Under consideration for publication in Network Science

Brokerage based attack on real world temporal networks

Souvik Sur*, Niloy Ganguly†, Animesh Mukherjee‡

Abstract

In this paper, we attempt to investigate the attack tolerance of human mobility networks where the mobility is restricted to some extent, for instance, in a hospital, one is not allowed to access all locations. Similar situations also arise in schools. In such a network we will show that people need to rely upon some intermediate agents, popularly known as the *brokers* to disseminate information. In order to establish this fact, we have followed the approach of attack in a network which in turn helps to identify important nodes in the network in order to maintain the overall connectivity. In this direction, we have proposed, a new temporal metric, *brokerage frequency* which significantly outperforms all other state-of-the-art attack strategies reported in (Trajanovski *et al.*, 2012; Sur *et al.*, 2015).

1 Introduction

A notion of attack in complex networks was systemically studied by Albert et al. in their seminal paper (Albert *et al.*, 2000). In the work mentioned above, the authors established that scale-free networks are vulnerable to targeted node degree based attack due to the inherent inhomogeneity of the degree distribution whereas exponential networks are resilient from such an attack. In later years, significant efforts have been made to explore the attack tolerance of static networks (Holme *et al.*, 2002; Newman & Ghoshal, 2008; Latora & Marchiori, 2005). However, due to the advancement of technology, today we can model empirical data, for instance, mobility traces to email transactions as time-varying networks. In the context of human mobility a few publicly available temporal traces are (Isella *et al.*, 2011; Scott *et al.*, 2006; Scott *et al.*, 2009; Pietilainen, 2012). All of these datasets contain mobility traces of participants in different conference venues like ACM HyperText, 2009; IEEE INFOCOM, 2005 and 2006; ACM SIGCOMM, 2009. One of the key features of these mobility networks is that the natural movement of the participants is not limited by permission-based restrictions. However, this assumption might not be true in many cases. For instance, in a hospital, patients might not be permitted to access all locations; similarly, in a school premise, students might not have the permission to

∗ G. S. Sanyal School of Telecommunications, Indian Institute of Technology, Kharagpur, India – 721302, Email: souviksur@gssst.iitkgp.ernet.in
† Department of Computer Science and Engineering, Indian Institute of Technology, Kharagpur, India – 721302, Email: niloy@cse.iitkgp.ernet.in
‡ Department of Computer Science and Engineering, Indian Institute of Technology, Kharagpur, India – 721302, Email: animeshm@cse.iitkgp.ernet.in

move freely at all locations. Such permission-based restrictions necessitate the members of the network remain relatively more segregated. Therefore, in such a permission-restricted network people need to rely upon some in-between agents or *brokers* to pass on information and, thereby, maintain global connectivity.

This observation forms the primary motivation of our current work that aims to investigate how information/disease may find a pathway to spread in these restricted networks. In view of this fact, we use the notion of attack on the network for our subsequent experiments. In particular, we introduce a novel attack strategy based on the assumption that in such restricted networks information/disease pathways are formed through brokers. We provide a quantitative definition of brokerage and show that this can be used as an effective metric for targeted node removal. In fact, the results manifest that brokerage based attacks significantly outperform all other forms of attack reported in the context of time-varying networks (Sur *et al.*, 2015).

The notion of brokers in a social network was instigated by Granovetter (Granovetter, 1973). In the above work, he showed that there are certain "weak ties" in social networks that uphold more information than relatively stronger ties. This initial idea was translated into the notion of brokerage in later works (Weimann, 1982; Cook, 1981; Cook *et al.*, 1983; Bonacich, 1987).

In recent years, there have been a lot of works based on the concept of brokerage. In (Sarkar *et al.*, 2006), authors show that in case of sensor networks a double ruling scheme based on information brokerage enhances the possibility to acquire the desired data. A direct application on GPS of this scheme has been described in (Lin *et al.*, 2010) which relies upon information brokerage in turn. Moreover, Heemskerk et al. show that there is an important role of brokerage in the construction of European network of interlocking directorates (Heemskerk *et al.*, 2013). Jiao et. al. establish the fact that brokers are responsible to form cohesive and sparse modules, simultaneously, in a social network (Jiao *et al.*, 2013). It has been shown that even in online social network like Twitter[1] there are some inter-group information brokers who pass information with the help of certain weak ties among these groups (Grabowicz *et al.*, 2012). Lind et al. discuss the role of brokerage in the context of pre-disaster management issues (Lind *et al.*, 2008).

We would like to mention that to the best of our knowledge the concept of brokerage has been applied as an attack strategy for the very first time here. Our motive is just not to introduce a novel attack strategy, rather, in this paper, we emphasize the importance of brokers in empirical human contact networks. To attack, we adapt the methodology described in (Sur *et al.*, 2015) for meaningful comparison only. We believe that the idea of brokerage and the subsequent quantification of it in temporal networks plus the mechanism to identify the important nodes based on this quantification is a fundamental contribution of our work that has never been done in a systematic and rigorous way before.

In particular, our finding may add some novel dimensions to the rich literature of **mobile ad-hoc network (MANET)**. Since there is no well-defined underlying infrastructure in MANET, sometimes it may happen that all the agents (communication devices) willing to communicate with each other may not be within the communication range of each other

[1] http://www.twitter.com

directly. In such a scenario, the underlying routing protocol may take the advantage of the broker nodes to pass messages (Funke *et al.*, 2006; Daly & Haahr, 2007; Hui *et al.*, 2011). MANET has special applications in **military communication** as well as in building **post-diaster temporary networks** if the normal connectivity gets disrupted. To make such networks more efficient, many times specialized devices like message ferries (Zhao *et al.*, 2004; Shah *et al.*, 2003) are deployed. These devices mostly have higher mobility span and so can pass information among localized devices. The framework developed in this paper can help in identifying such *ferries* from within the system - thus saving the extra cost and overhead of deploying specialized equipment.

On the other hand, in the context of attack in time-varying networks Trajanovski et al. suggest three attack strategies for temporal networks and show that empirical temporal networks behave similar to their random counterparts (Trajanovski *et al.*, 2012). However, one major drawback of this work is that it does not take into account the short-time correlations (Sur *et al.*, 2015) present in such empirical networks. Considering such correlations, authors of (Sur *et al.*, 2015) have recently proposed a different model of attack based on recurrent community structure. In this paper, we show that in the context of permission-restricted networks, brokerage based attack strategy significantly outperforms the recurrent community based attack scheme. To this purpose, we first propose a method to quantify the extent of brokerage of nodes in a permission-restricted network followed by a set of thorough experiments to substantiate the effectiveness of the proposed scheme.

The rest of the paper is structured as follows. In section 2, we describe the data that we have investigated, temporal network modeling of the data and the different attack strategies. In section 3, we present the results obtained from our investigation. Finally, we summarize our contributions in section 4.

2 Methodology

2.1 Data

For the purpose of our experiments, we consider two specific real-world face-to-face contact datasets and present our results for each of them.

A detailed description of the datasets on which we conduct our experiments are as follows:

1. HOSPITAL, 2009 (*Hospital*): This dataset contains the temporal network of contacts between patients, patients and health-care workers (HCWs) and among HCWs in a hospital ward in Lyon, France, from Monday, December 6, 2010 at 1:00 pm to Friday, December 10, 2010 at 2:00 pm. The study included 46 HCWs and 29 patients (Vanhems *et al.*, 2013). For data collection, active RFID devices were used to detect and record face-to-face proximity relation among people wearing the RFID badges. These devices can detect face-to-face proximity ($1-1.5$ meter) of another device with a temporal resolution of $\tau = 20$ seconds. Thus in a single hour there can be a maximum of $n = 3600/\tau = 180$ network snapshots. In this data, along with the temporal information, the nodes are also labeled by their role/occupation. Each set of nodes with a particular role/occupation can be thought of as a cohesive group of individuals usually termed as ground-truth communities in the literature (Yang &

Leskovec, 2012). The different categories here are medical staffs (MED), administrators (ADM), nurses (NUR) and patients (PAT), each representing a ground-truth community. The time series showing number of active nodes (i.e., nodes with degree > 0) in each hour in each of these ground-truth communities (stacked one after another) is shown in Fig. 1(a).

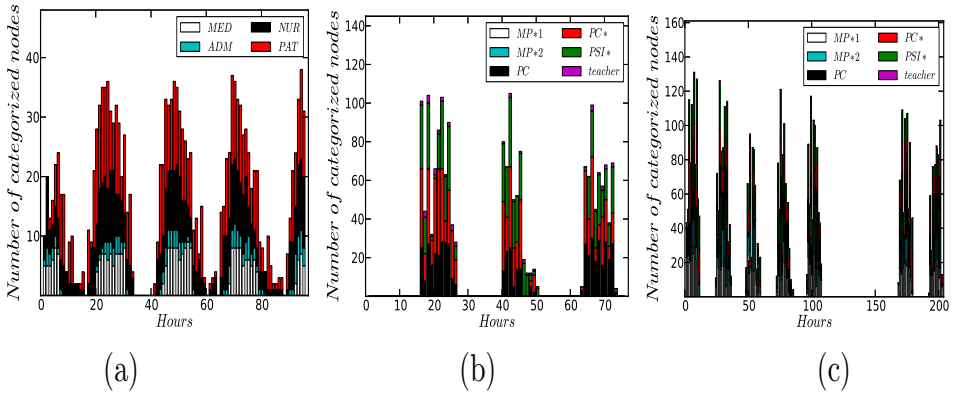

Fig. 1: (Color online) Time series of the number of active nodes in each hour in different ground-truth communities for (a) *Hospital* (b) *High School* 2011 and (c) *High School* 2012. The number of active nodes in the different categories are stacked one after another for every hour.

2. HIGH SCHOOL (*High School*): These datasets contain the temporal network of contacts between students in a high school in Marseilles, France. The first dataset corresponds to the contacts of the students of three classes on 4 days in November, 2011 (referred to *High School* 2011), and the second corresponds to the contacts of the students of 5 classes on 7 days (from a Monday to the Tuesday of the following week) in November, 2012 (denoted as *High School* 2012) (Fournet & Barrat, 2014). Once again, τ is equal to 20 seconds here. A link has been constructed at a certain time if any two nodes were within the communication range. In this case, the different categories can be broadly divided into two groups, a group of two classes (MP*1 and MP*2) and a group of three classes (PC, PC*, PSI*), each of which corresponds to a ground-truth community. Once again, the time series of the number of active nodes at each of the hours in the different categories (stacked one after another) are shown in Fig. 1(b) and (c) respectively for the two sets of data.

These networks also exhibit the existence of *silence hours* as defined in (Sur *et al.*, 2015). Silence hours refer to those hours when the human activity (in terms of number of edges in this case) becomes significantly lower than that in the other hours (See Fig. 2). In order to quantify this effect, we identify and discard those hours which have active node participation lower than 25% of the mean of the entire time series of the number of active nodes over time, as the silence hours and retain the others as the active hours.

Table 1 summarizes some of the basic statistics of the datasets used in our experiments. In general, these statistics indicate that the graphs are usually sparse like many other social networks (Clauset *et al.*, 2004).

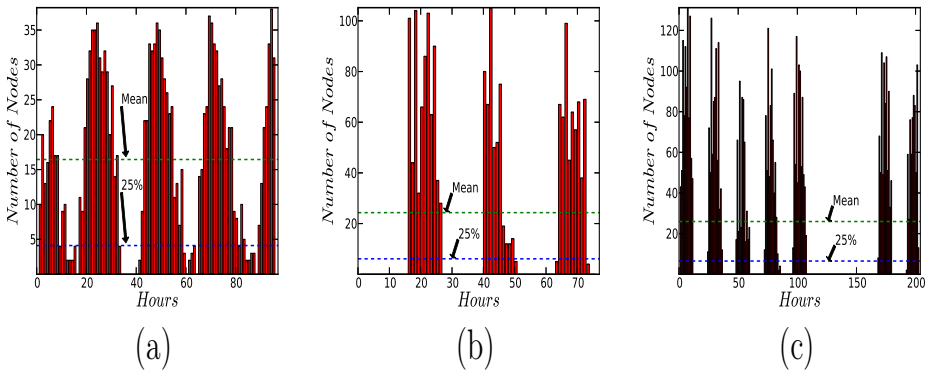

Fig. 2: (Color online) Time series of the number of active nodes in each hour for (a) *Hospital* (b) *High School* 2011 and (c) *High School* 2012.

Table 1: *Datasets statistics*

Dataset	No. of nodes	No. of edges/hour	No. of active hours
Hospital	75	337.75	69
High School 2011	126	375.80	31
High School 2012	180	221.90	83

2.2 Brokerage

Marsden defines brokerage as a process "by which intermediary actors facilitate transactions between other actors lacking access to or trust in one another (Marsden & V., 1982)." On the other hand, Burt defines brokers as actors who simultaneously send and receive resources from different parts of the network in which they are embedded (Burt, 1976).

Formally, brokerage can be defined as follows: in a graph representing the non-symmetric binary relation R, j is said to be a broker between i and k if and only if iRj, jRk, and $i\bar{R}k$, where iRj indicates that i is tied to j by the relation R, and $i\bar{R}k$ is the negation of iRk (Gould & Fernandez, 1989). Here negation of R indicates that i is not related to j according to the definition of R. Specifically, in our case it means that there is no edge between i and j.

According to (Hanneman & Riddle, 2005; Gould & Fernandez, 1989) the brokers can be classified into following five categories noted in Fig. 3.

However, these configurations of different brokerages are entirely based upon static network model. In this paper, we attempt to extend the same idea for time-varying networks. The key modification is that, here in time-varying networks the time-respecting paths have been considered instead of simple paths in the static counterpart. Fig. 4 illustrates the idea.

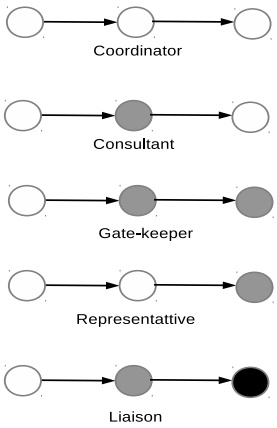

Fig. 3: (Color online) Classification of brokerage. Different colors represent nodes from different ground-truth communities.

The node y turns out to be a potential broker between nodes x and z since it can receive information from node x at time $t = 1$ and pass it to node z at time $t = 3$. While in a static network, y always qualifies as a broker, in a temporal network y can act as a broker only if it has first got linked with x and received a message that can then be transmitted at a later step to z when a link is formed between y and z. In other words, in the static aggregation, y is always adjudged as a broker; in contrast, only if the explicit time order is maintained in a time-varying network, y can qualify as a broker. Note that the edges in the network can be thought of having dynamic directions defined by their explicit time ordering.

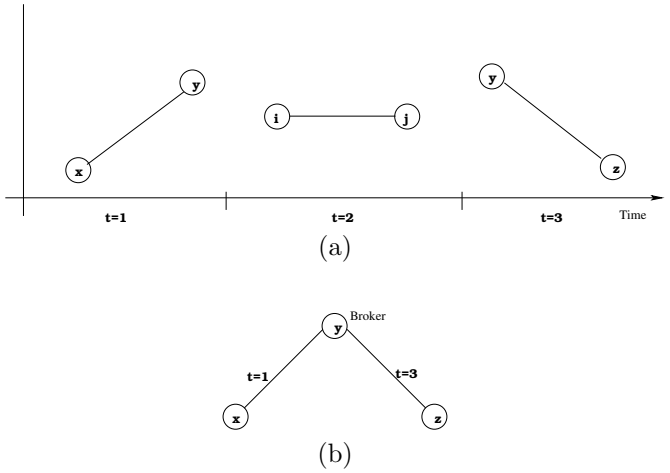

Fig. 4: (Color online) A possible configuration of a temporal broker.

Temporal brokerage: One can now attempt to introduce, a node j's total brokerage activity in a network with N nodes. For example, if we assume, iRj refers to an edge between i and j, the total brokerage for a particular node j can be defined as the number of ordered pairs (i,k) in the network for which the condition iRj and jRk and $i\bar{R}k$ hold simultaneously (Gould & Fernandez, 1989). For a time-varying network, iRj and jRk need not be simultaneously true. In particular, the brokerage can be defined as, $iR_{t_1}j$, $jR_{t_2}k$, and $i\bar{R_{t^*}}k$ where $t_1 \leq t_2$ and t^* could be any time-point within the time-window under investigation. Note that, in case of static networks, the path from i to k via j is a static path while in case of temporal networks the path has to be time-respecting (Trajanovski *et al.*, 2012). Intuitively, if the existence of a node turns out to be essential to diffuse information between another two nodes, then the essential node qualifies as a broker.

We can quantify the idea of brokerage using the number of 'brokerage relations' of a node is involved in. This is referred to as brokerage frequency of a node and can be computed by constructing the *first contact matrix* which is a matrix whose (i,j) cell represents the time of the first contact between the node pair i and j. If $t_{ij} = \infty$ then i and j remain disconnected for the entire time-window under investigation. Therefore, the node j acts as a broker between nodes i and k if $t_{ij} \leq t_{jk}$ and $t_{ik} = \infty$.

In a given time interval $[T_1, T_n]$, the brokerage frequency of a node j is the fraction of ordered pairs (i,k) in the network for which the conditions $t_{ij} \leq t_{jk}$ and $t_{ik} = \infty$ hold during this time interval.

$$B(j;T_1,T_n) = \frac{1}{(N-2)(N-1)} \sum_{i=1,k=1,i\neq j\neq k}^{N,N} \delta_{ik} \tag{1}$$

where

$$\delta_{ik} = \begin{cases} 1, & \text{if } t_{ij} \leq t_{jk} \text{ and } t_{ik} = \infty. \\ 0, & \text{otherwise.} \end{cases}$$

2.3 Temporal Networks, Variables and Metrics

Our objective is to identify the role of brokerage in the network as one of its structural properties. One possible way to judge the importance of any structural property would be to eliminate that property partially or fully and observe how the resultant network is affected. This is popularly modeled as *attack* in the literature.

Before going into the details of the attack models, here we present some of the important terminologies required for further discussion. For the rest of our discussion, we consider N as the total number of unique nodes in the network in a given time-window $[t_1,t_n]$.

Temporal distance: Temporal distance $d_{ij}(t_1,t_n)$ between nodes i and j is the minimum number of time-steps required to reach node j from node i in the time interval $[t_1,t_n]$ (Scellato *et al.*, 2011).

In case where it is not possible to spread the message between two particular nodes i and j, the temporal distance is infinity; $d_{ij}(t_1,t_n) = \infty$ and on the other hand if i and j are connected since the first time-step then $d_{ij}(t_1,t_n) = 1$. Usually, temporal distance

among all pairs of nodes in a graph are calculated by flooding the network with messages. The messages can traverse along the edges only when these edges are present in the network (Trajanovski *et al.*, 2012).

Temporal efficiency: Temporal efficiency is the averaged sum of the inverse temporal distances over all pairs of nodes in the time interval $[t_1, t_n]$:

$$E(t_1, t_n) = \frac{1}{N(N-1)} \sum_{i,j:i \neq j} \frac{1}{d_{ij}(t_1, t_n)} \tag{2}$$

where N is the total number of unique nodes in the network and $d_{ij}(t_1, t_n)$ is the temporal distance between nodes i and j in the time interval $[t_1, t_n]$ (Scellato *et al.*, 2011).

Temporal robustness: Temporal robustness is the relative change of the efficiency after a structural damage. If the temporal efficiency of the damaged network is E, then the temporal robustness is expressed as

$$R_G = \frac{E'}{E} = 1 - \frac{\Delta E'}{E} \tag{3}$$

where E' is the efficiency of the temporal network before the damage (Scellato *et al.*, 2011).

The Attack Model: We adopt a simple approach to formulate the attack scheme. In a particular hour, we rank the nodes based on a particular attack strategy, for example, (i) average node degree (Trajanovski *et al.*, 2012) or (ii) temporal closeness (Trajanovski *et al.*, 2012) or (iii) number of node contacts-updates (Trajanovski *et al.*, 2012) or (iv) nodes within communities of hourly aggregated network (Sur *et al.*, 2015) – and remove a fraction (P_{attack}) of the highest ranked nodes based on each of these strategies from the subsequent hour. In other words, we conduct the measurement and ranking of the nodes in a particular hour and then attack the high ranked nodes in the following hour. Precisely, for each of the consecutive pairs of hours, we perform the following independently: for every i^{th} hour we study the networks at 20 seconds interval, i.e., we actually consider 180 static snapshots and compute the different attack metrics, e.g., average degree of a node, temporal closeness, etc. Based on the rankings obtained from each of these metrics we select the candidates for the attack in the next hour i.e., the $(i+1)^{th}$ hour. Therefore, this one hour is our observation window where we extract statistics from all the 180 snapshots with no aggregation of the networks at all. For the $(k+1)^{th}$ pair, we bring back the nodes into the system removed in the k^{th} iteration provided they are still active in the hour being considered. The assumption is that attacks on such short-time spans (specifically an hour) should appropriately reflect the effect of the shorter-time correlations (Sur *et al.*, 2015). We describe each of the attack strategies and the associated results below. In each case, the temporal robustness is averaged over the total number of active hours (hours that are not silent) for different values of P_{attack}.

3 Results

For the purpose of our experiment, we have considered these following five temporal metrics along with the 'brokerage frequency' to attack the empirical networks mentioned in section 2.1. The metrics are,

1. **Average node degree**: The temporal equivalent of the degree centrality in static network (Trajanovski *et al.*, 2012). The nodes are removed in decreasing order of their average node degree values.
2. **Temporal closeness**: The temporal equivalent of the closeness centrality in static network (Trajanovski *et al.*, 2012). The nodes are removed in increasing order of their temporal closeness centrality values.
3. **Number of node contacts-updates**: The temporal equivalent of the betweenness centrality in static network (Trajanovski *et al.*, 2012). Once again, the nodes are removed according to decreasing values of node contacts-updates.
4. **Aggregated community**: A node belonging to the largest recurrent community is randomly picked up for removal and the scheme is repeated for the other communities in decreasing order of their sizes. (Sur *et al.*, 2015).
5. **Ground-truth community**: A node from the largest recurrent ground-truth community (See section 2.1) is randomly picked up for removal, and the scheme is repeated for the other communities in decreasing order of their sizes.

As an initial step, we plot in Fig. 5, the robustness values for different attack strategies that are based on the various metrics used to rank the nodes to be attacked. It is evident from the result that 'brokerage frequency' affects the network robustness most significantly in comparison to the others. Moreover, in panel (a), it can be clearly observed that the random strategy performs poorly than the other intelligent strategies. It holds true for the other two datasets also. We argue that this is due to effect of short-time correlation of empirical human proximity networks (Sur *et al.*, 2015).

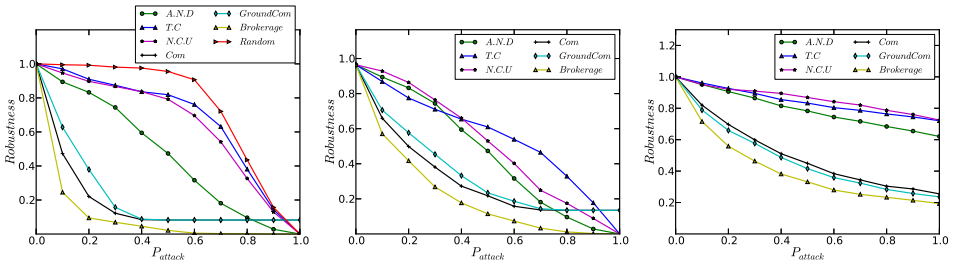

Fig. 5: (Color online) Temporal robustness (shown as *Robustness*) as a function of the fraction of nodes under attack (shown as P_{attack}) for different attack strategies. (a) *Hospital* (b) *High School* 2011 and (c) *High School* 2012.
A.N.D: Average Node Degree, *T.C*: Temporal Closeness, *N.C.U*: Number of Node Contact-updates, *Com*: Aggregated Community, *GrondCom*: Ground-truth Communities, *Brokerage*: Brokerage Frequency.

As a following step, we show that while community based attack proposed in (Sur *et al.*, 2015) is more suitable than brokerage based attack for face-to-face interaction networks like ACM HyperText (Isella *et al.*, 2011) (see Fig. 6), the opposite is true for networks with permission based restrictions like *Hospital* (see Fig. 5).

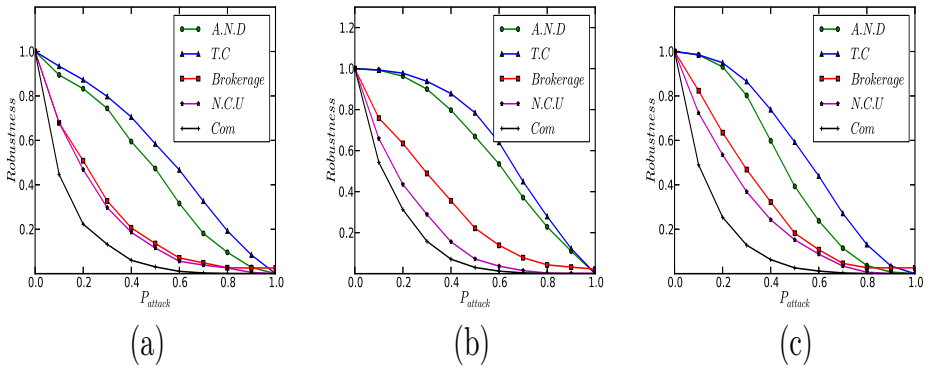

Fig. 6: (Color online) Temporal robustness (shown as *Robustness*) as a function of the fraction of nodes under attack (shown as P_{attack}) for each different attack strategies, (a) $HYPERTEXT, 2009$, (b) $INFOCOM, 2005$,(c) $INFOCOM, 2006$
A.N.D: Average Node Degree, *T.C*: Temporal Closeness, *Brokerage*: Brokerage Frequency, *N.C.U*: Number of Node Contact-updates, *Com*: Aggregated Community.

To investigate this fundamental difference in results further, in Fig. 7(a) we observe that although in this case, the edge emergence factor (ξ)[2] (Sur *et al.*, 2015) is correlated to largest community size (*L.C.S*), the correlation seems to be way weaker than in the case of HyperText network (Pearson's $r = 0.4$) in Fig. 7(b) . The primary reason for this is that in movement-restricted networks, community structures are not very strong and well-defined.

This thorough comparison unfolds that the brokerage based attack outperforms all other forms of attack described in (Sur *et al.*, 2015). Since these networks contain explicit node labels, so it is possible to classify every node triplet into one of the five classes discussed in Fig. 3. However, since these networks are undirected, so there is no difference between 'gate-keeper' and 'representative' – we club these two into a new class, 'fringe-keeper'. In Fig. 8 we plot the time series of the number of brokerage classes (i.e., the number of brokerages appearing in each class) at different time-points.

This time series seems to be significantly uneven (i.e., the number of different classes of brokers is very different in each hour) and therefore one might argue that the class with the most frequent brokerage might dominate the other classes. In order to, eliminate this effect,

[2] Let, E_t = set of edges at time instance t and A_{t+1} = set of edges at $t+1$ adjacent to these E_t edges. The edge emergence factor(ξ) for that time window is expressed as

$$\xi(t_1, t_n) = \frac{\sum_{t=1}^{n-1} |A_{t+1}|}{\sum_{t=1}^{n-1} |E_t|} \tag{4}$$

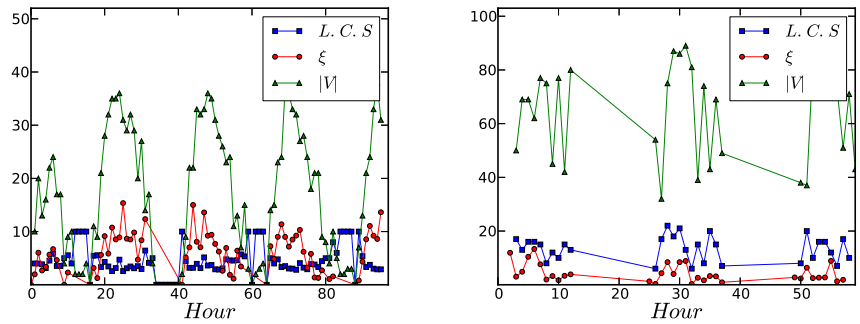

Fig. 7: (Color online) Relation between edge emergence factor (ξ) and size of the largest community and number of nodes.

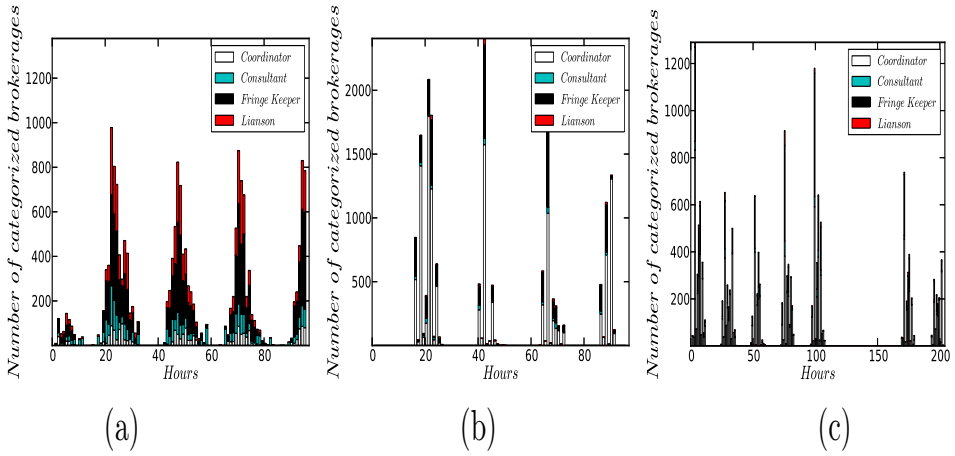

Fig. 8: (Color online) Time series of the number of different brokerage classes for (a) *Hospital* (b) *High School* 2011 and (c) *High School* 2012.

we re-define the brokerage frequency of a node by normalizing this term with the total frequency of brokerage that is present in the class to which the node under investigation belongs to. The results comparing the community based attack and the two brokerage based attacks are shown in Fig. 9. The results once again indicate that brokerage based attack schemes significantly outperform the community based schemes. In general, two different strategies yield the same results if and only if they produce the same ranking of nodes for each of the values of the attack probability (P_{attack}). So, it is evident that both the brokerage based attack schemes enumerate more or less same ranking of nodes. The subtle differences observed are most probably due to the alteration of one or two nodes in the resultant ranking. In particular, networks that we investigate, the normalization does not bring a large change in the ranking. However, it appears that the normalized brokerage frequency is a more principled measure.

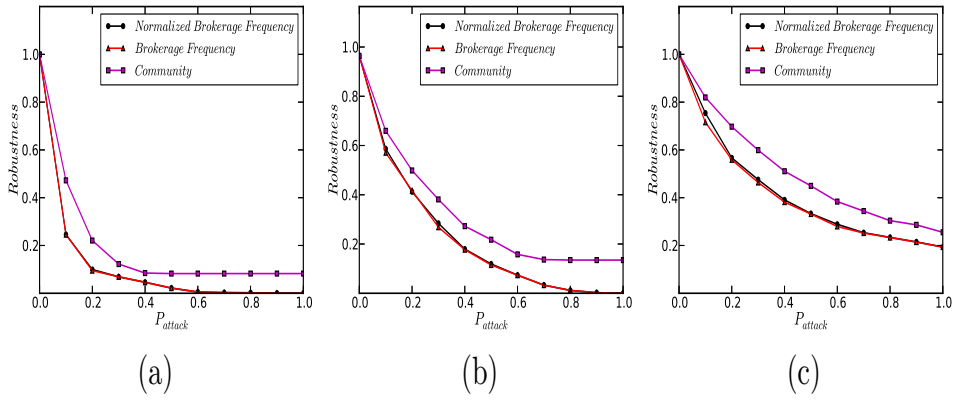

Fig. 9: (Color online) Temporal robustness (shown as *Robustness*) as a function of the fraction of nodes under attack (shown as P_{attack}) for normalized brokerage frequency based attack strategy. (a) *Hospital* (b) *High School* 2011 and (c) *High School* 2012.

From these experimental inferences it can be realized that in these permission-restricted empirical networks people fail to form cohesive groups of significant size since, otherwise community based attack would have outperformed all other strategies as it has been established in (Sur *et al.*, 2015). The effectiveness of the temporal brokerage based attack indicates that in such permission-restricted empirical networks people need to rely upon some intermediate agents or brokers to maintain the overall connectivity. For example, in a hospital where a patient may not be allowed to move out from his/her cabin, staffs (including doctors and nurses) may turn out to be responsible for maintaining the overall connectivity. Consequently, removal of these *brokers* from the network affects the network mostly which results in a sharp drop in network robustness.

4 Conclusion

In summary, the contribution of this work is to introduce a novel attack strategy, *brokerage frequency*, for empirical human contact networks where the movements are restricted. The state-of-the-art attack strategies fail in case of such networks. The most important observation in this context is that even in the human contact networks there is a crucial role of information brokers who are responsible for the dissemination of messages. As a future step, we wish to investigate the performance of the attack schemes on newer samples of data.

References

Albert, R., Jeong, H., & Barabasi, A.L. (2000). Error and attack tolerance of complex networks. *Nature*, **406**(6794), 378–382.

Bonacich, Phillip. (1987). Power and centrality: A family of measures. *American journal of sociology*, **92**(5), pp. 1170–1182.

Burt, Ronald S. (1976). Positions in network. *Social forces*, **55**, 93–122.

Clauset, Aaron, Newman, M. E. J., & Moore, Cristopher. (2004). Finding community structure in very large networks. *Phys. rev. e*, **70**(Dec), 066111.

Cook, Karen S., Emerson, Richard M., Gillmore, Mary R., & Yamagishi, Toshio. (1983). The distribution of power in exchange networks: Theory and experimental results. *American journal of sociology*, **89**(2), pp. 275–305.

Cook, K.S. (1981). *Network structures from an exchange perspective*. State University of New York, Department of Sociology.

Daly, Elizabeth M., & Haahr, Mads. (2007). Social network analysis for routing in disconnected delay-tolerant manets. *Pages 32–40 of: Proceedings of the 8th acm international symposium on mobile ad hoc networking and computing*. MobiHoc '07. New York, NY, USA: ACM.

Fournet, Julie, & Barrat, Alain. (2014). Contact patterns among high school students. *Plos one*, **9**(9), e107878.

Funke, Stefan, Guibas, Leonidas J., Nguyen, An, & Wang, Yusu. (2006). *Distributed computing in sensor systems: Second ieee international conference, dcoss 2006, san francisco, ca, usa, june 18-20, 2006. proceedings*. Berlin, Heidelberg: Springer Berlin Heidelberg. Chap. Distance-Sensitive Information Brokerage in Sensor Networks, pages 234–251.

Gould, R. V., & Fernandez, R. M. (1989). Structures of Mediation: A Formal Approach to Brokerage in Transaction Networks. *Sociological methodology*, **19**, 89–126.

Grabowicz, Przemyslaw A., Ramasco, José J., Moro, Esteban, Pujol, Josep M., & Eguiluz, Victor M. (2012). Social features of online networks: The strength of intermediary ties in online social media. *Plos one*, **7**(1), e29358.

Granovetter, Mark S. (1973). The Strength of Weak Ties. *American journal of sociology*, **78**.

Hanneman, Robert A., & Riddle, Mark. (2005). *Introduction to social network methods*. `http://faculty.ucr.edu/~hanneman/nettext/C9_Ego_networks.html#brokerage`. [Online; accessed 17 July 2016].

Heemskerk, Eelke M., Daolio, Fabio, & Tomassini, Marco. (2013). The community structure of the european network of interlocking directorates 2005–2010. *Plos one*, **8**(7), e68581.

Holme, Petter, Kim, Beom Jun, Yoon, Chang No, & Han, Seung Kee. (2002). Attack vulnerability of complex networks. *Phys. rev. e*, **65**(May), 056109.

Hui, P., Crowcroft, J., & Yoneki, E. (2011). Bubble rap: Social-based forwarding in delay-tolerant networks. *Ieee transactions on mobile computing*, **10**(11), 1576–1589.

Isella, Lorenzo, Stehlé, Juliette, Barrat, Alain, Cattuto, Ciro, Pinton, Jean-François, & Van den Broeck, Wouter. (2011). What's in a crowd? analysis of face-to-face behavioral networks. *Journal of theoretical biology*, **271**(1), 166–180.

Jiao, Qing-Ju, Huang, Yan, Liu, Wei, Wang, Xiao-Fan, Chen, Xiao-Shuang, & Shen, Hong-Bin. (2013). Revealing the hidden relationship by sparse modules in complex networks with a large-scale analysis. *Plos one*, **8**(6), e66020.

Latora, Vito, & Marchiori, Massimo. (2005). Vulnerability and protection of infrastructure networks. *Phys. rev. e*, **71**(Jan), 015103.

Lin, Chia-Hung, Kuo, Jian-Jhih, & Tsai, Ming-Jer. (2010). Reliable GPS-Free Double-Ruling-Based Information Brokerage in Wireless Sensor Networks. *Pages 351–355 of: Ieee infocom*.

Lind, Benjamin E., Tirado, Miguel, Butts, Carter T., & Prahova, Miruna Petrescu. (2008). Brokerage roles in disaster response: organisational mediation in the wake of Hurricane Katrina. *International journal of emergency management*, **5**.

Marsden, & V., Peter. (1982). Brokerage behavior in restricted exchange network. *Social structure and network analysis*, Jun, 201–18.

Newman, M. E. J., & Ghoshal, Gourab. (2008). Bicomponents and the robustness of networks to failure. *Phys. rev. lett.*, **100**(Mar), 138701.

Pietilainen, Anna-Kaisa. 2012 (July). *CRAWDAD data set thlab/sigcomm2009 (v. 2012-07-15)*. Downloaded from http://crawdad.org/thlab/sigcomm2009/.

Sarkar, Rik, Zhu, Xianjin, & Gao, Jie. (2006). Double rulings for information brokerage in sensor networks. *Ieee/acm transactions on networking*, **17**, 286–297.

Scellato, S., Leontiadis, I, Mascolo, C., Basu, P., & Zafer, M. 2011 (April). Understanding robustness of mobile networks through temporal network measures. *Pages 1–5 of: Infocom, 2011 proceedings ieee*.

Scott, James, Gass, Richard, Crowcroft, Jon, Hui, Pan, Diot, Christophe, & Chaintreau, Augustin. 2006 (Jan.). *CRAWDAD trace cambridge/haggle/imote/infocom (v. 2006-01-31)*. Downloaded from http://crawdad.cs.dartmouth.edu/cambridge/haggle/imote/infocom.

Scott, James, Gass, Richard, Crowcroft, Jon, Hui, Pan, Diot, Christophe, & Chaintreau, Augustin. 2009 (May). *CRAWDAD trace cambridge/haggle/imote/infocom2006 (v. 2009-05-29)*. Downloaded from http://crawdad.cs.dartmouth.edu/cambridge/haggle/imote/infocom2006.

Shah, R. C., Roy, S., Jain, S., & Brunette, W. 2003 (May). Data mules: modeling a three-tier architecture for sparse sensor networks. *Pages 30–41 of: Sensor network protocols and applications, 2003. proceedings of the first ieee. 2003 ieee international workshop on*.

Sur, Souvik, Ganguly, Niloy, & Mukherjee, Animesh. (2015). Attack tolerance of correlated time-varying social networks with well-defined communities. *Physica a: Statistical mechanics and its applications*, **420**(0), 98 – 107.

Trajanovski, S., Scellato, S., & Leontiadis, I. (2012). Error and attack vulnerability of temporal networks. *Phys. rev. e*, **85**(Jun), 066105.

Vanhems, Philippe, Barrat, Alain, Cattuto, Ciro, Pinton, Jean-François, Khanafer, Nagham, Régis, Corinne, Kim, Byeul-a, Comte, Brigitte, & Voirin, Nicolas. (2013). Estimating potential infection transmission routes in hospital wards using wearable proximity sensors. *Plos one*, **8**(9), e73970.

Weimann, Gabriel. (1982). On the importance of marginality: One more step into the two-step flow of communication. *American sociological review*, **47**(6), pp. 764–773.

Yang, Jaewon, & Leskovec, Jure. (2012). Defining and evaluating network communities based on ground-truth. *Pages 3:1–3:8 of: Proceedings of the acm sigkdd workshop on mining data semantics*. MDS '12. New York, NY, USA: ACM.

Zhao, W., Ammar, M., & Zegura, E. (2004). A message ferrying approach for data delivery in sparse mobile ad hoc networks. *Pages 187–198 of: Proceedings of the 5th acm international symposium on mobile ad hoc networking and computing*. MobiHoc '04. New York, NY, USA: ACM.