Rumor Spreading in Social Networks with Individual Privacy Policies

(Article begins on next page)

Rumor Spreading in Social Networks with Individual Privacy Policies

*Bioglio L.[1], Pensa R. G.[1]

[1]University of Turin, Turin, Italy

Humans are social animals that love to disseminate ideas and news, as proved by the huge success of social networking websites such as Facebook or Twitter. On the other hand, these platforms have emphasized the dark side of information spreading, that is the diffusion of private facts and rumors in the society. The users of these social networks can usually set a level of privacy, and specify which of their contacts are allowed to see their notifications, but they do not have any control on how these contacts will use the information: friends could spread the rumor through other social networks, blogs, websites, medias or simply with face-to-face communication.

The behavior of an individual in these situations highly depends on his level of privacy awareness: an aware user tends to not share on social network his private information, or the private information of their friends, while an unaware user could not recognize an information as private, and could share it without care to his contacts, even to untrusted ones, putting at risk his privacy or the privacy of his friends.

The classic Susceptible-Infectious-Recovered (SIR) epidemic model can be adopted for modeling the spread of information in a social network: susceptible individuals do not know the information, then are susceptible to be informed; infectious individuals know and spread the information, while recovered individuals already know the information but do not spread it anymore. A susceptible individual in contact with an infectious one can become infectious with a transmission probability, while an infectious individual naturally recovers from infection with a recovery rate, turning into a recovered individual.

Here we extend this compartmental model in order to represent several kinds of privacy policies, from unsafer to more rigorous: each individual belongs to a class that models the privacy behavior by tuning the transmission probability, the recovery rate and the susceptibility to information, that specifies the interest of the individual on the information.
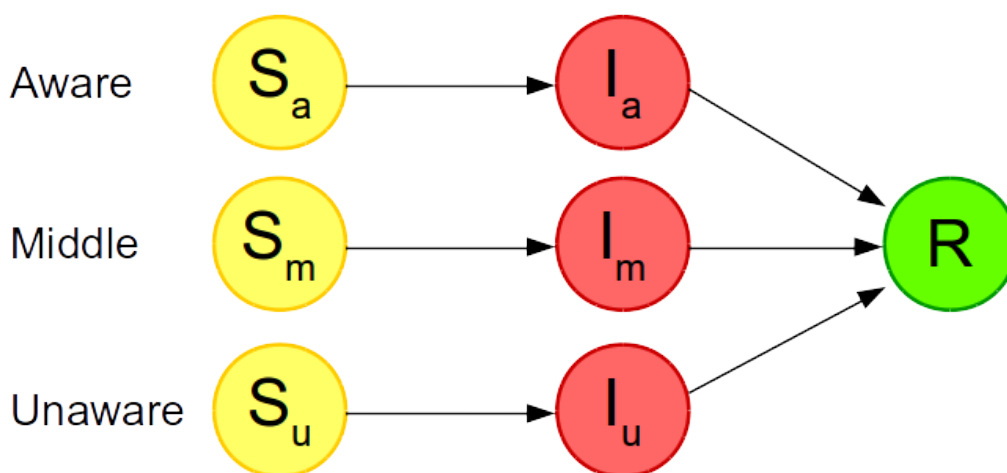
We calculate a privacy score for each individual based on the privacy policies of his contacts, so as to infer the local robustness to the spread of personal information.

We test our model by means of stochastic simulations on synthetic contact networks and on a small partition of the Facebook social network, provided by few hundreds of volunteers that replied to an online survey.