Physica A 420 (2015) 98–107

Contents lists available at ScienceDirect

Physica A

journal homepage: www.elsevier.com/locate/physa

Attack tolerance of correlated time-varying social networks with well-defined communities

Souvik Sur [a,c,*], Niloy Ganguly [b,c], Animesh Mukherjee [b,c]

[a] G. S. Sanyal School of Telecommunications, Kharagpur, 721302, India
[b] Department of Computer Science and Engineering, Kharagpur, 721302, India
[c] Indian Institute of Technology, Kharagpur, 721302, India

HIGHLIGHTS

- We identify the existence of short time correlation in temporal networks.
- The community based attack affects time correlated real-world networks most severely.
- We introduce a novel metric edge emergence factor to quantify short-time correlation.

ARTICLE INFO

Article history:
Received 28 October 2013
Received in revised form 18 August 2014
Available online 4 November 2014

Keywords:
Time-varying networks
Efficiency
Robustness
Attack tolerance
Community analysis

ABSTRACT

In this paper, we investigate the *efficiency* and the *robustness* of information transmission for real-world social networks, modeled as time-varying instances, under targeted attack in shorter time spans. We observe that these quantities are markedly higher than that of the randomized versions of the considered networks. An important factor that drives this efficiency or robustness is the presence of short-time correlations across the network instances which we quantify by a novel metric the—*edge emergence factor*, denoted as ξ. We find that standard targeted attacks are not effective in collapsing this network structure. Remarkably, if the hourly community structures of the temporal network instances are attacked with the largest size community attacked first, the second largest next and so on, the network soon collapses. This behavior, we show is an outcome of the fact that the *edge emergence factor* bears a strong positive correlation with the size ordered community structures.

1. Introduction

The seminal work [1] by Barabási et al. introduced the concept of error and attack tolerance of complex networks. They showed 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 attacks. The extent of vulnerability was measured in terms of change (before and after attack) in diameter, size of the individual clusters and average cluster size of the network. Following this, in later years, the resilience of static networks has been considerably investigated in Refs. [2–4]. However, since most of the real-world networks are time-varying [5] in nature, the attack strategies as well as the measurement tools effective for static networks may not be actually suitable to quantify the robustness of such networks, specially using epidemic dynamics [6].

* Corresponding author at: G. S. Sanyal School of Telecommunications, Kharagpur, 721302, India.
E-mail addresses: souviksur@gssst.iitkgp.ernet.in (S. Sur), niloy@cse.iitkgp.ernet.in (N. Ganguly), animeshm@cse.iitkgp.ernet.in (A. Mukherjee).

http://dx.doi.org/10.1016/j.physa.2014.08.074
0378-4371/

In order to better quantify the resilience of time-varying networks, the concept of temporal robustness has been introduced in Ref. [7], to measure the degree of tolerance against random failure in the network and has been subsequently used for targeted attack [8]. To effectively find the influential nodes in a time-varying network, researchers [8–10] have divided the network in two parts by considering the temporal network as a sequence of static networks taken at suitable time resolution [11]. They then identified important nodes from the initial data which can be used to launch attack on the remaining network. For example, [8] estimates important nodes using different metrics—average node degree, temporal closeness and number of node contacts-updates from the first half (50%) of the data and subsequently launch an attack by progressively removing those 'important' nodes. Considering such a framework, they study the effects of attacks on several real world networks (INFOCOM 2006 mobility trace and San Francisco Cab spotting data); however, since they consider two halves of the data they fail to observe any difference in effect between the real-world networks and random graphs.

On closer inspection, from the perspective of an attacker, it seems infeasible to split up the entire window of a sufficiently large network into two equal halves (or into 75%–25% as in Ref. [9]). This is because, to study the dynamics of a temporal network, one needs to observe it at the correct level of granularity. Therefore, for a sufficiently large network, one may investigate it at shorter time slices and study how the dynamics changes over the consecutive time slices. In other words, a more rational and practical way to launch an attack would be to do it in almost real time possibly by collecting evidences from the network instances within a shorter time-window (an hour) and attack the network structure in the following time-window (next hour) based on the evidence collected. For the purpose of our investigation, we choose the window of an hour since we observe that it is a representative choice among different others (e.g., 15 min, 30 min, 2 h and 6 h) for the dataset we considered. Intuitively, the scheme in [8], (a) is a less meaningful attack for dynamic networks and (b) leaves the shorter-time correlations in the network completely unseen. Note that by correlation we denote structural correlation, i.e., the existence of part of the network that recur over consecutive time-points.

We observe that there are certain attack strategies which work well for the network samples considered in Ref. [8], fail completely here. We see, in this shorter time-window, unlike [8], the temporal efficiency [7] of a real-world temporal network is significantly higher than that of its random counterpart. We find that if these networks are attacked based on the underlying hourly community structures with those nodes that appear in the largest size community targeted first for removal, then the attack seems to be successful in gradually collapsing the network thus allowing us to conclude that identification of the community structures as the target of the attack almost surely collapses the network even in the shorter-time window.

The different results obtained can be explained by considering the degree of time correlation present in subsequent (training and testing) networks. We quantify these shorter-time correlations in terms of a new metric called the *edge emergence factor* (ξ) that precisely computes how many edges branch out at some time instance from the end points of a single edge that existed in the immediate previous time instance. As we shall see, the ξ of a real time-varying social graph is significantly higher than uncorrelated random graphs. Note that the ξ is a manifestation of the dynamics of information spread that takes place through the social contacts in a temporal graph. We find that the key reason for the higher robustness in empirical networks arises from the fact that the ξ bears a strong correlation with the size of the hourly communities.

The paper is structured as follows. In Section 2, we describe the data that we have investigated, temporal network modeling of the data and different attack strategies. In Section 3, we present the results obtained from our investigation and attempt to connect the structure and the function of real-world temporal networks. Finally, we summarize our contributions in Section 4.

2. Materials and methods

2.1. Data

For the purpose of our investigation of robustness of time-varying networks, we consider three specific real-world face-to-face contact datasets and present our results for each of them.

2.1.1. Real-World networks

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

1. HYPERTEXT, 2009 ($HT^{09}_{Original}$): These data corresponds to face-to-face interactions of 113 attendees of ACM Hypertext 2009 conference held for 2.5 days between June 29th and July 1st, 2009 [12]. For data collection, active RFID devices were used to detect and record face-to-face proximity relations of persons wearing the RFID badges. These devices can detect face-to-face proximity (1–1.5 m) of another device with a temporal resolution of $\tau = 20$ s. Thus in a single hour there can be a maximum of $n = 3600/\tau = 180$ network snapshots.
2. INFOCOM, 2005 ($INF^{05}_{Original}$): The data were collected over 4 days at the IEEE INFOCOM 2005 conference [13]. Participants in the experiment were 50 students and researchers, equipped with mobile communication devices (i-Motes). The time resolution τ was again assumed to be 20 s. A link has been constructed at a certain time, if the two nodes were within the communication range.
3. INFOCOM, 2006 ($INF^{06}_{Original}$): These data were collected over 5 days at the IEEE INFOCOM 2006 conference in Barcelona [14]. In this case, number of participants were 78 students and researchers, equipped with i-Motes and an additional 20 stationary i-Motes were deployed as location anchors. The value of $\tau = 20$ s is also used here.

Table 1
Datasets abbreviation.

Dataset	Real network	Random temporal model	Configuration model	Shuffled snapshots model
HYPERTEXT, 2009	$HT^{09}_{Original}$	RG^{09}_{HT}	HT^{09}_{Config}	$HT^{09}_{Shuffled}$
INFOCOM, 2005	$INF^{05}_{Original}$	RG^{05}_{INF}	INF^{05}_{Config}	$INF^{05}_{Shuffled}$
INFOCOM, 2006	$INF^{06}_{Original}$	RG^{06}_{INF}	INF^{06}_{Config}	$INF^{06}_{Shuffled}$

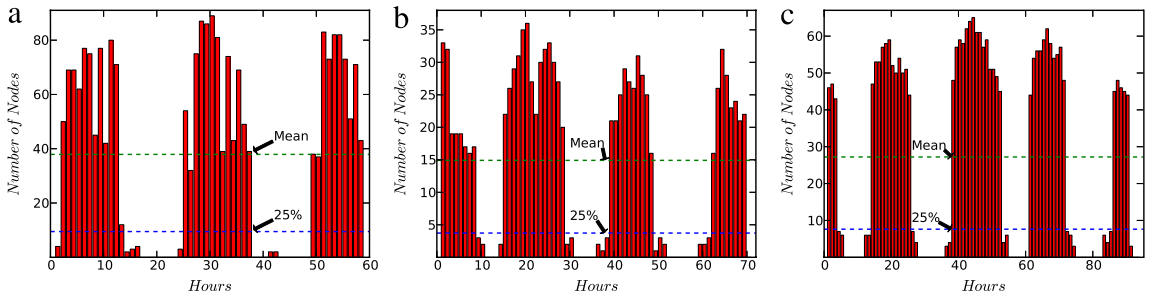

Fig. 1. (Color online) Node distribution for (a) $HT^{09}_{Original}$, (b) $INF^{05}_{Original}$ and (c) $INF^{06}_{Original}$.

Moreover, on more careful inspection we found that both the INFOCOM networks (2005 and 2006) contain a large number of links which has duration less than the reported resolution, even with same starting and finishing time. These may have typically arrived due to some network error, rebooting etc. For all practical purposes we can assume that a contact less than 20 s is not a social contact. Hence, we eliminated those links from the network snapshots.

2.1.2. Control networks

We produce three synthetic datasets for each of the aforementioned real-world network (G).

1. Random temporal model (G): For this purpose, we keep the number of nodes for each snapshot same as in G. The edges in each snapshot are formed based on the edge formation probability, $p = \langle k \rangle / N$, where $\langle k \rangle$ is the average degree of a snapshot in G and N is the number of live nodes in that snapshot of G.
2. Configuration model (G): In this case, we generate each snapshot according to the configuration model [15] to keep the degree sequence same as in G. This model preserves the effect of hubs in the generated random network.
3. Shuffled snapshots model (G): In this case, we randomly shuffle the temporal ordering of the snapshots of G using Fisher–Yates shuffling algorithm [16] as described below.

```
Fisher–Yates Shuffling Algorithm (Array, n)      # To shuffle an array
  for i from n − 1 downto 1 do                        a of n elements
      j ← random integer with 0 ≤ j ≤ i               (indices 0 . . . n − 1)
      exchange a[i] and a[j]
  return Array
```

We pass a temporal network consisting of an array of 180 static network snapshots to this algorithm and a shuffled sequence of network snapshots is produced.

Table 1 shows the naming conventions used for all the networks in rest of the paper.

2.1.3. Silence hour

It is important to note that usually human interactions are bursty in nature [12,17–20]. Similar evidences have been found in each of the datasets. We identify these as *silence hours* and discard them from the rest of our analysis. To identify these silence hours first we plot the histogram of the number of active nodes and we find that in case of $HT^{09}_{Original}$, certain hours have very low number of active nodes (see Fig. 1(a)), specifically lower than 25% of the mean of the distribution. Hence, for the HT^{09} networks, we identify these hours as silence hours. For consistency, we have applied the same analysis for the other two data ($INF^{05}_{Original}$ and $INF^{06}_{Original}$).

Table 2 shows the overall statistics of the used datasets in our experiments.

2.2. Temporal networks, variables and parameters

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 function is affected. This is popularly modeled as *attack* in the literature.

We adopt a simple approach to formulate the attack scheme. In a particular hour, we rank the nodes based on a particular attack strategy – (i) average node degree [8], (ii) temporal closeness [8], (iii) number of node contacts-updates [8], (iv) node

Table 2
Datasets statistics.

Dataset	No. of nodes	No. of edges/hour	No. of active hours
$HT^{09}_{Original}$	113	358.94	32
$INF^{05}_{Original}$	41	2756.72	41
$INF^{06}_{Original}$	78	3853.10	50

persistence and (v) nodes within communities of hourly aggregated network – and remove a fraction (P_{attack}) of the highest rank nodes based on each of these strategy 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, we perform the following: for every hour we study the networks at 20 s 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 provided by each of these metrics we select the candidates for attack in the next 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. The assumption is that attacks on such short time spans should appropriately reflect the effect of the shorter-time correlations. 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 for different values of P_{attack}.

For the rest of our discussion, we consider N as the total number of unique nodes in the network in a given time window $[t_1, t_n]$.

2.3. The attack strategies

In this section, we discuss in detail the different metrics we use to produce the ranking of nodes for the purpose of attack.

2.3.1. Average node degree

In a given time interval $[t_1, t_n]$ the average node degree of a node i is the average degree of i during this time interval [8].

$$deg_G(i; t_1, t_n) = \frac{1}{(N-1)} \sum_{j=1}^{n} deg_{G(t_j)}(i) \tag{1}$$

where $deg_{G(t_j)}(i)$ denotes the degree of node i in jth snapshot of G [8].

2.3.2. Temporal closeness

In a given time interval $[t_1, t_n]$, the temporal closeness of a node i is defined as an average sum of the temporal distances of i from all the other nodes in the network [8].

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

where $d_{ji}(t_1, t_n)$ is the temporal distance between nodes j and i in the time interval $[t_1, t_n]$ [8].

2.3.3. Number of node contacts-updates

Since a temporal network evolves with time, here we cannot measure betweenness centrality [21] as in static graphs. To extend the similar concept for a temporal network, the authors in [8] have proposed a new metric known as *number of node contacts-updates*. For a node, it is defined as the number of shortest temporal paths between all pairs of nodes passing through it during a given time window. Formally, a node i increases its score by 1 for a pair of nodes j and k if $d_{ik}(t_1, t_2) < 1 + d_{jk}(t_1, t_2)$ [8]. The fundamental difference between these two metrics is, betweenness centrality deals with shortest path in static graphs whereas number of node contacts-updates considers temporal shortest paths [7].

2.3.4. Node persistence

In a given time interval $[t_1, t_n]$ the temporal node persistence of a node i is the average frequency of occurrence of the node i during the time interval $[t_1, t_n]$.

$$Np_G(i; t_1, t_n) = \frac{1}{n} \sum_{j=1}^{n} \delta_{t_j}(i) \tag{3}$$

where

$$\delta_{t_j}(i) = \begin{cases} 1, & \text{if } i \in V_{t_j} \text{ at } t_j{}^{th} \text{ time step.} \\ 0, & \text{otherwise.} \end{cases} \tag{4}$$

$\delta_{t_j}(i)$ represents the presence of node i in the jth snapshot of the network. If it is present then $\delta_{t_j}(i)$ is 1 otherwise it remains 0.

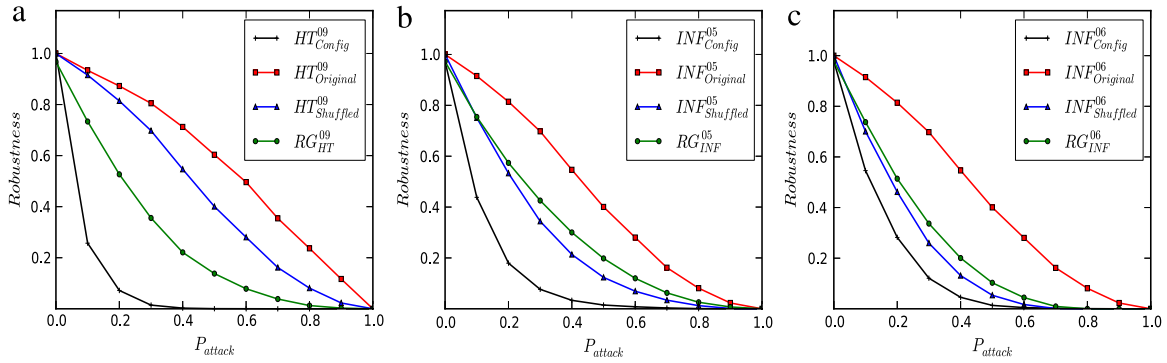

Fig. 2. (Color online) Temporal robustness (shown as *Robustness*) as a function of the fraction of nodes under attack (shown as P_{attack}) for average node degree based attack. (a) HYPERTEXT, 2009 (HT^{09}), (b) INFOCOM, 2005 (INF^{05}), (c) INFOCOM, 2006 (INF^{06}).

2.3.5. Communities in hourly aggregated network

In a static network, a community represents a bunch of nodes that are well-connected among themselves but less-connected with the other nodes in the network. Similarly, such well-connected nodes in a temporal network can exist within a given time window. It can be seen that if we do community analysis on the aggregated network during a given time window then these communities could tell us about those nodes who remain well-connected among themselves during the given time window. Therefore, to detect the communities within each hour, we have aggregated the network during each hour followed by community analysis using Louvain algorithm [22]. Note that this is the only attack strategy where we aggregate the 180 snapshots together into one single network since we intend to extract a few temporal cores which are actually the recurrent substructures of that particular hour. Using these representative temporal cores we attack the individual 180 snapshots one by one and obtain the average robustness of the entire time period.

We then rank the nodes according to the size of the communities in which they appear in decreasing order and remove a fraction of them during attack. For the nodes occurring within the same community, we break ties by choosing one of them randomly for elimination at each step. The results are averaged over 50 such random trials.

2.4. The robustness measurement

In this subsection, we review the metric introduced in Ref. [7] for measuring the extent of attack tolerance of a network. It depends on another network metric known as temporal efficiency defined as follows.

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

$$E_G(t_1, t_n) = \frac{1}{N(N-1)} \sum_{i,j;i\neq j} \frac{1}{d_{ij}(t_1, t_n)} \tag{5}$$

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 $[t_1, t_n]$.

Temporal network robustness is the relative change of the efficiency after a structural damage D. If the temporal efficiency of the damaged network is E_{G_D}, then the temporal robustness is expressed as

$$R_G(D) = \frac{E_{G_D}}{E_G} = 1 - \frac{\Delta E_{G_D}}{E_G} \tag{6}$$

where E_G is the efficiency of the temporal network before the damage.

3. Results

3.1. Attacks

Fig. 2 shows the robustness of each of the datasets under average node degree attack. Note that this attack is not so pronounced. It is not able to affect the real-world networks in all the cases as it does to any of the randomized versions of the same network. Since, the curves for all the real networks in Fig. 2 show higher robustness than the shuffled and randomized versions for all choices of P_{attack}, we infer that attack tolerance against targeted attack of the real-world networks is markedly higher than that of shuffled and randomized networks. In case of configuration model, it shows sharp degradation in the robustness since the graph contains hubs i.e., higher degree nodes; further, as the time correlation is also absent, the network is significantly vulnerable to this attack.

The comparison with the random counterparts for the other 4 attacks also indicate similar trends as in Fig. 2. Thus, in Fig. 3(a)–(c) we only compare the different attack strategies when applied to the three real networks. Note that the

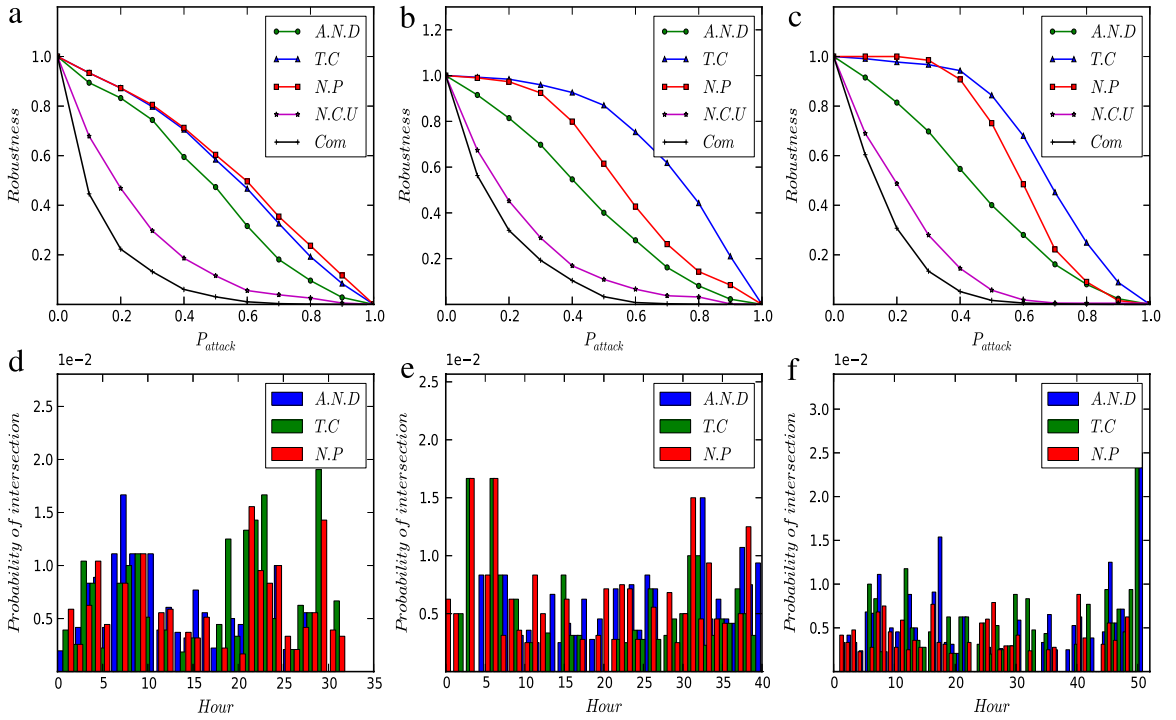

Fig. 3. (Color online) (a)–(c) correspond to temporal robustness (shown as *Robustness*) as a function of the fraction of nodes under attack (shown as P_{attack}) for each different attack strategies, (a) HYPERTEXT, 2009 ($HT^{09}_{Original}$), (b) INFOCOM, 2005 ($INF^{05}_{Original}$),(c) INFOCOM, 2006 ($INF^{06}_{Original}$) and (d)–(f) show the probability of intersection of top 10% nodes through different ranking schemes in each hour with the largest community in the next hour. The same order of the dataset is preserved in (d)–(f) also. *A.N.D*: Average Node Degree, *T.C*: Temporal Closeness, *N.P*: Node Persistence, *N.C.U*: Number of Node Contact-updates, *Com*: Aggregated Community.

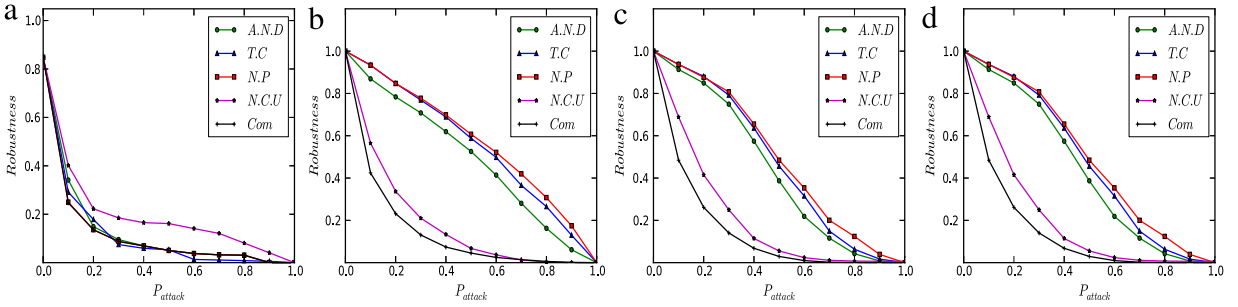

Fig. 4. (Color online) Robustness profile for $HT^{09}_{Original}$. (a) 15 min, (b) 30 min, (c) 2 h, (d) 6 h.

community based attack causes the largest damage to all the three networks and is hence the most successful one. In addition, we also report in Fig. 3(d)–(f), for the three respective datasets, the probability that the top 10% nodes ranked in a particular hour, by the 3 most unsuccessful attack strategies are found to be present in the largest community of the next hour. The very low probability values indicate that these nodes are usually not the part of the largest community and hence are not able to disturb the network structure. One may also choose the top 20% or 30% nodes; however this shall only dilute the restriction and result in less meaningful outcomes.

3.2. Effect of the size of observation windows

In this section, we present results for different sizes of the observation windows in Fig. 4. The result consists of windows of 15 min, 30 min, 2 h and 6 h respectively. It can be observed that the community based attack performs always better than the others. For even smaller size observation windows the statistics obtained is too noisy to produce an accurate ranking, thereby, leading to inappropriate results.

Further, in Fig. 5 we present the difference between our work and that of [8] in terms of the choice of the window size. Here we can see, as we increase the time window from 1 h to 30 h (one half of the entire data) all the curves almost collapse

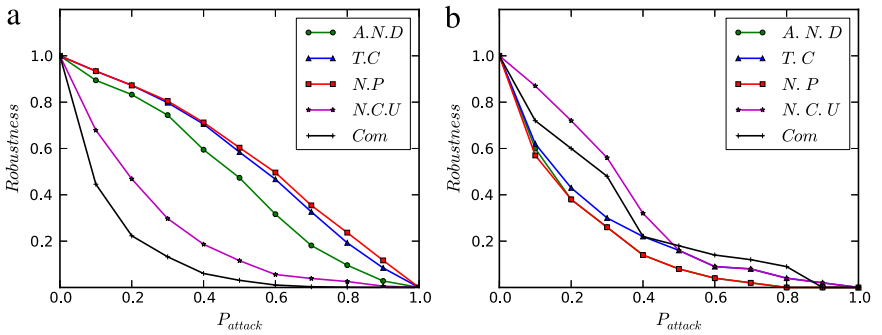

Fig. 5. (Color online) Robustness profile for $HT^{09}_{Original}$ with window size (a) 1 h and (b) 29 h.

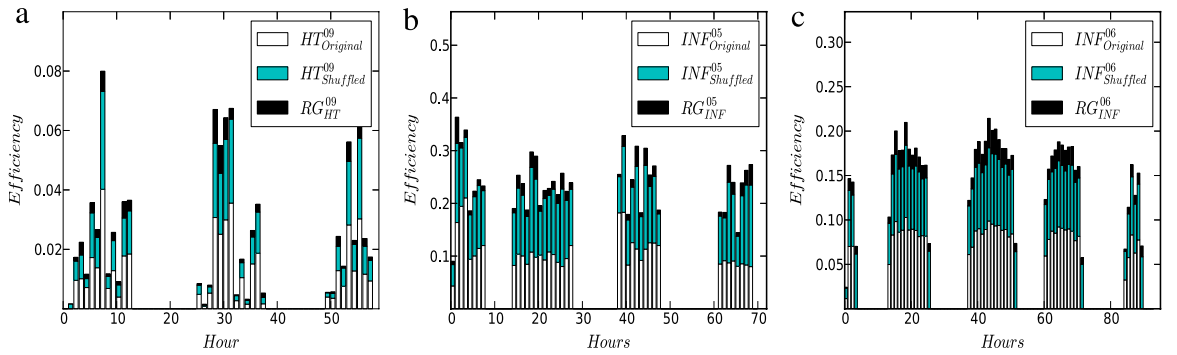

Fig. 6. (Color online) Stacked bar plot of efficiency of different temporal networks. (a) HT^{09}, (b) INF^{05}, (c) INF^{06} along with the shuffled and the randomized versions.

on each other which is exactly same as Fig. 11(a) in [8]. In addition, the community based attack performs equally as other attack schemes since the short time correlations are no longer prevalent.

3.3. Temporal efficiency and edge emergence factor (ξ)

To understand the structural properties of a real and a random network better, we evaluate the temporal efficiency of both these networks corresponding to each single dataset.

3.3.1. Temporal efficiency

Fig. 6 shows the efficiency profile for three above mentioned networks. The efficiency has been measured separately in each observation window of one hour.

It can be seen, $INF^{05}_{Original}$ and $INF^{06}_{Original}$ have much higher efficiency than that of the $HT^{09}_{Original}$. It is possibly due to two different devices i-Mote and RFID badge that have been used for data collection in the INFOCOM and HYPERTEXT conferences, respectively. i-Motes start each single scan after a certain interval and record all the Bluetooth devices that are within a predetermined radius. On the other hand, RFID devices track only face-to-face proximity. Hence the number of links recorded per device is more in the former case than in the latter causing the former graphs to be relatively more dense.

In order to explain the higher efficiency of the real network, we investigate the dynamical property of these networks tied to their functional behavior at shorter time scales. We call this property the edge emergence factor and define it as follows.

3.3.2. Edge emergence factor (ξ)

Edge emergence factor precisely estimates the number of edges that branch out at a particular time instance from the endpoint of any single edge existing in the immediate previous time instance. We define this quantity as follows.

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

$$\xi(t_1, t_n) = \frac{\sum_{t=1}^{n-1} |A_{t+1}|}{\sum_{t=1}^{n-1} |E_t|} \tag{7}$$

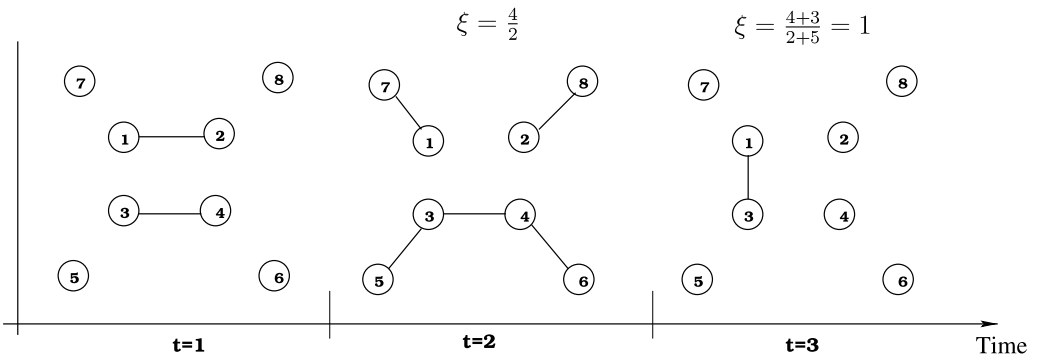

Fig. 7. A temporal network with 3 time-steps, i.e., $n = 3$. ξ stands for edge emergence factor. In this example, ξ is $\frac{(4+3)}{(2+5)} = 1$. At $t = 1$ there are two edges $(1, 2)$ and $(3, 4)$; at $t = 2$ the edges $(1, 7)$, $(2, 8)$ emerge from $(1, 2)$ and the edges $(3, 5)$, $(4, 6)$ emerge from $(3, 4)$. Hence out of 2 edges at $t = 1$, 4 edges emerge at $t = 2$. Similarly the edge $(1, 3)$ at $t = 3$ has emerged from $(1, 7)$ or $(3, 5)$ or $(3, 4)$ thus making the final $\xi = \frac{(4+3)}{(2+5)}$.

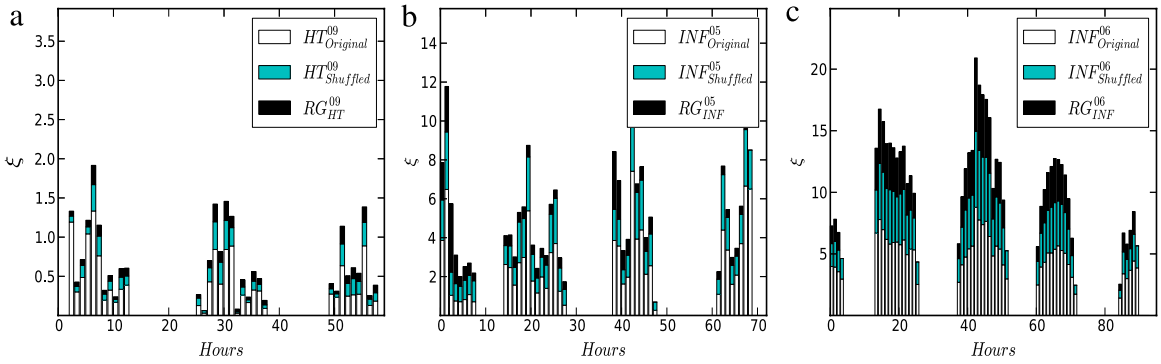

Fig. 8. (Color online) Stacked bar plot of edge emergence factor (ξ) of different temporal networks. (a) HT^{09}, (b) INF^{05}, (c) INF^{06} along with the shuffled and randomized versions.

Fig. 7 illustrates an example showing the calculation of ξ of a network. Note that in this definition, edges have been counted multiple times to account for the fact that the message could get disseminated via any one of the edges emanating out.

Fig. 8 indicates that the real-world time-varying networks have a significantly higher edge emergence factor than the randomized counterparts. Note that any sort of randomization actually destroys the shorter-time correlations in the network, thereby, reducing manifolds the ξ that are usually found in the real networks.

3.4. Connecting structure and function

An important issue that needs to be discussed in order to complete the picture is why the community based attack is effective in destroying the higher temporal robustness in real-world networks. The key reason for this is possibly tied to the fact that this structural property determines the functional behavior (i.e., the ξ) controlling the dynamic flow of information over the network. A simple way to understand the importance of community is to take into consideration the size of the largest community. Fig. 9 indicates that the size of the largest community bears a very high correlation with the ξ, for all the three different datasets. The community based attack actually quickly destroys all possible paths of communication in the network, thereby, resulting in the collapse of the network backbone consisting of most of the active nodes, (see the profile for $|V|$ in the same figure) which does not take place even when certain high-ranked nodes (in terms of average degree, centrality etc.) are removed from the system.

3.5. Comparisons of the results

To summarize all the analysis we have shown the Jensen–Shannon divergence for all 3 datasets. In Table 3, rows correspond to the divergence between the robustness distribution of the real-world network versus the random counterpart. Each of the columns, describes the strategy for which the Jensen–Shannon divergence has been reported. The divergence in general is significantly indicating that the robustness distribution obtained from the real and the random network are very different. In addition, the arrow heads indicate whether the robustness distribution of the real network lie above (up-arrow) or below (down arrow) the random networks. Note that as expected, for the community based attack we always observe a down arrow.

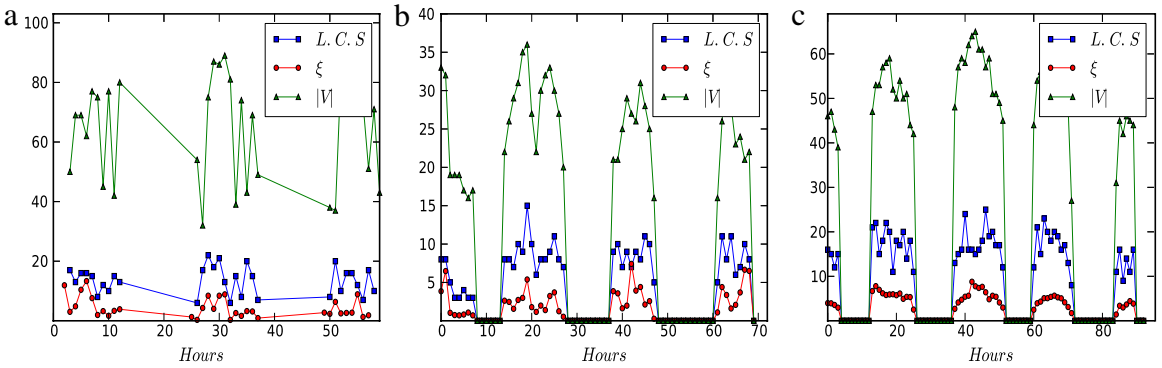

Fig. 9. (Color online) Relation between edge emergence factor (ξ) and size of the largest community and node distribution in each hour for different real-world networks. (a) HYPERTEXT, 2009 ($HT^{09}_{Original}$), (b) INFOCOM, 2005 ($INF^{05}_{Original}$), (c) INFOCOM, 2006 ($INF^{06}_{Original}$). In case of HYPERTEXT ($HT^{09}_{Original}$), the values of ξ are multiplied with a scaling factor 10 for a better visualization.

Table 3
Jensen–Shannon divergence between robustnesses of real networks and its random counterpart.

Jensen–Shannon divergence	Average node degree	Temporal closeness	Node persistency	Node contact updates	Aggregated community
$HT^{09}_{Original}$& RG^{09}_{HT}	0.032 ↑	0.053 ↑	0.059 ↑	0.0017↓	0.036 ↓
$INF^{05}_{Original}$& RG^{05}_{INF}	0.009 ↑	0.071 ↑	0.037↑	0.03↓	0.06↓
$INF^{06}_{Original}$& RG^{06}_{INF}	0.041 ↑	0.028 ↑	0.025 ↑	0.011 ↓	0.048 ↓

4. Conclusions

In conclusion, the summary of our contributions are that we are able to identify the presence of short-time correlations in dynamic networks followed by the quantification of such correlations using the edge emergence factor. We launch various targeted attacks in shorter time spans of the network and observe that a majority of the attack strategies fail to collapse the network. A crucial finding in this respect is that, community based attacks appear to be the most effective method to disrupt the temporal robustness of real-world dynamic networks.

There are quite a few interesting future directions of this work. As a first step, we would attempt to analytically formulate and estimate the effect of different attack strategies on the available models of temporal networks. We would also attempt to investigate the resolution limit of the current study, i.e., the temporal resolution for which the current observations hold true. Finally, we would like to analyze at a further microscopic level, whether the timing behavior of the network bears any correlation with the type of the attack launched thus pointing to a hybrid and perhaps even more successful strategy of targeted attack.

References

[1] R. Albert, H. Jeong, A. Barabasi, Error and attack tolerance of complex networks, Nature 406 (6794) (2000) 378–382. http://dx.doi.org/10.1038/35019019.
[2] P. Holme, B.J. Kim, C.N. Yoon, S.K. Han, Attack vulnerability of complex networks, Phys. Rev. E 65 (2002) 056109. http://dx.doi.org/10.1103/PhysRevE.65.056109.
[3] M.E.J. Newman, G. Ghoshal, Bicomponents and the robustness of networks to failure, Phys. Rev. Lett. 100 (2008) 138701. http://dx.doi.org/10.1103/PhysRevLett.100.138701.
[4] V. Latora, M. Marchiori, Vulnerability and protection of infrastructure networks, Phys. Rev. E 71 (2005) 015103. http://dx.doi.org/10.1103/PhysRevE.71.015103.
[5] [link]. URL http://www.cl.cam.ac.uk/~cm542/phds/johntang.pdf.
[6] T. Takaguchi, T. Hasegawa, Y. Yoshida, Suppressing epidemics on networks by exploiting observer nodes, Phys. Rev. E 90 (2014) 012807. http://dx.doi.org/10.1103/PhysRevE.90.012807.
[7] S. Scellato, I. Leontiadis, C. Mascolo, P. Basu, M. Zafer, Understanding robustness of mobile networks through temporal network measures, in: INFOCOM, 2011 Proceedings, IEEE, 2011, pp. 1–5. http://dx.doi.org/10.1109/INFCOM.2011.5935006.
[8] S. Trajanovski, S. Scellato, I. Leontiadis, Error and attack vulnerability of temporal networks, Phys. Rev. E 85 (2012) 066105. http://dx.doi.org/10.1103/PhysRevE.85.066105.
[9] S. Lee, L.E.C. Rocha, F. Liljeros, P. Holme, Exploiting temporal network structures of human interaction to effectively immunize populations, PLoS One 7 (5) (2012) e36439. http://dx.doi.org/10.1371/journal.pone.0036439.

[10] M. Starnini, A. Machens, C. Cattuto, A. Barrat, R. Pastor-Satorras, Immunization strategies for epidemic processes in time-varying contact networks, J. Theoret. Biol. 337 (0) (2013) 89–100. http://dx.doi.org/10.1016/j.jtbi.2013.07.004.
[11] V. Kostakos, Temporal graphs, Physica A 388 (6) (2009) 1007–1023. http://dx.doi.org/10.1016/j.physa.2008.11.021.
[12] L. Isella, J. Stehlé, A. Barrat, C. Cattuto, J. Pinton, W. Van den Broeck, What's in a crowd? analysis of face-to-face behavioral networks, J. Theoret. Biol. 271 (1) (2011) 166–180. http://dx.doi.org/10.1016/j.jtbi.2010.11.033.
[13] J. Scott, R. Gass, J. Crowcroft, P. Hui, C. Diot, A. Chaintreau, CRAWDAD trace cambridge/haggle/imote/infocom (v. 2006-01-31).
[14] J. Scott, R. Gass, J. Crowcroft, P. Hui, C. Diot, A. Chaintreau, CRAWDAD trace cambridge/haggle/imote/infocom2006 (v. 2009-05-29).
[15] M. Newman, The structure and function of complex networks, SIAM Rev. 45 (2) (2003) 167–256. http://dx.doi.org/10.1137/S003614450342480.
[16] [link]. URL http://en.wikipedia.org/wiki/Fisher–Yates_shuffle.
[17] A.-L. Barabasi, Bursts: The Hidden Patterns Behind Everything We Do, from Your E-mail to Bloody Crusades, Reprint Edition, Plume, 2011.
[18] A.-L. Barabasi, The origin of bursts and heavy tails in human dynamics, Nature 435 (2005) 207. http://dx.doi.org/10.1038/nature03459.
[19] R.D. Malmgren, D.B. Stouffer, A.E. Motter, L.A.N. Amaral, A Poissonian explanation for heavy tails in e-mail communication, Proc. Natl. Acad. Sci. 105 (47) (2008) 18153–18158. http://dx.doi.org/10.1073/pnas.0800332105.
[20] L.E.C. Rocha, F. Liljeros, P. Holme, Information dynamics shape the sexual networks of internet-mediated prostitution, Proc. Natl. Acad. Sci. (2010) http://dx.doi.org/10.1073/pnas.0914080107.
[21] L.C. Freeman, A set of measures of centrality based on betweenness, Sociometry 40 (1) (1977) 35–41. http://dx.doi.org/10.2307/3033543.
[22] V. Blondel, J. Guillaume, R. Lambiotte, E. Mech, Fast unfolding of communities in large networks, J. Stat. Mech. (2008) P10008. http://dx.doi.org/10.1088/1742-5468/2008/10/P10008.