Error and attack vulnerability of temporal networks

S. Trajanovski,[1,*] S. Scellato,[2,†] and I. Leontiadis[2,‡]
[1]*Faculty of Electrical Engineering, Mathematics and Computer Science, Delft University of Technology, P.O. Box 5031, 2600 GA Delft, The Netherlands*
[2]*Computer Laboratory, University of Cambridge, William Gates Building, 15 JJ Thomson Avenue, Cambridge CB3 0FD, United Kingdom*
(Received 6 January 2012; revised manuscript received 1 April 2012; published 6 June 2012)

The study of real-world communication systems via complex network models has greatly expanded our understanding on how information flows, even in completely decentralized architectures such as mobile wireless networks. Nonetheless, static network models cannot capture the time-varying aspects and, therefore, various temporal metrics have been introduced. In this paper, we investigate the robustness of time-varying networks under various failures and intelligent attacks. We adopt a methodology to evaluate the impact of such events on the network connectivity by employing temporal metrics in order to select and remove nodes based on how critical they are considered for the network. We also define the temporal robustness range, a new metric that quantifies the disruption caused by an attack strategy to a given temporal network. Our results show that in real-world networks, where some nodes are more dominant than others, temporal connectivity is significantly more affected by intelligent attacks than by random failures. Moreover, different intelligent attack strategies have a similar effect on the robustness: even small subsets of highly connected nodes act as a bottleneck in the temporal information flow, becoming critical weak points of the entire system. Additionally, the same nodes are the most important across a range of different importance metrics, expressing the correlation between highly connected nodes and those that trigger most of the changes in the optimal information spreading. Contrarily, we show that in randomly generated networks, where all the nodes have similar properties, random errors and intelligent attacks exhibit similar behavior. These conclusions may help us in design of more robust systems and fault-tolerant network architectures.

DOI: 10.1103/PhysRevE.85.066105 PACS number(s): 89.75.Fb

I. INTRODUCTION

In the famous example of the "six degrees of separation" [1], a message initiated by one person needs at most six intermediate steps to reach anyone on the planet. Yet these social networks constantly evolve over time. For instance, the fact that two people met at some point in time does not necessarily indicate that they will meet again in future. These temporal correlations greatly affect information propagation, as a specific time ordering of events is required to allow two entities to communicate. Consequently, temporal-network metrics have been introduced, since they allow a better understanding of the dynamic properties of such systems. In addition, it has been shown [2,3] that such temporal aspects cannot be ignored, otherwise the system performance can be greatly overestimated.

An important issue in communication networks is to understand whether these systems can maintain acceptable performance when they sustain varying degrees of damage. In general, network damages can be divided into two classes: random errors, reflecting internal faults, and intelligent attacks, which represent malicious external damage on influential nodes (e.g., electric power stations).

While the reliability of static networks has been widely studied [4–7], network robustness and temporal network analysis have rarely been used together in performance evaluation of time-varying systems [8]. Our work considers temporal network vulnerability under several intelligent attack strategies. The present paper further expands this research thread by studying the effects of several error and attack strategies on real systems and theoretical models with either presence or absence of dominant nodes. Our main goal is to understand how time-varying networks react to random errors and targeted attacks.

Network robustness has been intensively studied in the past years [9,10]. Initially, such studies investigated connectivity after failures [11–13], using common theoretical [14] and empirical methodologies. The robustness of power-law networks has been studied [4,15,16], as they accurately model real world examples, such as World Wide Web [17]. In particular, the robustness of the Internet has been considered by Cohen *et al.* under random errors [15] or targeted attacks [16]. In order to fully characterize network vulnerability, several metrics different from connectivity have been used, such as average shortest path [18], global clustering coefficient [19], or bicomponent [6]. The vulnerability of static networks under errors and different types of attacks has been intensively researched [4,5,7]. Intelligent attacks are usually based on centrality node measures [20], such as node degree [21], closeness [22–24], betweenness [25], or data-information centrality [26]. However, all these studies used a static network representation that, as it was shown in Refs. [2,3], vastly overestimate the network robustness in temporal networks. The first attempt to express temporal network properties was made by Kempe *et al.* [27], considering time labels of links, but neglecting temporary disconnected nodes. A thorough survey on temporal networks and existing analysis methods has been proposed by Holme and Saramäki [28]. Temporal

*s.trajanovski@tudelft.nl; part of the research was done while S.T. was a student at University of Cambridge.
†salvatore.scellato@cl.cam.ac.uk
‡ilias.leontiadis@cl.cam.ac.uk

correlations and periodical behavior of human interactions was considered in Ref. [29]. The concept of temporal networks as a collection of static network topologies taken in suitable time resolution was proposed in Ref. [30]. More recently, in Refs. [2,3] the authors defined a set of temporal metrics in order to characterize the properties of such dynamic networks. Finally, in Ref. [8] the concept of temporal network robustness is explored. However, this work only considered random failures. Our work applies temporal network theory to study the robustness of dynamic real-world networks against intelligent attacks. Furthermore, we describe how our results can be used to characterize the importance of nodes based on their temporal properties.

The paper continues as follows. Section II presents the concepts of temporal metrics, temporal robustness, and used error and attacking strategies. In Sec. III, theoretical models are introduced and the results of temporal robustness evaluation are discussed. Section IV presents the real temporal networks; the results of the evaluation are given and possible directions for improving the robustness of temporal networks are suggested. Finally, we conclude in Sec. V.

II. TEMPORAL ROBUSTNESS AND ATTACKING STRATEGIES

Before introducing the temporal metrics that we use for our study, we will describe the notion of temporal networks as in Ref. [30].

Definition 1. A temporal network $G(t) = G(V, E(t))$ is a sequence of n undirected static network representations $\{G(t_i)\} = \{G(V, E(t_i))\}$ $(i = 1,2,\ldots,n-1,n)$.

A temporal network may be thought as sequence of consecutive static graphs with a fixed set of nodes V and time evolving set of links (Fig. 1).

At a certain time instance t, a node b receives a message from node a if and only if there is a direct link between a and b at that moment t. We define a temporal path between nodes a and b as a sequence of nodes $\{n_i\}$ by a flooding concept: a message sent by a at time t_0 is received by n_1 at time $(t_0 + 1)$; the message sent by n_1 is received by n_2 at the next time step $(t_0 + 2)$; a message sent by n_i is received by n_{i+1} at $(t_0 + i)$, where $a \equiv n_0$ and $b \equiv n_d$. The temporal length of this path is d—the time required for a message sent by a to be received by b. In general, there might be more than one temporal path between two nodes. At this point, temporal distance can be defined.

Definition 2. Temporal distance $d_{ij}(t_1,t_2)$ between nodes i and j is the smallest temporal length among all the temporal paths between i and j in the time interval $[t_1,t_2]$.

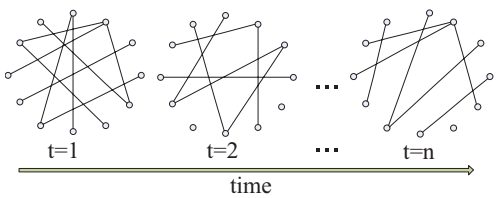

FIG. 1. (Color online) Example of temporal network. During the time evolution, the number of nodes is fixed and the presence of each link changes.

In the case where it is not possible to spread the message between two particular nodes i and j, the temporal distance is infinity. In order to resolve those cases, the inverse value of temporal length is considered.

Definition 3. Temporal efficiency is the averaged sum of the inverse temporal distances over all pairs of nodes in the time interval $[t_1,t_2]$:

$$E_G(t_1,t_2) = \frac{1}{N(N-1)} \sum_{i,j;i\neq j} \frac{1}{d_{ij}(t_1,t_2)}.$$

The average temporal efficiency is normalized in the interval $[0,1]$. The value 0 is achieved if and only if there are no links in the network and all the nodes are isolated during the whole period $[t_1,t_2]$. On the other hand, value 1 is achieved if and only if the temporal network is fully connected.

Due to the network's constant evolving, we need to define an appropriate window $\tau = t_2 - t_1$ to evaluate the efficiency. In essence, the efficiency $E_G(t)$ of a network at time t is evaluated in a time window $[t-\tau,t]$. The size of the window τ effectively imposes an upper bound on the temporal distances as all paths longer than τ will be ignored. It has been shown [8] that temporal efficiency has an increasing and transient behavior, which depends on the size of the network, until reaching a stable stationary value. Therefore, τ should be large enough so that any possible communication delay can be considered.

Definition 4. 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 by

$$R_G(D) = \frac{E_{G_D}}{E_G} = 1 - \frac{\triangle E(G,D)}{E_G},$$

where E_G is the efficiency of the temporal network $G(t)$ before the damage.

It is important to highlight that both E_{G_D} and E_G have to be taken as stable values (τ large enough) for relevant robustness evaluation. The effect of taking a small τ is also shown in the evaluation.

A. Random error

When such errors occur, a random subset of the nodes is removed. The selection of nodes is not related to some static or temporal property as each node can fail with independent identical probability P_{error}. Therefore, the expected number of attacked nodes is $N_{\text{attacked}} = P_{\text{error}}N$, where N is the original number of nodes in the network.

B. Intelligent attacks

A planned attack might quickly cripple real-world networks where few nodes are significantly more important than all the other. Intelligent attacks are strategies that target nodes that exhibit some specific temporal properties. The knowledge of how well a system operates when the most important nodes are damaged can help in the decision for future protection of such nodes or even to design robust architectures and mobility models. To evaluate the temporal robustness of a network under intelligent attacks, we designed a methodology that consists of two steps: (i) initially, nodes are ranked using a

certain temporal property and (ii) the top $N_{\text{attacked}} = P_{\text{attack}}N$ nodes are removed. Based on the selected classifying metric, these nodes represent the most important nodes in the network. Furthermore, to study whether this metric is capable of truly selecting those nodes that are significant we also study the robustness of the network when the bottom N_{attacked} are selected. The fluctuation between the best-case and worst-case scenario is defined as the robustness range.

Definition 5. If R_1 and R_2 is the temporal robustness of the best and worse case scenario, respectively, then for a particular attack strategy we define the interval $[R_1, R_2]$ as the temporal robustness range.

For each of the strategies we remove the same portion P_{attack} of the initial set of N nodes. The difference is how these nodes are ranked. In the following part, we will define a number of attack strategies that are based on various temporal metrics.

1. Temporal closeness nodes attack

This attacking strategy is closely related to the closeness centrality of a node: this metric has been initially defined for a static graph as the average shortest path length to all other nodes. Nodes with smaller values are considered more central than nodes with higher values. This metric was extended to be used in temporal networks.

Definition 6. In a given time interval $[t_1,t_2]$, the temporal closeness $C_i(t_1,t_2) = \frac{1}{N-1}\sum_{j;j\neq i} d_{ji}(t_1,t_2)$ of a node i is defined as an average sum of all temporal distances between i and other nodes in the temporal network.

Therefore, the resulting attack strategy picks the nodes with the lowest temporal closeness centrality as these nodes are considered more central and, thus, more "important"in the network.

2. Average node degree attack

In the static graph, the degree of a node i is defined as the number of other nodes that are directly connected to i. For temporal networks, we can define the average degree of a node as follows.

Definition 7. In a given time interval $[t_1,t_n]$ the temporal degree $\deg_G(i;t_1,t_n) = \frac{1}{N-1}\sum_{j=1}^{n} \deg_{G(t_j)}(i)$ of a node i is the average degree of i during this time interval.

Therefore, in this attack strategy the nodes with the highest temporal degree are attacked, as these are likely to quickly spread messages.

3. Number of node contacts-updates attack

Another important metric is to identify the nodes that pass on more messages in the network. These can be highly mobile nodes or even nodes that bridge distant clusters. For example, in an epidemic routing protocol the nodes that forward the latest information are more important than the nodes that send less updates. In static graphs, we have betweenness centrality as a measure of what fraction of the shortest paths between all pairs of nodes pass through a certain node [31]. Similarly, in temporal networks we can capture this notion by measuring the number of message exchanges that occur when two nodes meet. Node i triggers an update when it connects with node j and node i is aware of a shorter temporal distance for another node k. Formally, i updates j for a distance to node k when $d_{ik}(t_1,t_2) < 1 + d_{jk}(t_1,t_2)$.

III. TEMPORAL MODELS

In this section, we evaluate the robustness of various synthetic models. By analyzing theoretical models we can investigate particular properties on very controlled topologies (i.e., we can vary the number of nodes, density, mobility, etc). We consider three classes of such models: the Erdős-Rényi model, the Markov model, and various mobility models.

A. Erdős-Rényi temporal model

In the Erdős-Rényi model, a link between a pair of nodes may appear independently with fixed probability. The static version of the model is well studied, as most of its features (e.g., degree distribution, expected number of edges) are already known [32,33]. The temporal version of this model $G_p(N,t)$ is considered as a sequence of Erdős-Rényi static random graphs $G_p(N,t_i)$ taken in several moments t_i. The Markov temporal model [Fig. 2(a)] is a generalization of Erdős-Rényi temporal model [Fig. 2(b)]. The theorems, regarding average node degree or temporal closeness, also hold for Erdős-Rényi temporal model.

B. Markov temporal model

The Erdős-Rényi model does not take into account temporal correlations and time dependencies at previous moments. The Markov model, which is based on the Markov process evolution, extends the previous model by adding temporal dependencies on previous states.

Depending on the presence or absence of a link, we can define two possible states: ON and OFF. In the sequel of the paper, we denote the probabilities that a link is in the state ON and OFF by Pr[ON] and Pr[OFF], respectively (Pr[ON] + Pr[OFF] = 1). Considering a two-state Markov process [Fig. 2(a)], we denote a transition probability p that a link present at the moment t will not appear at the moment $(t+1)$; and probability q that a link will be added at the moment $(t+1)$, if it was not present at the moment t. According to the Markovian model and the formula for total probability we can calculate the probability for both states ON and OFF [8,34]: $\Pr[\text{ON}] = \frac{q}{p+q}$ and $\Pr[\text{OFF}] = \frac{p}{p+q}$.

In a special case where $p + q = 1$, there is no time correlation and we have a fixed probability q for a link appearance, which corresponds to Erdős-Rényi temporal network as shown in Fig. 2(b).

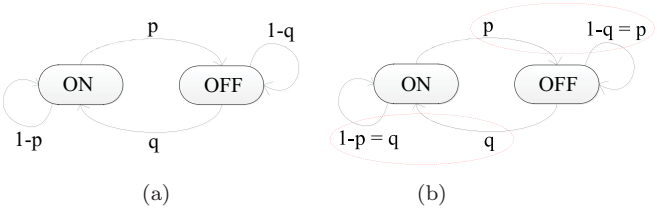

FIG. 2. (Color online) (a) Diagram for link appearance probabilities in Markov temporal model. (b) Erdős-Rényi temporal model. If $p + q = 1$, one can notice that for each link the probability that the same is in the state ON is fixed and equal to q and does not depend on the previous state (ON or OFF). Similarly, for each link the probability that the same is in the state OFF is fixed and equal to p and does not depend on the previous state (ON or OFF). Consequently, it represents the Erdős-Rényi temporal model.

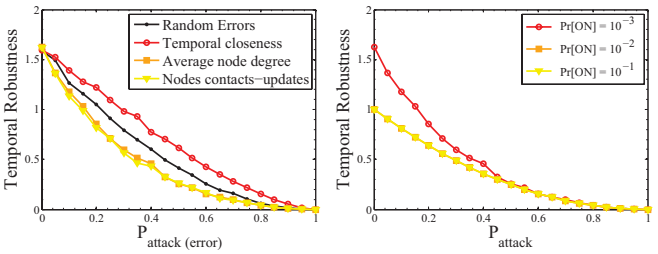

FIG. 3. (Color online) Temporal robustness as a function of removed (attacked) nodes percentage. The small τ effect ($\tau = 20$) in Erdős-Rényi temporal network. Variations and instability in temporal efficiency cause differences in temporal robustness. (a) For different attacking strategies and fixed $\Pr[\text{ON}] = 10^{-3}$; and (b) for average node degree strategy and different probability of link appearance $\Pr[\text{ON}]$.

The following Lemma 1 is a generalization for the Markov models of Lemma 1 in Ref. [8].

Lemma 1. The probability that a node will receive a message, if exactly m other nodes have the message is $p_m = 1 - \Pr[\text{OFF}]^m$.

Based on Lemma 1, the theoretical results for Erdős-Rényi in Ref. [8] regarding temporal metrics and temporal robustness under random errors are applicable for Markov temporal models. Regarding targeted attacks, we have Lemmas 2 and 3.

Lemma 2. The average node degree in Markov temporal network is $(N - 1)\Pr[\text{ON}]$.

Similarly, for temporal closeness of a node in a Markov temporal network we have the following.

Lemma 3. The expected value of temporal closeness in Markov temporal random network is the same for each node.

The proofs of Lemmas 1, 2, and 3 can be found in the Appendix at the end of the paper.

Lemmas 2 and 3 are strong arguments for absence of predominant and important node in Markov temporal models, as simulations (Fig. 14) will confirm later. In conclusion, all the nodes in Markov temporal model have the same properties on average, resulting with a unique robustness curve, independent from the choice of targeted attack or random error. Therefore, we have the same robustness behavior either attacking from the top or the bottom of the ranked list of nodes. In this case, the length of the robustness range interval is 0.

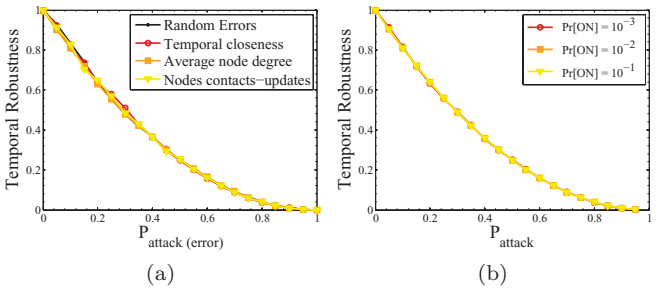

FIG. 4. (Color online) Temporal robustness as a function of removed (attacked) nodes percentage for Erdős-Rényi and Markov temporal network ($N = 100$, $\tau = 150$). Similar results are obtained (a) for different attacking strategies and fixed $\Pr[\text{ON}] = 10^{-3}$; and (b) for average node degree strategy and different probability of link appearance $\Pr[\text{ON}]$.

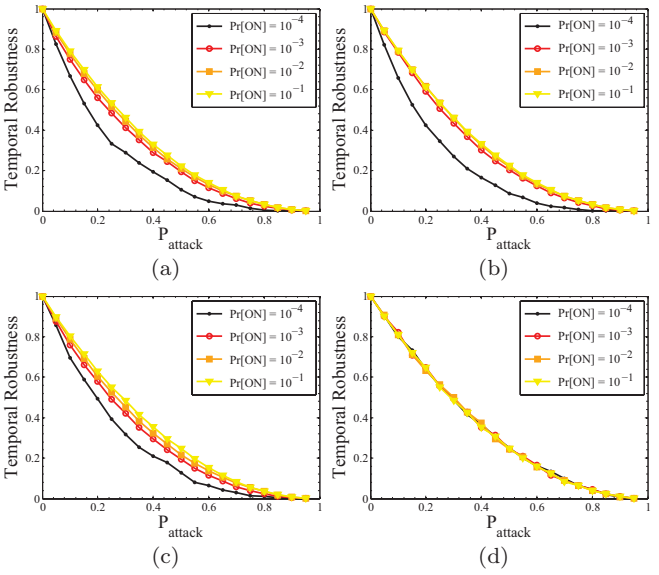

FIG. 5. (Color online) Temporal robustness as a function of removed (attacked) nodes percentage in RWP mobility models ($\tau = 3600$). (a) Temporal closeness, (b) average node degree, (c) nodes number of contacts-updates, and (d) random errors.

C. Mobility models

This group of theoretical models aims to simulate the behavior of mobile networks. Like the Markov temporal model, mobility models preserve time correlations with the previous state. Unlike the Markov temporal model, the probability for changing the state from link presence to absence and vice versa is not constant as it depends on spatio-temporal correlations. These models consider a fixed geographic area where nodes move from one coordinate to another. The probability of link appearance P_{ON} is determined by the communication range r

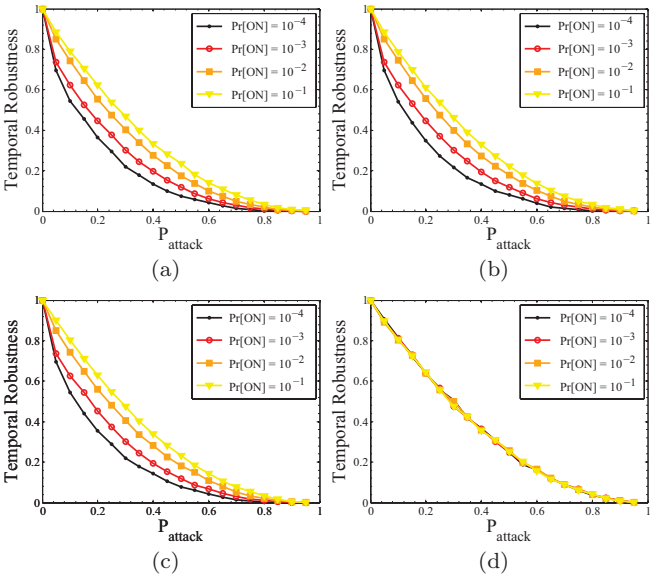

FIG. 6. (Color online) Temporal robustness as a function of removed (attacked) nodes percentage. RWPG mobility models ($\tau = 3600$). (a) Temporal closeness, (b) average node degree, (c) nodes number of contacts-updates, and (d) random errors.

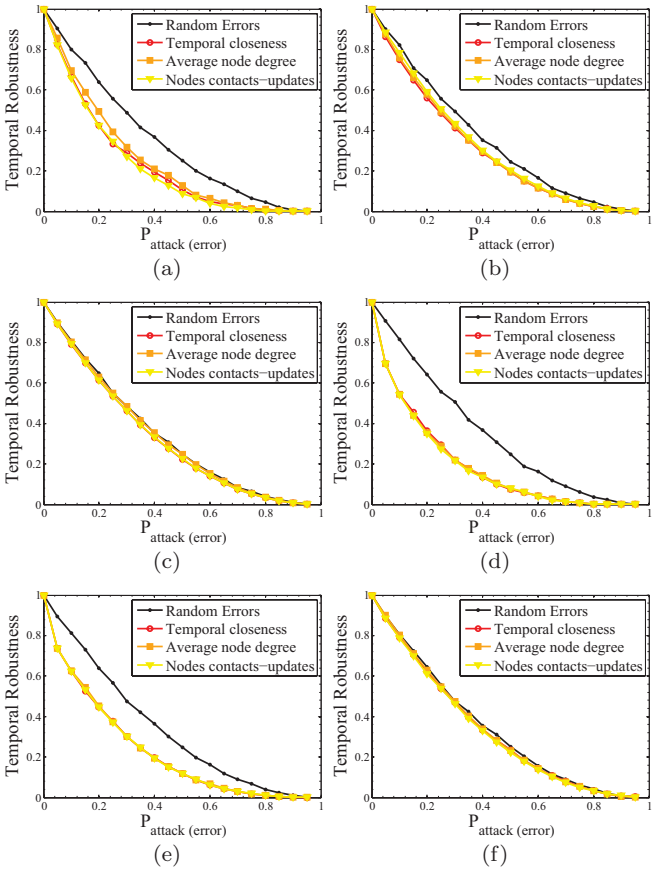

FIG. 7. (Color online) Temporal robustness of RWP and RWPG mobility models ($\tau = 3600$) for different probability of link appearance Pr[ON] as a function of removed (attacked) nodes percentage. As Pr[ON] increases, temporal robustness decreases slowly and intelligent attack robustnesses are closer to the random error. (a) RWP: Pr[ON] $= 10^{-4}$; (b) RWP: Pr[ON] $= 10^{-3}$; (c) RWP: Pr[ON] $= 10^{-1}$; (d) RWPG: Pr[ON] $= 10^{-4}$; (e) RWPG: Pr[ON] $= 10^{-3}$; and (f) RWPG: Pr[ON] $= 10^{-1}$.

and by the density of nodes in the area: if at time t the Euclidean distance between two nodes is shorter than r then we consider that there is a link. We used the UMMF [35] mobility simulator to generate two sets of mobility traces with 100 nodes moving in a $1000m \times 1000m$ area.

A node in the random waypoint model (RWP) uniformly chooses a random location and moves toward this location with a velocity randomly and uniformly chosen in the interval (5–40 mph). After a node has reached the picked destination, it first waits for a randomly chosen number of seconds in the range (0–120 s) and the procedure starts again by picking a destination and appropriate speed. The benefit of the model is that it provides homogeneous spatial mixing among nodes. However, randomness may not express all the aspects of mobility behavior.

In the random waypoint group model (RWPG) there are two types of nodes: group leaders and followers. Denoting the number of group leaders by M, $(N - M)$ followers are assigned to a group with a unique leader. The size of each group is $\frac{N}{M}$ nodes in total, with 1 leader and $(\frac{N}{M} - 1)$ followers. The movement rule here is that only the leader of a group picks a destination, as in the RWP model. Followers in a group just follow their leader, such each keeping a distance shorter than a given span (e.g., 100 meters).

D. Results and discussion

In this section, we investigate the temporal robustness for temporal network models under different attacking strategies and random errors. Temporal network models are generated, such that they contain a fixed number of nodes and in a certain moment a link exists according to the link activation rules for different models. For random temporal networks models (Erdős-Rényi and Markov), the results are obtained after averaging the simulations over 100 repetitions.

1. *Erdős-Rényi and Markov temporal models*

For Erdős-Rényi and Markov models the total length of the time window is $2\tau = 300$, the resolution of the temporal model is 1 (unit time), and the network is attacked in the middle of the time window after $\tau = 150$ moments from the start, which is used for all the simulations regarding Erdős-Rényi and Markov models. It was shown that this time is enough for achieving a stable value for temporal efficiency before and after the error or attack. However, in order to investigate the effect when temporal efficiency does not reach a stable value before and after the error or attack, additional simulations were conducted for $\tau = 20$. The results are shown in Fig. 3.

In Fig. 4(a) we plot the values of temporal robustness for the Erdős-Rényi temporal network with $N = 100$ nodes and probability of link appearance Pr[ON] $= 10^{-3}$ for various intelligent attacks or random error strategies. As we observe, the temporal robustness is irrelevant to the choice of strategy. Furthermore, we obtain similar results for different values of the probability of link appearance Pr[ON] [Fig. 4(b)]. This behavior can be understood taking into account Lemmas 2 and 3.

The Markov temporal model shows similar features to the ones of the Erdős-Rényi. Although there are time correlations in the network evolution, all nodes exhibit the same properties. This leads to a unique curve for temporal robustness for all the attacking strategies.

2. *Mobility models*

Here we present the evaluation for the random waypoint model (RWP) and the random waypoint group model (RWPG) that were presented in Sec. III C.

With regards to the mobility models, in Fig. 5 the temporal robustness of the random waypoint mobility (RWP) under different attacks is plotted. The value of $\tau = 3600$ has been used for correct robustness evaluation. We observe that under different densities, random errors affect the network in the same manner [Fig. 5(d)]. However, the model is less robust in poor-connected cases (lower Pr[ON]), whereby intelligent attacks are applied.

Like the RWP model, the temporal robustness for the random waypoint group mobility model (RWPG) (Fig. 6) shows similar decreasing behavior for different probability of link appearance Pr[ON]. Unlike the RWP model, the temporal robustness decreases faster for the RWPG model.

In Fig. 7, for both the RWP and the RWPG mobility models we can see that for a fixed Pr[ON] the choice of

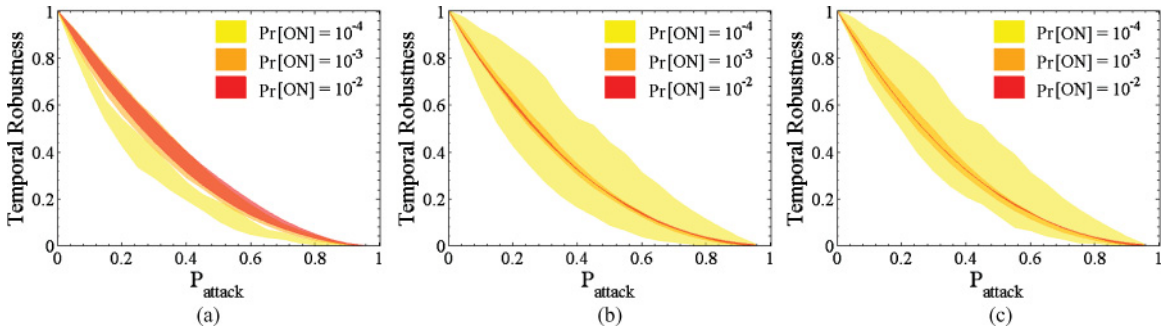

FIG. 8. (Color online) Robustness range of RWP models ($\tau = 3600$) for different attacking strategies: (a) temporal closeness, (b) average node degree, and (c) nodes number of contacts-updates as a function of removed (attacked) nodes percentage. As Pr[ON] decreases, the robustness range area becomes wider.

an intelligent attack strategy is irrelevant and all types of intelligent attacks are more effective than random errors, particularly for smaller Pr[ON]. In well-connected RWPG (Pr[ON] = 0.1), the temporal robustness values for intelligent attacks and random failures are leveled.

3. *Comparison*

The difference for temporal robustness by the choice of nodes can be evaluated by the robustness range. Figure 8 illustrates the robustness range for different attacking strategies in RWP models. This is the area demarcated by the lines or the temporal robustness curves when both the most and least important nodes are attacked. For smaller values of Pr[ON] we have larger robustness range area, which indicates that the choice of attacked nodes significantly influences the temporal robustness value. Contrarily, for well-connected networks (larger values of Pr[ON]), the robustness range area is small as there are multiple redundant paths that keep the network connected. In the RWPG model (Fig. 9), the choice of attacked nodes (e.g., group leaders) plays a crucial role and this is why the robustness range is larger than the one in the RWP models.

As we observed, Erdős-Rényi and Markov temporal networks do not contain predominant nodes. This is a corollary of Lemmas 2 and 3, as all the nodes are statistically identical; the expected degree and temporal closeness of a node are fixed values for all the nodes. This means that for each attacking strategy, the nodes are equally ranked and any choice of the attacked nodes affects the robustness in the same way. Therefore, the robustness range area is 0. The Markov temporal model differs from the Erdős-Rényi because we have transitional probabilities from link appearance to absence. However, the relative changes of temporal efficiency are the same, which results in the same value of temporal robustness. In Fig. 14 we show histograms about the average degree, the temporal closeness and the number of updates for the Markov temporal network, which once again confirm Lemmas 2 and 3.

For the mobility models, when the most important nodes are attacked, the resulting robustness is similar between different attacking strategies as the same nodes are ranked as most important. Additionally, sparse mobility models (with smaller Pr[ON]) are more affected as in these models some crucial temporal paths are more likely to be removed than in the dense models. The robustness range is wider for the RWPG than the RWP models because of the existence of "leaders,"whose removal influences the temporal robustness more than the other nodes.

IV. REAL TEMPORAL NETWORKS

A. Cabspotting traces

This case study uses the data from the Cabspotting system for collecting information [36] from taxi movements in the San Francisco area. All 488 participating taxis have been equipped

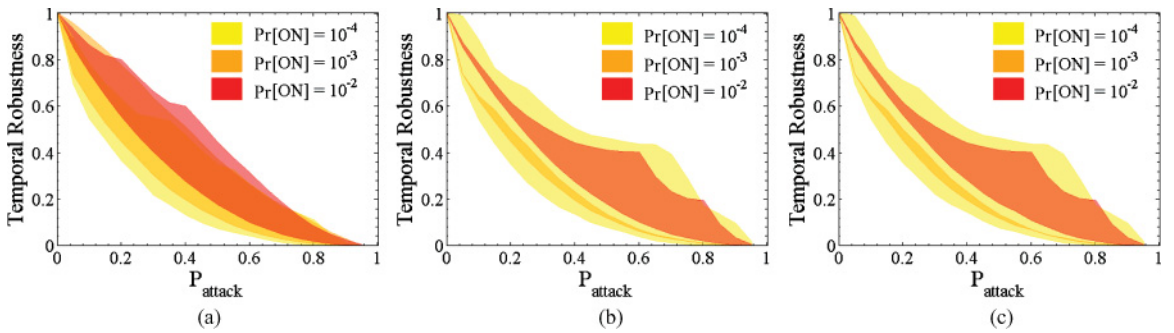

FIG. 9. (Color online) Robustness range of RWPG models ($\tau = 3600$) for different attacking strategies: (a) temporal closeness, (b) average node degree, and (c) nodes number of contacts-updates as a function of removed (attacked) nodes percentage. As Pr[ON] decreases the robustness range area becomes wider.

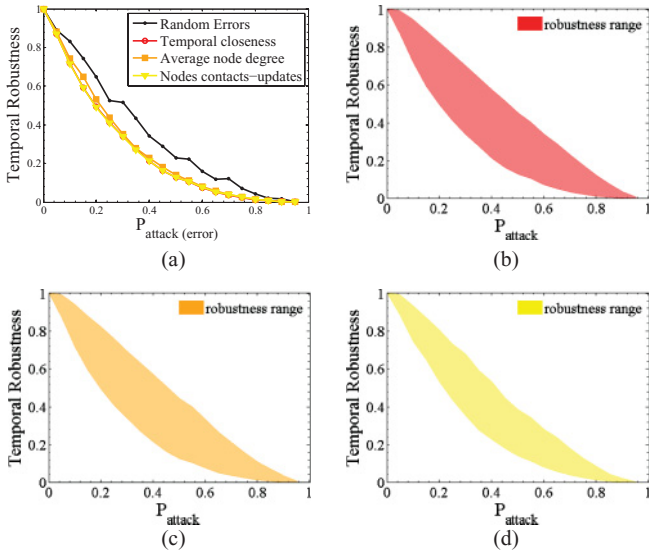

FIG. 10. (Color online) Temporal robustness and robustness range of INFOCOM temporal network ($\tau = 345600$) as functions of removed (attacked) nodes percentage. (a) The temporal robustness is similar for different attacking strategies. The robustness range for (b) temporal closeness, (c) average node degree, and (d) nodes number of contacts-updates strategies.

with GPS devices. The data contain information for a 24 h period on 21 May 2008 in an area 20 km × 20 km around San Francisco. The resulting temporal network has been derived by considering that a link exists when two taxis are within 200m of each other, which is a common distance for WiFi devices. The sampling time granularity is 1 s and the value of $\tau = 86400$ is used for a correct robustness evaluation.

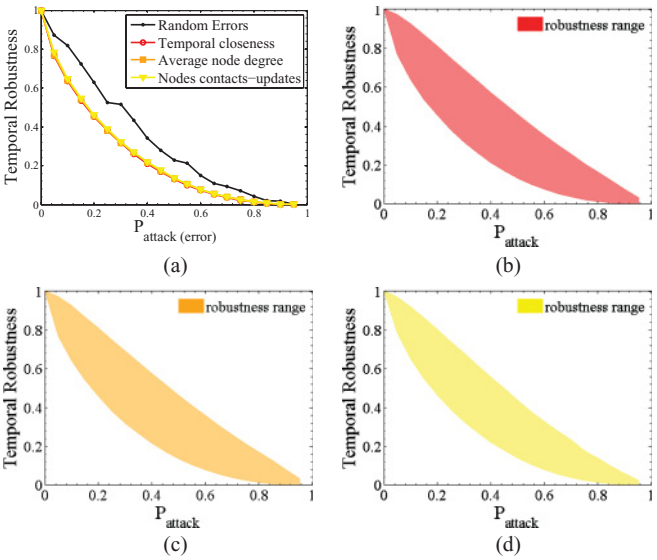

FIG. 11. (Color online) Temporal robustness and robustness range of Cabspotting temporal network ($\tau = 86400$) as functions of removed (attacked) nodes percentage. (a) The temporal robustness is similar for different attacking strategies. The robustness range for (b) temporal closeness, (c) average node degree, and (d) nodes number of contacts-updates strategies.

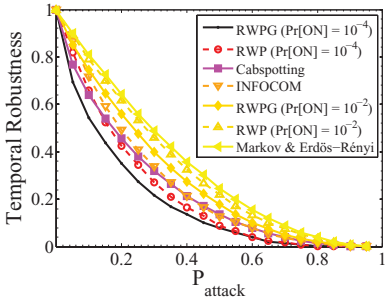

FIG. 12. (Color online) Temporal robustness of various temporal networks under unique attacking strategy (average node degree) as a function of attacked nodes percentage.

B. INFOCOM traces

The data were collected over four days at the IEEE INFOCOM 2006 conference in Barcelona. Participants in the experiment were 78 students and researchers, equipped with mobile communication devices (iMotes) [37] and an additional 20 stationary iMotes were deployed as location anchors. The wireless range of mobile iMotes is 30 m and that of stationary devices is about 100 m [37]. The value of $\tau = 345\,600$ has been used for correct robustness evaluation. In the temporal network, a link is constructed at a certain time, if the two nodes were within communication range. The intensity of the communication was different during the overnight periods and the peak periods (conference's sessions).

C. Results and discussion

Here, we present the results for the real networks. For random errors, the final results are obtained after averaging the simulations over 100 repetitions.

In Fig. 10(a), we observe that all intelligent attack strategies clearly outperform random errors due to the topology of the INFOCOM temporal network, while Figs. 10(b)–10(d) show the robustness range for each particular attacking strategy. Similar analysis (Fig. 11) is conducted on the Cabspotting data set for the temporal robustness and the robustness range. The aim of the simulations is to spot the difference when targeted nodes are attacked rather than randomly chosen nodes. In addition, the range of all possible values shows the significance of the important hubs and their contribution to the network performance.

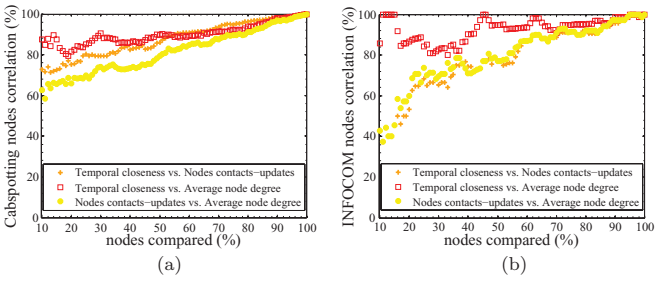

FIG. 13. (Color online) (a) Cabspotting network and (b) INFOCOM network. Correlation between targeted attacks. For instance, it indicates whether nodes that appear to be with high degrees have also high betweenness.

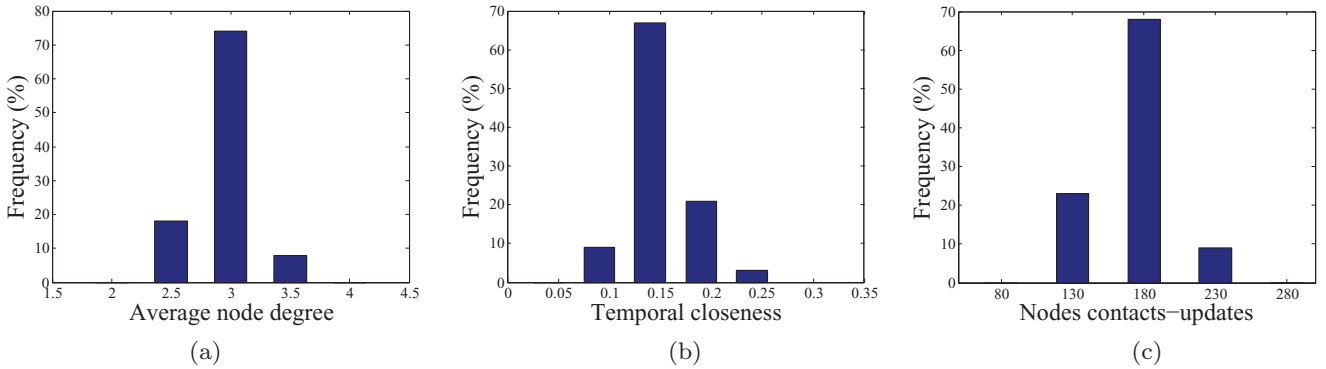

FIG. 14. (Color online) Histograms of Markov model nodal properties. The nodal properties are similar for all the centrality measures: (a) average node degree, (b) temporal closeness, and (c) nodes number of contacts-updates.

The comparison of the temporal robustness for different temporal networks under the average node degree attack strategy is given in Fig. 12. Temporal robustness curves for the real temporal networks and mobility models decrease faster than random models for a certain attacking strategy, because of the predominant nodes.

The analysis of the real-world data sets shows that intelligent attacks are significantly more effective than random errors, because of the presence of important nodes. Moreover, different attacking strategies equally affect the network. The main reason is that the same nodes are most important according to all three attacking strategies, which has been confirmed by our nodes correlation analysis. Figure 13 expresses the nodes correlation between different attacking strategies in temporal networks. The x axis presents the percentage of the nodes considered from the top of the lists of targeted attacks, while the y axis presents "the correlation" (percentage of overlapping nodes) for each pair of targeted attacks. It indicates whether the same nodes are highly ranked according to two attacking strategies. Particularly, it shows whether the same nodes that appear to be the highest connected are also important hubs on the shortest paths in the temporal network and contribute the most in the information spreading in a temporal network.

Figure 13 shows a general trend that targeted attacks are pairwise correlated, which means "important" (highly ranked) nodes for one are also important for other targeted attacks. For instance, the overlapping between the highest 25% ranked nodes is more than 70% for each pairwise combination of targeted attacks in both Cabspotting and INFOCOM temporal networks. Particularly, the correlation is the highest for the temporal closeness and the average degree for both real networks. In addition, the correlation is more expressed in large temporal networks (those with more nodes), which is shown by the comparison of the Cabspotting network [in Fig. 13(a)] and the INFOCOM temporal network [in Fig. 13(b)].

The temporal robustness also decreases faster in real networks than "balanced"models (Erdős-Rényi and Markovian) under all intelligent attacks. Moreover, as shown in Figs. 15 and 16, nodes in real networks significantly differ in temporal properties: the average degree, the temporal closeness, and the number of contacts-updates. In real networks, groups of nodes with similar values of temporal properties are less than 30% of all the nodes in all three strategies.

Furthermore, real temporal networks can be related with mobility models. More precisely, the robustness range of both INFOCOM and Cabspotting networks are similar to the RWP mobility model for small Pr[ON] values. This indicates a presence of predominant entities and important hubs. For the INFOCOM network, the reason relies on the fact that some of the conference participants were widely recognized, thus attracting more connections, while for the Cabspotting network some of the taxi cabs used to drive in central places and to wait for clients in specific locations. Although there are important entities in both real-world networks, no nodes cannot be characterized as "leaders" as in RWPG models.

Based on the results, in a centralized network system it is worth introducing an additional protection in "central nodes."Particularly, mobile networks are more sensitive on

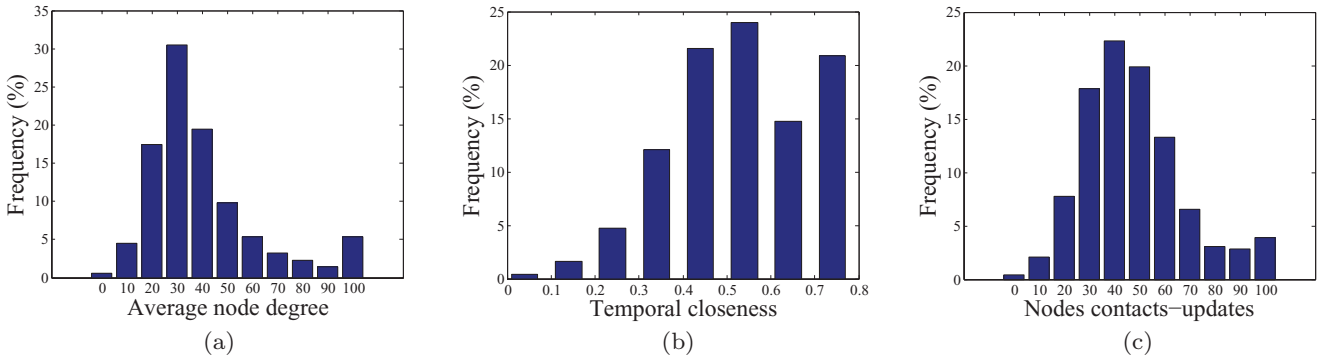

FIG. 15. (Color online) Histograms of Cabspotting nodal properties. The nodal properties are different for all the centrality measures: (a) average node degree, (b) temporal closeness, and (c) nodes number of contacts-updates.

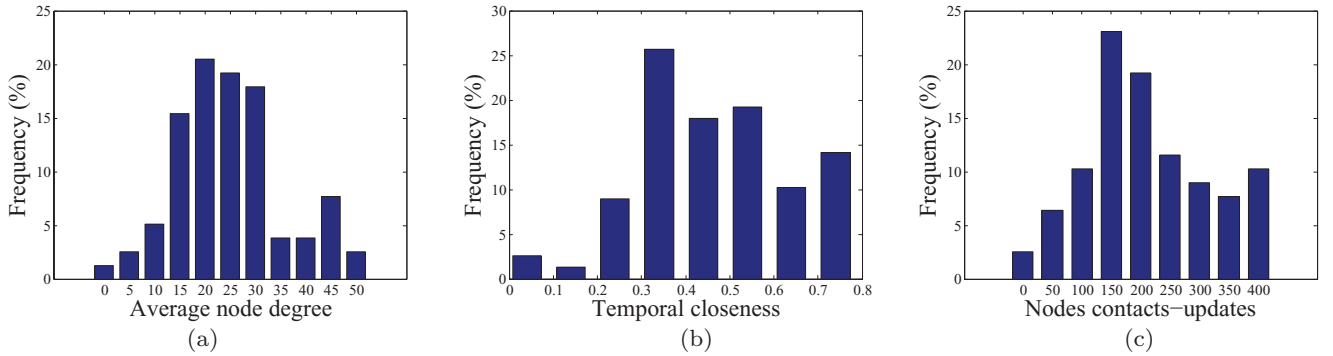

FIG. 16. (Color online) Histograms INFOCOM nodal properties. The nodal properties are different for all the centrality measures: (a) average node degree, (b) temporal closeness, and (c) nodes number of contacts-updates.

malicious attacks [38], which emphasize the requirement for better protection (e.g., multilevel instead of link-level encryption). However, decentralizing of the topology works better in networks, where an additional protection is expensive or causes deployment problems.

V. CONCLUSION

The paper investigates temporal network robustness for different time-varying networks under several attacking strategies and random errors. The main contributions of this paper can be summarized as follows: (i) using temporal robustness as a metric to quantify the ability of a time-varying network to function after an attack, we introduce a methodology in order to identify critical nodes that, when removed, can cripple the network's performance; (ii) we describe a method to quantify the impact of intelligent attacks: the temporal robustness range; based on this metric, we design various attack strategies and we show which one is the most disruptive for various real-world scenarios; and (iii) we thoroughly evaluate these attack strategies for various synthetic temporal models and for real-world temporal networks.

Our results show that, in homogeneous networks, intelligent attacks and random errors show similar performance, as all the nodes have similar temporal properties. These findings have been confirmed theoretically and by simulations as that nodes have similar values for the average degree, the temporal closeness, and the number of contacts-updates. However, in real-world networks, the impact of intelligent attacks is considerably higher, with about 50–75% reduced network performances compared to random errors. This significant difference demonstrates how by better protecting or disguising the important hubs in the network more robust network architectures can be achieved. Moreover, we show that there exists a high correlation between intelligent attacks, which expresses that highly connected nodes also trigger most of the changes in the optimal information spreading.

APPENDIX: PROOFS OF THE LEMMAS

Proof of Lemma 1. Assuming that m nodes have the message, a node will not receive it, if all the links between the node and the m nodes are in the state OFF. Therefore, the probability that a node will not receive the message is $(\Pr[\text{ON}]p + \Pr[\text{OFF}](1-q))^m = (\frac{p}{p+q})^m = (\Pr[\text{OFF}])^m$. Hence $p_m = 1 - \Pr[\text{OFF}]^m$.

Proof of Lemma 2. Let us consider possible states (ON or OFF) of all possible $(N-1)$ links of a fixed node and all the other nodes. A node a in a Markov temporal network has a degree k in a moment $(t+1)$, if for the links where a is an end-node hold: i links move from the state OFF in the moment t to the state ON in $(t+1)$; $(k-i)$ links preserve the state ON; exactly j links move from the state ON in the moment t to the state OFF in $(t+1)$ and exactly $(N-1-k-j)$ links preserve the state OFF for each $i \in \{0,1,\ldots,N-1\}$ and $j \in \{0,1,\ldots,N-1-k\}$. There are exactly

$$P(i,j,k,N) = \binom{N-1}{i}\binom{N-1-i}{j}\binom{N-1-i-j}{k-i} = \binom{N-1}{k}\binom{k}{i}\binom{N-1-k}{j}$$

possible combinations for i and j. Hence the degree distribution $\Pr[D=k]$ in the Markov temporal model is

$$\begin{aligned}\Pr[D=k] &= \sum_{i=0}^{k}\sum_{j=0}^{N-1-k} P(i,j,k,N)(q\Pr[\text{OFF}])^i((1-p)\Pr[\text{ON}])^{k-i}(p\Pr[\text{ON}])^j((1-q)\Pr[\text{OFF}])^{N-1-k-j} \\ &= \binom{N-1}{k}\sum_{i=0}^{k}\binom{k}{i}\left(\frac{pq}{p+q}\right)^i\left(\frac{q}{p+q}-\frac{pq}{p+q}\right)^{k-i}\end{aligned}$$

$$\times \sum_{j=0}^{N-1-k} \binom{N-1-k}{j} \left(\frac{pq}{p+q}\right)^{j} \left(\frac{p}{p+q} - \frac{pq}{p+q}\right)^{N-1-k-j}$$

$$= \binom{N-1}{k} \left(\frac{q}{p+q}\right)^{k} \left(\frac{p}{p+q}\right)^{N-1-k} = \binom{N-1}{k} \Pr[\text{ON}]^{k} \Pr[\text{OFF}]^{N-1-k}.$$

Therefore, the degree distribution in the Markov temporal model is binomial. For the binomial distribution $B(N,p)$, it is known [32–34] that the average degree is $(N-1)p$. Hence the average node degree in the Markov temporal model is $(N-1)\Pr[\text{ON}]$.

Proof of Lemma 3. Denoting by R_t the probability that a node has received the message after t steps and using the result in [8], for the random variable d_{ji} we have $\Pr[d_{ji} = t] = R_{t+1} - R_t$. Therefore,

$$E[C_i(t_1,t_2)] = \frac{1}{N-1} \sum_{j;j\neq i} d_{ji}(t_1,t_2) = \sum_{t=t_1}^{t_2} t \Pr[d_{ji} = t] = \sum_{t=t_1}^{t_2} t(R_{t+1} - R_t) = t_2 R_{t_2+1} - (t_1 - 1)R_{t_1} - \sum_{t=t_1}^{t_2} R_t.$$

Consequently, the temporal closeness does not depend on the choice i.

[1] S. Milgram, Psych. Today **2**, 60 (1967).

[2] J. Tang, M. Musolesi, C. Mascolo, and V. Latora, in *Proceedings of the 2nd ACM workshop on Online social networks*, WOSN '09 (ACM, New York, USA), pp. 31–36.

[3] J. Tang, S. Scellato, M. Musolesi, C. Mascolo, and V. Latora, Phys. Rev. E **81**, 055101 (2010).

[4] P. Holme, B. J. Kim, C. N. Yoon, and S. K. Han, Phys. Rev. E **65**, 056109 (2002).

[5] R. Albert, H. Jeong, and A.-L. Barabasi, Nature (London) **406**, 378 (2000).

[6] M. E. J. Newman and G. Ghoshal, Phys. Rev. Lett. **100**, 138701 (2008).

[7] V. Latora and M. Marchiori, Phys. Rev. E **71**, 015103 (2005).

[8] S. Scellato, I. Leontiadis, C. Mascolo, P. Basu, and M. Zafer, in *Proceedings of INFOCOM, 2011* (IEEE, Shanghai, China, 2011).

[9] P. Cholda, A. Mykkeltveit, B. Helvik, O. Wittner, and A. Jajszczyk, Commun. Surv. Tutorials, IEEE **9**, 32 (2007).

[10] C. M. Schneider, A. A. Moreira, J. S. Andrade, S. Havlin, and H. J. Herrmann, Proc. Natl. Acad. Sci. USA **108**, 3838 (2011).

[11] A. Satyanarayana and A. Prabhakar, IEEE Trans. Reliability **R-27**, 82 (1978).

[12] R. Wilkov, IEEE Trans. Commun. **20**, 660 (1972).

[13] S. Rai and K. K. Aggarwal, IEEE Trans. Reliability **R-27**, 206 (1978).

[14] D. S. Callaway, M. E. J. Newman, S. H. Strogatz, and D. J. Watts, Phys. Rev. Lett. **85**, 5468 (2000).

[15] R. Cohen, K. Erez, D. ben-Avraham, and S. Havlin, Phys. Rev. Lett. **85**, 4626 (2000).

[16] R. Cohen, K. Erez, D. ben-Avraham, and S. Havlin, Phys. Rev. Lett. **86**, 3682 (2001).

[17] M. Faloutsos, P. Faloutsos, and C. Faloutsos, in *Proceedings of SIGCOMM '99* (ACM, New York, 1999), pp. 251–262.

[18] R. Albert, I. Albert, and G. L. Nakarado, Phys. Rev. E **69**, 025103 (2004).

[19] L. D. F. Costa, F. A. Rodrigues, G. Travieso, and P. R. Villas Boas, Adv. Phys. **56**, 167 (2007).

[20] P. Crucitti, V. Latora, and S. Porta, Phys. Rev. E **73**, 036125 (2006).

[21] J. Nieminen, Scand. J. Psych. **15**, 322 (1974).

[22] S. Boccaletti, V. Latora, Y. Moreno, M. Chavez, and D. Hwang, Phys. Rep. **424**, 175 (2006).

[23] J. Scott, *Social Network Analysis: A Handbook* (SAGE Publications Ltd, London, UK, 2000).

[24] G. Sabidussi, Psychometrika **31**, 581 (1966).

[25] L. C. Freeman, Social Netw. **1**, 215 (1978/79).

[26] V. Latora and M. Marchiori, New J. Phys. **9**, 188 (2007).

[27] D. Kempe, J. Kleinberg, and A. Kumar, J. Comput. Syst. Sci. **64**, 820 (2002).

[28] P. Holme and J. Saramäki, Physics Reports (in press, 2012).

[29] A. Clauset and N. Eagle, in *DIMACS/DyDAn Workshop on Computational Methods for Dynamic Interaction Networks* (Rutgers University, NJ, USA, 2007).

[30] V. Kostakos, Physica A **388**, 1007 (2009).

[31] S. Wasserman and K. Faust, *Social Network Analysis: Methods and Applications* (Cambridge University Press, Cambridge, UK, 1994).

[32] P. Erdos and A. Renyi, Pub. Math. Inst. Hung. Acad. Sci. **5**, 17 (1960).

[33] E. Gilbert, Ann. Math. Stat. **30**, 1141 (1959).

[34] P. Van Mieghem, *Performance Analysis of Communications Networks and Systems* (Cambridge University Press, Cambridge, UK, 2006).

[35] A. Medina, G. Gursun, P. Basu, and I. Matta, in *Proceedings of the 2010 IEEE International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems*, MASCOTS '10 (IEEE Computer Society, Washington, DC, USA, 2010), pp. 444–446.

[36] M. Piorkowski, N. Sarafijanovic-Djukic, and M. Grossglauser, "CRAWDAD mobility cab", downloaded from crawdad.cs.dartmouth.edu/epfl/mobility/cab.

[37] J. Scott, R. Gass, J. Crowcroft, P. Hui, C. Diot, and A. Chaintreau, "CRAWDAD imote infocom", downloaded from crawdad.cs.dartmouth.edu/cambridge/haggle/imote/infocom 2006.

[38] S. Corson and J. Macker, "Mobile ad hoc networking (manet): Routing protocol performance issues and evaluation considerations", available on ietf.org/rfc/rfc2501.txt (1999), ietf note.