the traffic from neighborhood roads and channeling it to metropolitan roads, and so on. As each type of roads have therefore a different role, we now try to further improve our flow prediction by examining the Betweenness values achieved when calculating it for every group separately.

The results of the correlation that is achieved using this method are presented in Figure 7. We can clearly see that for the more important roads (namely, those with lower type number, representing a more infrastructural role in the transportation network) this technique yields $R^2$ values that are consistently above 0.74, reaching 0.83(!) for road of types 2 and 9 (note that roads of type 90 are fictive roads with infinite capacity that were artificially added in order to connect distinct regions in the network).

It should be noted that each node may have incoming roads of different types. Each plot corresponds to a set of nodes whose max incoming road type is as specified. In addition, the BC calculations were not made for each set of nodes separately — BC was computed for the complete network, while the correlations were computed separately for each type.

5 Optimizing the Locations of Surveillance and Monitoring Stations

In this section we use the Group variant of shortest path Betweenness Centrality (GBC) [24] as an estimate for the utility of collaborative monitoring for homeland security threats. In other words, we are interested in verifying that given some mobile threat agent, we position the monitoring stations in a way that maximize the chance the agent would be captured, given the traffic patterns of the transportation network. In this case, however, significant computational complexity issues arise, rendering the generation of an optimal solution impractical in real time by conventional tools that are based mostly on behavioral based modeling. Using Group Between Centrality we propose a way to generate efficient approximations of the optimal solution to this optimization problem.

GBC of a given group $(M \subseteq V)$ of vertices accounts for all routes that pass through at least one member of the group. Let $\sigma_{st}(M)$ and $\sigma_{st}(M)$ be the number of routes from $s$ to $t$ and the number of routes from $s$ to $t$ passing through at least one vertex in $M$ respectively:

$$GBC(M) = \sum_{s,t \in V} \frac{\sigma_{st}(M)}{\sigma_{st}(M)} OD_{st}$$

(3)
GBC can be efficiently computed using the algorithm presented in [34].

Assuming the routes are weighted by the origin destination flow in transportation networks, GBC will account for the net number of vehicles that are expected to pass by the monitors during an hour. This net number is different from the total number of vehicles passing by the monitors since the same vehicle can pass by several monitors during a single trip. For example, searching for a suspected escaping terrorist car, one would like to avoid stopping the same vehicle twice and increase the number of distinct vehicles that were inspected. It is therefore important to maximize the GBC value of the set of inspection stations given the number of stations deployed.

Several combinatorial optimization techniques can be used to find a group of nodes of given size that has the largest GBC. In the following discussion we refer to a greedy approximation algorithm for the monitors location optimization problem (Greedy) [21], a classical Depth First Branch and Bound (DFBnB) heuristic search algorithm [30], and recently proposed Potential Search [41].

The Greedy approximation algorithm chooses at every stage the node that has the maximal contribution to the GBC of the already chosen group. The approximation factor of the Greedy algorithm as reported in [21] is:

$$e - \frac{1}{e} \approx 0.632$$
Both the heuristic search algorithms DFBnB and the Potential Search provably find the group having the maximal GBC. The Greedy algorithm and DFBnB were previously compared in [35] in the context of monitoring optimization in computer communication networks. The authors have shown that in preferential attachment networks [9] greedy algorithm produced results that are 0.3% far from optimal. Given the fact that finding a group of a given size having the maximal GBC is a hard problem\(^1\), the greedy algorithm is good enough for any practical purpose. Figure 8 presents the results of selecting one to 39 inspection locations using the greedy algorithm.

![Graph of total net traffic flow vs. number of monitors](image)

**Fig. 8** The total net traffic flow that passes by monitors as a functions of the number of monitors. As expected the marginal value of additional monitors gradually decreases as more of them are added reaching potential traffic coverage of 30% when 39 monitoring stations are deployed.

In homeland security applications deployment of monitoring systems are often done under tight timing conditions, as a result of new intelligence information. Therefore, any optimization method should provide close-to-real-time capabilities. In this context, it is interesting to note that both the DFBnB and the Potential algorithms are anytime search algorithms [50]. Their execution can be stopped at any point of time, yielding the best solution found so far. Therefore, in the following experiments we limit the search time to one hour, simulating a quasi-real-time optimization constraint. Still, as can be seen in Figure 9 the running time of then Greedy algorithm is by far lower than one hour, for the entire Israeli transportation system.

\(^1\) It can be proven by a straightforward reduction from the Minimal Vertex Cover problem that the problem of maximizing GBC is NP-Complete.
When DFBnB and Potential Search algorithms cannot complete the search process within the given time bounds they produce a close to optimal solution and an estimate of its optimality (i.e. certificate). The certificate is computed by dividing the best solution found so far by the upper bound on the optimal solution. The upper bound is computed using admissible heuristic functions and is maintained by the search algorithms for efficient pruning the search space. Figure 10 shows that Potential Search produces higher certificates for its solutions within the one hour time bound for all sizes of the monitors deployment.

6 Applications and Considerations for Policy Makers

As discussed in the introduction of this work, a strong positive correlation can be found between the Betweenness Centrality of nodes of a transportation network and the traffic volume that they have access to. Hence, monitoring deployment schemes that are characterized in high Betweenness values would be far more likely to successfully intercept potential threats compared to low Betweenness ones.

This understanding can be used by policy makers in order to enhance the coverage performance of the existing nation-level infrastructure monitoring system, as well as design protocols for fast-response that could be used ad-hoc in case of alerts regarding a suspected threat. In such cases, the two most dominant factors are re-
sponse time and overall monitoring probability (the probability that the target, if such exists, would eventually be engaged). Hence, the as response time is usually pre-defined and is heavily affected by many other factors, having the ability to improve the monitoring factor, for any short-response-time, is of the utmost importance. Moreover, using our proposed method implies that monitors can be deployed / activated gradually as they are needed (due to operational requirements or budget constraints).

In addition, we should note that it is not necessary to know ahead of time the total number of monitors that will be deployed in order to find their optimal locations. Upon requirement of additional monitors units, their locations can be suggested based on up-to-date network data as well as the current deployment (the effectiveness of this method is very close to optimal both in communication and transportation networks).

Another interesting issue to be considered is the trade-off between the number of monitoring units and their quality with respect to the number of vehicles each unit can monitor simultaneously (to be denoted as the units’ “Sampling Rate”, ranging between 0 and 1). Note that higher sampling rates directly implies a higher cost per unit. Therefore, the overall cost of the monitoring system can be modeled as:

$$\text{Overall Cost} = \text{Cost per Unit} \times \text{Number of Units}$$

whereas the overall monitoring performance of the system can be modeled as:
Overall Performance = System Monitoring Prediction × Sampling Rate =

\[ f_{BC}(\text{Number of Units}) \times f_{\text{Sampling}}(\text{Cost per Unit}) \]

For a given budget, the decision whether to deploy a higher number of units, or to invest to units of better monitoring capabilities can be directly resolved by studying the functions \( f_{BC} \) and \( f_{\text{Sampling}} \). Whereas the first was thoroughly studied in the previous sections, analyzing the effect of the sampling rate over the performance of the system is a much simpler task [20]. With low sampling rates, GBC becomes proportional to the sum of BC values of the group members (as the number of redundant inspections reduces with the sampling rate). We can therefore, consider a guideline saying that traffic monitors with very low sampling rates can be deployed on the most central nodes in the network, even if it means deploying several monitors on the same node. However, when the overall sampling rate of monitors deployed on each node is relatively high, then the set of monitored nodes should be chosen wisely using a more rigorous execution of the optimization algorithm.

Notice that BC and GBC based deployments have the same utility when selecting a single monitor as expected. However, GBC based strategy continuously improves the traffic coverage as more monitors are added with the marginal utility of each additional monitor slowly decreasing.

Figure 11 demonstrates the performance of our monitoring method, by showing the percentage of traffic monitored as a function of the number of monitors, for several deployment schemes: (a) Group Betweenness, (b) Betweenness, and (c) Random deployment. The benefits of the proposed method can clearly be seen from this chart.

BC based strategy produces relatively high quality deployments for small number of monitors (less than five). However, when 10 or more monitors need to be located random deployment is on average as effective as choosing the most central intersections. Moreover, for large numbers of monitors (more than 70-80) random deployment, although the simplest strategy, achieves coverage results that are very similar to choosing the most central intersections. This result may seem surprising but in fact it is absolutely reasonable. Central intersections tend to lay on the arterial roads and usually are quite close to each other. This results in reduced marginal utility of each additional junction joining the deployment.

Using the results of Figure 11 the effect of the number of monitors over the overall percentage of traffic coverage can be observed — and used by policy makers in order to decide on the optimal monitoring strategy:

**Definition 1.** Let us denote the cost of an attack as \( C_{\text{ATTACK}} \).

**Definition 2.** Let \( M(x) : \mathbb{Z}^+ \to [0, 1] \) be a monotonous function denoting the percentage of traffic that is monitored using \( x \) monitoring units\(^2\).

\(^2\) The function \( M(x) \) can be extrapolated using simulations, as demonstrated in Figure 11. Note that \( M(x) \) is domain dependant and may significantly change for different networks.
Therefore, an investment in a monitoring system of \( n \) units would be a rational decision as long as:

\[
\mathcal{C}_{\text{ATTACK}} \geq \frac{n}{M(n)} \cdot \text{Cost per Unit} \tag{4}
\]

If we focus on the monetary costs of attacks and disregard other aspects, then we see that the Normalized Benefit of a monitoring system can be defined as:

\[
\omega \triangleq \mathcal{C}_{\text{ATTACK}} \cdot M(n) - n \cdot \text{Cost per Unit} \tag{5}
\]

The optimal value of the Normalized Benefit would then be received for the number of monitoring units that nulls the derivative \( \frac{\partial \omega}{\partial n} \):

\[
\frac{\partial \omega}{\partial n} = \mathcal{C}_{\text{ATTACK}} \cdot \frac{\partial M(n)}{\partial n} - \text{Cost per Unit}
\]

Namely:

\[
\frac{\partial M(n)}{\partial n} = \frac{\text{Cost per Unit}}{\mathcal{C}_{\text{ATTACK}}} \tag{6}
\]

For example, if we use the function \( y = 1 - e^{-0.015x} \) in order to model the function \( M(n) \) (see Figure 12), after assigning it to Equation 6 we will obtain:

\[
0.015 \cdot e^{-0.015n} = \frac{\text{Cost per Unit}}{\mathcal{C}_{\text{ATTACK}}}
\]

which in turn implies:

\[
n = \frac{\ln 0.015 - \ln \frac{\text{Cost per Unit}}{\mathcal{C}_{\text{ATTACK}}}}{0.015} \tag{7}
\]

This is demonstrated in Figure 13, where the optimal number of monitoring units is presented, for any ratio between the cost of a single monitoring unit and the expected cost of a successful attack, based on the regression to the function that is presented in Figure 12.

7 Case Study — Attacks Scenarios in the Israeli Network

In this section we examine the Normalized Benefit estimation of various monitoring systems, for several attack scenarios, using the Israeli transportation network. We use the function \( y = 1 - e^{-0.015x} \) in order to approximate the evolution of our monitoring coverage with the increase in monitoring units, as illustrated in Figure 12. We use Equation 7 in order to calculate the optimal number of monitoring units, and Equation 5 in order to estimate the Normalized Benefit of the monitoring system.
The figure presents the results of deployment optimization performed on the Israeli transportation network with average travel times computed using state of the art traffic assignment model. Flows and the utility of the deployment were estimated using Betweenness Centrality and Group Betweenness Centrality models, and compared also to the random deployment model. Whereas the BC algorithm had chosen the locations for monitoring units according to the most central intersection based on their BC values, the GBC deployment was a greedy algorithm that tried to maximize the net-number of vehicles passing by the monitors. The benefits of the GBC strategy is clearly shown, as well as the ability to extrapolate this correlation between number of monitoring units and monitored traffic percentage, in order to find the minimal number of monitoring units required in order to guarantee certain levels of coverage.

An illustration of the function $M(n) = 1 - e^{-0.015n}$, that may be used as a model the simulative results that are presented in Figure 11.
Fig. 13  The optimal number of monitoring units as a function of the ratio between the cost of a single monitoring unit, and the cost of a successful attack (assuming the regression of the traffic coverage function to the function $M(n) = 1 - e^{-0.015n}$).

Scenario I (Limited Threat) :

A truck filled with oil that gets over-turned on a highway. The oil needs to be cleaned, but it does not spread and does is not lethal when exposed to. Main damage is the delay caused to the cars that get stuck in the huge traffic jam. Fast detection of the accident can save ($500,000) in wasted work hours.

Scenario II (Local Threat) :

A criminal prisoner escapes from prison and evades the police for house, using a stolen car with known license place number. A stationary traffic monitoring camera eventually tracks him down, not before he was able to rob a liqueur store, severely injuring the clerk and 3 customers. Costs of the chase and compensations to the victims are ($5,000,000).

Scenario III (Metropolitan Threat) :

A car packed with C4 plastic explosive and propane tanks, driven by a suicide bomber, rams the basis of an interchange carrying 3 levels of free-way as well as the main line of the metro-rail. In the collapse of the interchange 20 are killed and the train traffic in the metropolitan area suffers disruptions for 2 months while the trains are re-routed to alternative rails, until the damage is fixed. Costs are estimated in ($50,000,000).
Scenario IV (Regional Threat) :

A trailer carrying toxic liquid waste leaks due to bad maintenance, while driving through the interstate. 30 miles of the road needs to be closed for two weeks while the road is cleaned. Total damage soars to ($500,000,000).

Scenario V (National Threat) :

A van carrying a “dirty-bomb”, gets smuggled into main street and detonated. 8,000 causalities, and radioactive pollution that makes the major part of the city center uninhabitable. Total damage reaches ($5,000,000,000).

We examine three different kinds of monitoring units, ranging from $1,000 through $5,000 to $20,000 (e.g. the cost of a small scale stationary unit equipped with low-bandwidth communication channel, and sensors that can detect chemical or radioactive agents).

Figure 14 depicts the optimal number of monitoring units for these 5 attacks scenarios, for the 3 different types of monitoring units. Notice how optimal number of units is linearly increased as the damage costs are increased in orders of magnitude. Namely, due to the high monitoring efficiency obtained using the proposed GBC method, a relatively low number of units would be ideal for almost any kind of attack scenarios.

Figure 15 demonstrates the Normalized Benefit of the system. Notice that due to the extremely high efficiency of the proposed GBC-based monitoring method, the Normalized Benefit of the system can be made very close to the cost of the attack. That is, the Normalized Cost of the system is close to zero.

8 Conclusions

In this chapter we have discussed the problem of optimizing the locations of surveillance and monitoring stations for a variety of homeland security purposes. For this problem, known to be of high complexity, we propose a novel approximation, using the quasi-real time calculation of the Betweenness Centrality of the network. For this, we show a correlation between the Betweenness Centrality of a node and its expected traffic flow, in transportation networks. Using a comprehensive dataset that covers the Israeli transportation network we have first performed a simple analysis of the network and its properties, showing that there exists a correlation between the traffic flow of nodes and their Betweenness Centrality. We then revised the basic definition of Betweenness Centrality, showing that when analyzing the network in a way which takes into account additional known properties of the links (specifically, time to travel through links), a much stronger correlation can be achieved. Taking into account that a large portion of the traffic is being generated during rush hours, and that different roads may have different ‘roles’ in the transportation network,
Fig. 14  The optimal number of monitoring units for three different types of units, ranging from $1,000 through $5,000 to $20,000 in price, using the Normalized Benefit model. The Charts illustrate the results of the model for five different attacks scenarios, of $500,000, $5,000,000, $50,000,000, $500,000,000 and $5,000,000,000 in total damages. Notice that both charts are in Log scale in the X-axes. However, the top chart depicts the results in linear scale whereas the bottom charts uses double-log scale. The red line on the upper chart represents the investment rationality threshold, below which the normalized benefit on investing in a monitoring system would be negative. This chart assumes that the increase in monitoring coverage as a function of the number of monitoring units can be approximated using the function $M(n) = 1 - e^{-0.015 n}$. 
we show that a significantly higher correlation can be achieved when clustering the roads into groups based on their types (a known property of each road), while also giving increased weight to data that is associated with certain hours. Using this method that we call “Mobility Oriented Betweenness Centrality” we demonstrate correlation values of approximately $R^2 = 0.8$.

Using this method we show how the optimal locations of any (reasonable) amount of monitoring units can be approximated in high accuracy, and using very little computation resources (less than an hour using a standard server). This method can now be used in order to generate highly accurate approximations of the traffic flow in the network, based on its topology, the OD matrix, and time to travel without costly simulations. Furthermore, we can also use this method in order to estimate the dynamic changes in optimal deployment due to changes in the Betweenness of nodes, caused by events such as car accidents, road detours.

In addition, we have solved the monitors placement problem on an artificially produced preferential attachment networks (BA) [9] with similar parameters. We have applied the same OD matrix that was computed on the real-world network and arbitrarily chose the first 680 vertices to communicate with each other. We have then used the two algorithms presented in this work on this network. The results of this experiment clearly showed that the optimization problem is more difficult on the real world transportation network compared to the simulated BA network, despite the fact that both networks had similar parameters and Betweenness Distribution that followed a power law. Specifically, The GBC of the solutions produced for the random BA model and the provided certificates were lower and the running
time reaches its maximal bound sooner compared to the real-world transportation network. This experiment clearly demonstrates even further the applicability of the proposed method for homeland security usages, due to its high accuracy and fast computation time.

In the last section, we have demonstrated that the correlation between number of monitoring units and the overall monitored traffic percentage can be assessed and extrapolated in a way which enables policy makers to estimate the minimal number of monitoring units required in order to guarantee a required level of traffic monitoring. This, subsequently, can be used in order to assess also the overall amount of monetary investment required to guarantee a specific level of monitoring, or in other words — to prevent an attack with some assured probability. This linkage between the financial cost of attack prevention and the cost of the attack itself is perhaps the main contribution of this work.

It should be noted that the effectiveness of GBC based deployment is much higher and the effectiveness of BC based deployment is much lower in transportation networks compared to social networks, as reported for example in [44] (see for example Figures 4 and 5 in that paper).

Finally, it is interesting to note that the problem of finding an optimal (and optionally dynamic) deployment for monitoring units is closely related to dynamic decentralized search for evading targets by a flock of Unmanned Air Vehicles (UAV). In this problems, however, the fact that the paths of the UAVs are unconstrained (as they are flying in the air) makes the calculation of a near-optimal monitoring strategy fairly easy (see for example an analytically provable sub-optimal algorithm in [6, 7]). A more theoretical approach to this problem that studies the complexity of all possible strategies for this problem can be found in [3]. An additional similar variant to this problem is the search for pollutant emitting vehicles, where the merit function is derived from environments considerations [37]. It is interesting to mentioned that in those variants as well, the topological properties of the network along which the “targets” can move significantly influence the ability of monitoring units to track them, as was pointed out in [4, 5].

References

5. Y. Altshuler, I.A. Wagner, and A.M. Bruckstein. Shape factor’s effect on a dynamic cleaners swarm. In Third International Conference on Informatics in Control, Automation and


