Effects of Social Network Structure on Epidemic Disease Spread Dynamics with Application to Adhoc Networks

Nadra Guizani, Ali Elghariani, Jason Kobes, and Arif Ghafoor

Abstract

With the frequent appearance and spread of infectious diseases and their impact on major population areas, there is a growing interest to develop models for analyzing the dynamic behavior of epidemics. Such analysis can provide a better decision making process to combat and confine disease. In this article, we briefly survey the literature on network structure effect on disease spread models. Subsequently, we discuss an SEIR based epidemic model for different levels of aggregation of population. This model is subsequently applied to analyze virus propagation phenomena in mobile ad hoc networks. For managing this type of threat, we propose two security architectures for these networks based on several design criteria including scalability, power, and computation limitations.

Introduction

Public health care individuals are generally faced with the challenge of finding effective ways to combat epidemics. Deployment of effective and timely countermeasures is crucial for saving lives. A key factor in controlling epidemics is to understand the spatio-temporal dynamic and population demographics associated with the epidemic. For pre-planning exercises, disease spread models can be developed and analyzed. Generally these models capture human-to-human interactions among the population as such interactions generally serve as a media of disease transmission. Interactions among the population can be modeled in terms of social networks. These models can be developed at different levels of population granularity ranging from an individual up to an aggregated form representing the total population. The existing disease spread models such as Susceptible-Infected-Recovered (SIR) or Susceptible-Exposed-Infected-Recovered (SEIR)[1] are incorporated with the social network model to analyze the dynamics of the epidemic under various context.

Likewise, epidemic models can be applied to analyze the dynamics of virus propagation in mobile networks. In a mobile network, each device can be represented as an agent that communicates with other devices using underlying communication technologies such as WiFi, Bluetooth, and cellular services. The main countermeasure to combat mobile viruses is by deploying software updates. However, for large mobile networks, broadcasting global updates is not viable; rather, the updates can be sent to specific groups or regions.

Epidemic models can be used to predict the spread of viruses and efficiently deliver updates to affected groups. In this article we review the commonly used disease spread models and the effect of network topology on epidemics. In addition, we provide the assessment of efficacy of an SEIR model at different levels of granularity both for epidemics as well as for the spread of viruses in Mobile Ad-hoc Networks (MANETs). MANETs can also be observed at different levels of population granularity as discussed below.

Disease spread models are simulated to depict the effect of epidemics according to various epidemiological rules of disease spread. As shown in Fig. 1, an SEIR model is represented as a four stage finite state model (FSM) for individuals, represented as agents in a general population. In susceptible state (*S*) an agent is prone to get infected at any point in time. The transmission rate (β) from state *S* to exposed state *E* is calculated based on the number of contacts an agent has with agents that are already in states *E* and *I*. In state *E*, an individual does not show any symptoms of the disease but can infect others. Subsequently, the agent migrates to state *I* which is the infection state and is marked by the appearance of symptoms. After spending some indeterministic time in state *I*, the agent recovers and moves to recovered state *R*.

The SIR or SEIR model can be further classified into probabilistic and deterministic spread models. In a deterministic model, each agent spends a fixed amount of time in each state, which is a weak assumption. Probabilistic models have been developed to more accurately capture the indeterministic aspects of an epidemic. In these models the residency time (ϕ) of each state follows a known probability distribution. The main objective of both deterministic and probabilistic [1] SEIR models is to analyze various decision making options based on the behavior of the disease that encapsulates numerous factors such as maximum infected population, peak time of the disease, and final percentage of population infected. The most important factor in SEIR based analysis is the interconnectivity among agents. This factor provides a deeper understanding on how different social network structures affect the dynamics of an epidemic.

Digital Object Identifier:
10.1109/MNET.2019.1800026

The authors are with Purdue University.

0890-8044/19/$25.00 © 2019 IEEE

Modeling of social networks can be derived in multiple ways. This article first discusses the key attributes for modeling a social network with respect to epidemic spread including population demographics and human activities. The following section reviews the related work and investigates the disease spread when applied to an aggregated population model. Following that, we discuss the effect of network structure using the SEIR model and present some results for the aggregated population model. Then we illustrate how the spread of virus in a MANET can be analyzed using the SEIR epidemic model. The final section presents conclusions.

Related Work

Opuszko and Ruhland [2] have investigated the effect of seeding strategy and characteristics of a network structure for analyzing and predicting viral marketing problems using the SIR model. Fourteen different network characteristics are defined. These characteristics are analyzed to identify the one that has the most impact on the spread. The authors concluded that network size does not have significant impact on the spread of disease. Characteristics such as average node degree and number of network edges have a larger effect on the direction and speed of disease spread.

Xu and Xu [3] studied SIR modeling and control of infectious disease transmission on community structured networks. The community of network structure refers to a set of relatively independent nodes that are tightly connected similar to real world social population structure. Using a predefined connection threshold in terms of time and proximity, network connections among nodes are defined as strong or weak. An important conclusion presented in [3] is that the stronger the community structure is, the lesser the number of infected people. Another factor that effects disease spread is initial location of infection. If the initial infection is within one cluster of the population, the disease has a higher probability of being contained within that cluster.

In the following sections, we discuss different models that are used in the literature.

Agent Based (AB) Model

The agent based (AB) models have been applied to many different fields, such as traffic analysis, social networking, and economic studies, just to name a few [4, 5]. This model allows the visual rendering of an elaborated behavior of virus spread in a given network. An AB model is a microscopic simulation model that focuses on detailed behavior and unique features of individuals. Being computationally intensive is a major shortfall of this model as it entails a graphical analysis. Due to high computational cost, low granularity models are presented as an alternative.

The AB model can be used to simulate the SEIR disease spread model as seen in Fig. 1. Specific rules are assigned to each agent controlling its transition from state to state. In this article we apply SEIR to a population in which each agent performs three activities on a daily basis: home, work, and transportation. Based on these activities the population is represented as a graph where nodes represent agents and edges represent activities. An edge between two nodes represents agents who are involved in the same activity during an overlapping time period [6].

Contact rate	c_{ES}	c_{IS}
Home	4	1.5
Work	5	1.0
Transportation	3	2.0
Infection rate	i_{ES}	i_{IS}
All activities	.05	.06
Heterogeneity factor	δ	
Home	U[0.25–1.00]	
Work	U[0.05–0.25]	
Transportation	U[1.00–1.50]	

TABLE 1. SEIR disease spread parameters.

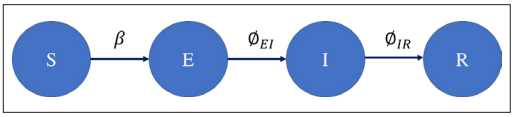

FIGURE 1. SEIR finite state model.

The parameters used in this model are shown in Table 1. Contact rate is the probability that an agent comes in contact with another agent. The contact rate is based on the activity and the state each agent is in. A susceptible agent can be infected if it comes in contact with both exposed and infected agents. c_{ES} is the contact rate between an exposed and susceptible agent while c_{IS} is the contact rate between an infected and susceptible agent. The same subscripts are also used for the infection rate. The infection rate is the probability that an agent gets infected based on the activity and disease state of the other agents. The heterogeneity factor quantifies the "strength" of the edge connecting two agents and is an indication of how likely the chances are to get infected. For each activity, the heterogeneity factor is determined based on a specific uniform distribution. It can be noted from Table 1 that the home activity has a lower heterogeneity factor than transportation. This is due to close proximity of agents in transportation requiring a higher heterogeneity factor. The infection rate, contact rate, and heterogeneity factor together determine the infection rate as given by Eq. 2.

Spatial Based (SB) Model

The spatial based (SB) model can be viewed as an aggregated version of the AB model. This model divides the population spatially in a grid-like structure. The work of Maciejewski *et al.* creates the SB model to analyze the effect of decision measures when implemented for different infectious disease scenarios [7]. The SB model is unique because it takes into account the distance factor between spatial grids in order to analyze the spread of disease in terms of speed and direction. Since the SB model is developed by aggregating the AB model, its contact rates are computed in terms of grouping some of the parameters of the AB model such as age [7].

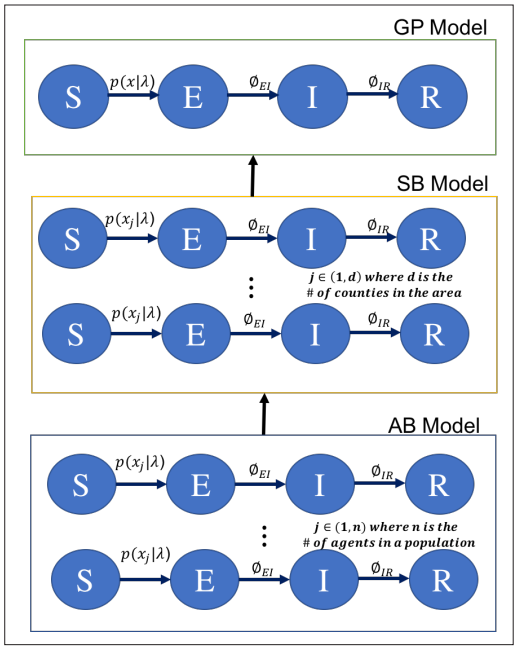

FIGURE 2. SEIR-FSM applied at different levels of aggregated population models.

Global Population (GP) Model

The global population (GP) model is a macroscopic simulation model that represents coarse grain epidemic dynamics of the whole population. The GP model is a generalized version of the AB model providing a more efficient prediction strategy. The infection and contact rates of this model are computed based on the rates provided in the AB model [8]. Note, the GP model does not take into account any attributes or network structure among the agents.

Eulers' method can be used to estimate both transmission rate (b) and contact rate (k) for the GP model through the SIR equations listed below [9]:

$$\begin{aligned} s_n &= s_{n-1} - bs_{n-1}\,(i_{n-1} + e_{n-1})\Delta t \\ i_n &= i_{n-1} + (be_{n-1} - ki_{n-1})\Delta t \\ r_n &= r_{n-1} + ki_{n-1}\Delta t \end{aligned} \quad (1)$$

where s_n the number of susceptible agents at time n, e_{n-1} is the number of exposed agents at time $n-1$, i_n is the number infected agents at time n, and Δt is the time transition from $n-1$ to n.

The AB, SB, and GP models can be presented as an SEIR-based FSM, as shown in Fig. 2. At the AB level, each agent has a corresponding SEIR-FSM as seen in Fig. 1. At the SB level the number of SEIR-FSMs decreases dependent on the aggregation criteria. Accordingly, the GP level is a single SEIR-FSM representing the global population spread over different states according to Eq. 1.

Effect of Network Topology on the Dynamics of Epidemic

Rahmandad and Sterman [8] explored the effect of the AB and GP models on five different types of network structures/topologies: small world, scale-free, random, connected, and lattice. The difference in outputs generated by the GP and AB models is measured by confidence interval percentage, peak population infection, and burn out rate of disease. For all the networks simulated, the experiments generate the classic diffusion model for epidemic spread. This is when the spread of disease initially increases at a high rate and then gradually declines as time passes.

Networks with clusters exhibit different epidemic spread dynamics. Low clustered networks have an equal chance of contacting neighbors versus distance nodes. High clustered networks contain hubs of connected nodes with sparse connections among hubs. Low clustered networks such as random and fully connected networks result in a faster initial disease growth and early disease burn out. High clustered networks such as scale free and lattice networks exhibit slower disease spread after initial neighbors are infected since the chance of contacting a susceptible agent declines. Table 2 shows that the peak prevalence (I_{max}) of lattice and scale free is lower than the fully-connected and random graphs. Clustering makes it highly unlikely to generate new cases of infected agents. Therefore, for high clustered networks, the die out rate of the epidemic is slightly slower than that of a fully connected or random network, as can be seen from Table 2. All metrics measured remain within the 75 to 95 percent confidence interval when compared to the AB simulation.

It is concluded that there are a few differences between GP and AB model simulation of these five network structures. The major contributor of the difference in metrics is the high or low clustering in networks.

Developed SEIR AB Model

SEIR-FSM for activity driven AB model is developed using a Gaussian mixture model. The transmission probability equation of an individual agent, $p(x \mid \mu_i, \Sigma_i) = \Sigma_{i=1}^{M} \omega_i g(x \mid \mu_i, \Sigma_i)$, is used to create the path from state S to state E. Here M is the number of activities within one process and x is a D-dimensional data vector that contains the agent's demographic and activity features. In our case there are three activities: home, transportation, and work. In the AB model, weights (w_i) for each activity is specific to the contact rates seen in Table 2. μ_i is the transmission rate β of the disease. β is calculated using the following Eq. 2 [8]:

$$\beta = \delta_j[i_{ES}E + i_{IS}I] \quad (2)$$

In the proposed unified SEIR, β accounts for the heterogeneity factor (δ_i) based on the different activities of the social network. Here E is the average number of exposed agents and I is the average number of infected agents. β for the GP model contains one uniform distribution for the heterogeneity factor among the entire population.

The transmission probability of an agent is computed at specific intervals of time. A threshold probability is assigned depending on the type of disease being analyzed. The transmission probability is recomputed every time an agent changes its activity.

Experimentation and Results for a Synthesized Population

We analyzed synthesized population activity based data for both the AB and GP models. The data set chosen is described in [7]. The data set includes 322,000 agents in a small world network

spanning three activities (home, work, transport) for each agent with corresponding demographic data. The simulation is performed in four different segments of time for an interval from 8:00 am to 11:59 pm, representing the four activities: home, transport, work, and transport. For the AB model each agent transitions from one state to the next using the disease equations discussed in the previous section. The parameters for the rate equation are specified in Table 1. Several experiments were conducted to assess the efficacy of Eulers' method for the GP model.

Figures 3a and 3b correspond to Scenario 1 where I_0 = 600 and estimated disease parameters b and k are 1.24 and 0.24, respectively. Note, the GP model closely follows the trend of the AB model for the individuals in both state S and state I.

Scenario 2 is illustrated in Figs. 3c and 3d corresponding to an I_0 = 153 and estimated parameters b = 0.848 and k = 0.099. This scenario has a smaller initial infected population. The initial infection for Scenario 2 was selected from a less dense area than Scenario 1. Accordingly, Scenario 1 has an early peak time of 10 days, whereas Scenario 2 has a peak time at 13 days. Due to the selection of this initial infection the estimated transmission rates b and k for Scenario 2 for the GP model are slightly smaller. These results conclude that both the size and the location of the initial infection play an important role in terms of the dynamics of disease spread.

Virus Spread in Mobile Ad-hoc Networks

A Mobile Ad-hoc Network (MANET) is a collection of mobile nodes that are connected to each other through wireless links. Any two nodes within the network can communicate directly if they are within a certain range. Nodes that are not in the same range can communicate indirectly through intermediary nodes, as shown in Fig. 4a. Generally mobile nodes in a MANET do not have any centralized controller, such as base stations or mobile switching centers. In addition, there are no restrictions on the nodes to join or leave the network. Therefore, the MANET topology dynamically changes. Note, the underlying communication media can be based on different technologies such as Bluetooth and WiFi. These characteristics of MANET devices make it possible to effectively apply the epidemic spread model discussed in the previous sections to analyze the issue of information dissemination or virus spread in a MANET. Moreover, the nodes in a MANET can be frequently and temporarily disconnected

	AB		GP		Confidence interval (%)
	Peak time, T_p (days)	Peak prevalence, I_{max} (%)	Peak time, T_p (days)	Peak prevalence, I_{max} (%)	
Fully connected	44.9	27.1	49.6	26.7	95
Random	49.5	25.1	58	24.2	95
Scale-free	43.6	23.9	47	21.4	98
Small world	83.6	16.5	83.2	14.9	95
Ring lattice	75.2	8.5	90.5	7.8	95

TABLE 2. The die out (T_p) and peak population infection (I_{max}) for five network topologies [8].

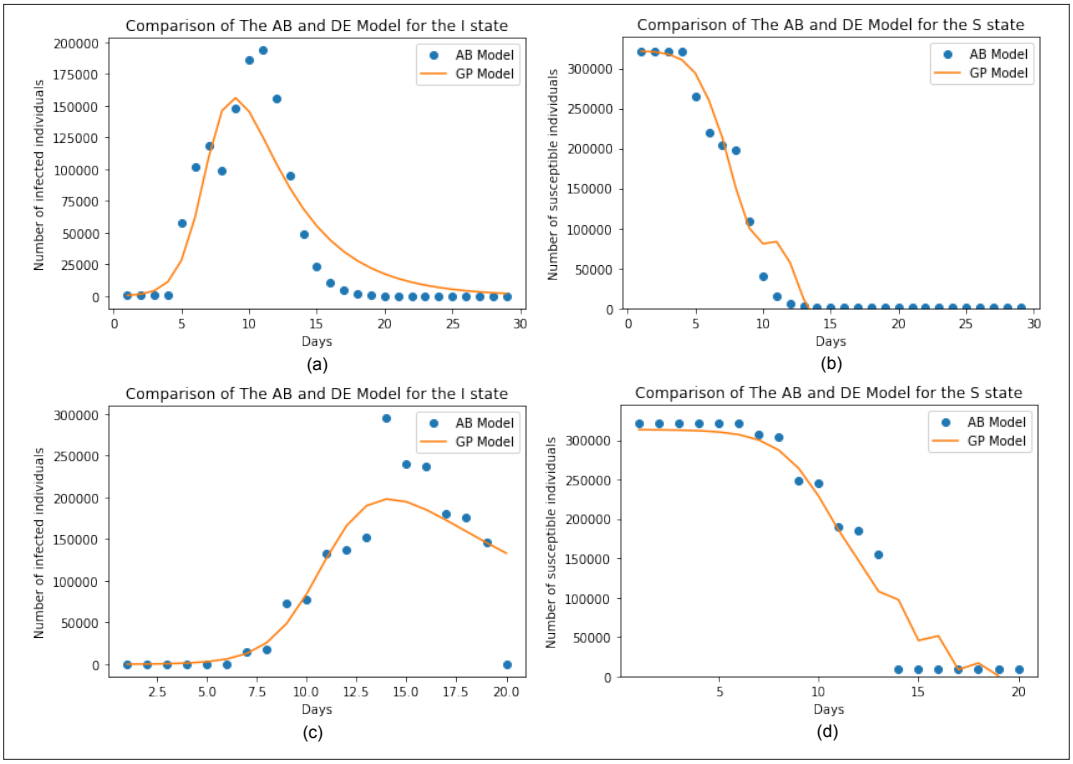

FIGURE 3. Experimental Results of Proposed SEIR Model: a) Number of Individuals in state I in Scenario 1(GP Model vs AB Model); b) Number of Individuals in state S in Scenario 1(GP Model vs AB Model); c) Number of Individuals in state I in Scenario 2(GP Model vs AB Model); d) Number of Individuals in state S in Scenario 2(GP Model vs AB Model).

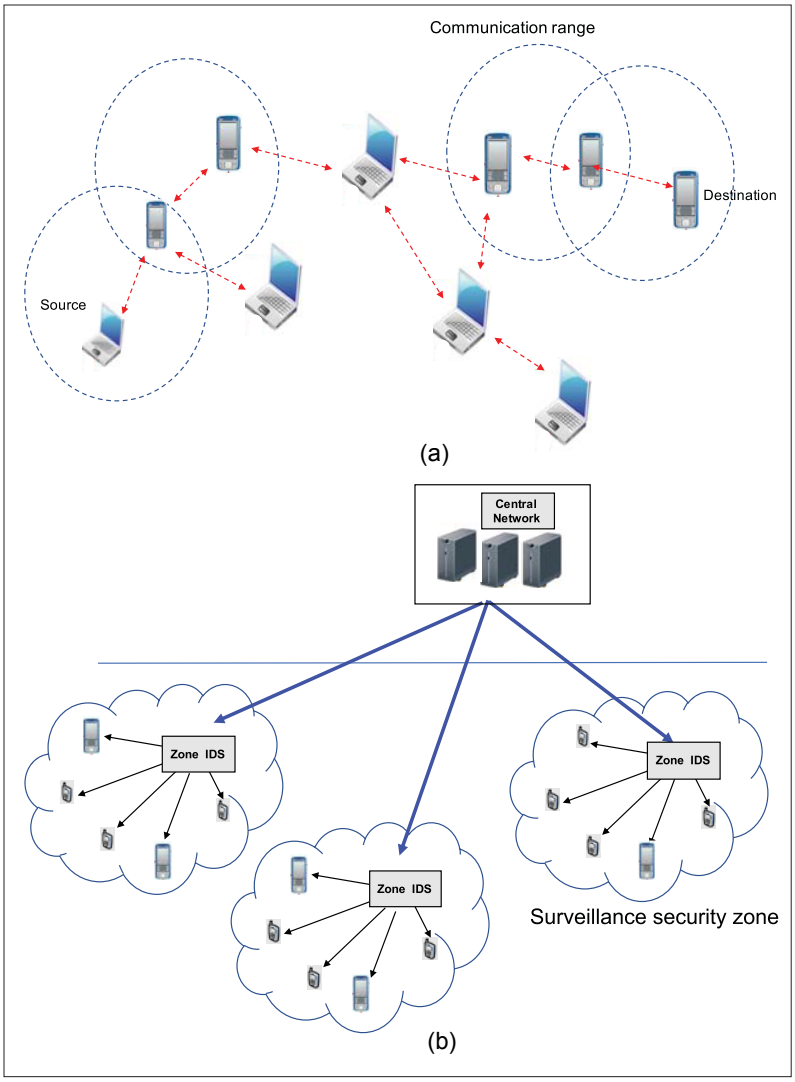

FIGURE 4. a) Example of MANET network; b) Semi-distributed hierarchical Security Structure based on IDS surveillance zone deployment in MANET.

changing the number of neighboring devices. This in turn changes the contact rate among MANET devices. Note, the larger the number of neighboring devices, the higher the contact rate and the higher the possibility of spreading the virus. Musolesi and Mascolo [10] presented a middleware that implements epidemic information dissemination techniques for ad hoc networks. They have proposed a primitive middleware for unicast and anycast communication and have used the epidemic model to measure the reliability of these two communication paradigms. They implemented an SIR model where an individual (host) is infected if it carries a virus message and susceptible if it does not. In this case, the initial number of virus messages is set to 1 ($I_0 = 1$), for which the infection rate (β) and removal rate (γ) are computed. β is computed through corresponding contact and infection rates. γ represents the time it takes for an update message to reach the infected device. In particular, the infection rate between devices can be predicted at three granularity levels as shown in Fig. 2.

The experimental results illustrated above can be extended to analyze the phenomena of such spread for a MANET. For the AB model each mobile device can be seen as an agent and the connections among agents can be monitored to detect any virus message. For this model we characterize agent based information including the location and time of infection, which is equivalent to the human demographic information presented above. For this information we utilize a Traffic Flow Table (TFT) and a Traffic Information Table (TIT) maintained by each mobile device. These tables are used for two purposes. First, they provide connectivity information among nodes. Second, a TFT can be used to identify infected agents through characteristics such as packet drop, buffer overflow, bandwidth consumption, and so on.

The SB aggregation method can be used to model and predict virus attacks and to create effective mechanisms to disseminate updates needed to halt the spread of the attacks. Mobile network connections are created through distance metrics. A mobile node sends a virus message within an RF range and the message is received by a neighboring node with a certain probability (p) as mentioned previously. In other words p represents the probability with which a mobile device can be exploited depending on the RF range.

The GP model estimates the total number of mobile agents that are infected versus the number that remain susceptible at a global level. As previously stated, the GP model does not provide any specific information about when and where the agents are infected. It provides an estimate of the number of devices that are attacked given some initial number of attacking/infected devices. Based on the AB, SB, and GP models, a structured security mechanism for MANET devices is presented below.

Disease Spread Rules in Ad-hoc Mobile Networks

In order to apply the epidemic model to a MANET we utilize the concept of a Common Vulnerability Scoring System (CVSS). A CVSS provides an open framework to characterize device vulnerabilities in terms of different virus attacks. CVSS has three metric groups that determine the base score in terms of the degree of vulnerability [11]. The virus spread rules between the SEIR states are defined in terms of the basic CVSS metrics. In state S a device is vulnerable to receive a virus message. A device in state E carries the virus message that can be transmitted to other devices while the device itself is not effected. In state I a device is infected by the virus message. A device in state R implies that the device is recovered after receiving a "clear virus" update message. CVSS metrics are used to compute the contact rate, infection rate, and heterogeneity factor for a MANET and in turn the probability of infection for a device to transition from state S to E. Basic CVSS metrics are: the access distance (access vector), number of times contacted (authenticity), and strength of connectivity (access complexity) at which a mobile agent can be reached. The contact rate is generally a function of the access vector and authenticity metrics, that is:

Contact rate = f(access vector, authenticity).

A high level of authenticity denotes that an agent while trying to connect to another agent needs to go through several steps of authentica-

tion. Access complexity corresponds to the heterogeneity factor (δ) of the MANET device which represents the number of devices that can make contact with any given mobile device. Accordingly, the probability of a mobile getting exploited for vulnerability, which corresponds to the transition from state *S* to *E*, can be calculated as [12]:

$$CVSS_E = \frac{1}{10} * 20 * AV * AC * Au \quad (3)$$

where *AV* is the access vector, *AC* is the access complexity, and *Au* is the authentication level.

Using the above equation and its parameters, the impact of various attack scenarios can be analyzed for a MANET. For example, for a virus spread attack scenario in a MANET akin to Scenario 1 discussed above, the average transmission rate $b = CVSS_E * 10 = 1.23$ based on the values of $AU = 0.45$, $AV = 0.395$ and $AC = 0.35$, which are taken from the CVSS database [12]. Referring to Fig. 3a, the 322,000 agents can be viewed as mobile devices in a MANET which exploit vulnerabilities to attack and "infect" each other at rate *b*. In this case, the peak number of infected mobile devices can be estimated in day 10 based on the AB model and on day 8 based on the GP model. Accordingly, one can deploy a patching mechanism using the recovery rate (*k*) by sending a "clear update" message to infected devices in a timely manner. This timely response can avoid the patch/virus race condition [13].

Intrusion Detection System Architecture for MANETs

Fixed or mobile networks play an increasingly vital role in modern day society; however, the security of these networks is always at risk. Therefore, there is a dire need to develop security assurance technology to protect these systems. An Intrusion Detection System (IDS) is one such technology with the aim to detect security threats and attacks in the network. For this purpose, an IDS monitors network traffic and generates relevant alerts when malware and traffic anomalies are detected [14].

The deployment of an IDS is an important design aspect in computer networks, and more challenging for a MANET because such a network has a dynamically changing topology with no centralized management [15]. Based on the unique characteristics of MANETs, one strategy to control the spread of virus is to deploy an IDS at each device which is akin to the AB model. In this case, the IDS is part of the mobile device software to detect active intrusion attempts. This software can in turn communicate with a centralized threat management system so that "clear virus" updates can be broadcasted to the infected devices. Note, such an AB IDS deployment strategy could be costly in terms of energy and memory constraints. In addition, using the AB IDS approach does not scale well for the centralized threat management system and cannot provide effective response to prevent such a spread.

In this section we propose two types of security architectures for monitoring and generating updates for virus spread attacks in a large scale MANET. We use the concept of multiple aggregated levels similar to the concept of the SEIR model introduced earlier to develop a hierarchical security structure as shown in Fig. 4b which can have two different architectural designs: fully distributed versus semi-distributed. In a fully distributed architecture, the IDS is deployed at the AB level that communicates alerts to a surveillance zone (SZ) monitor that collects these alerts and in turn reports to a centralized global security monitor. Alternatively, in a semi-distributed architecture, the IDS is deployed at the SZ level rather than at the AB level. In this case an SZ IDS monitors traffic and collects TFT and TIT information to detect infected devices. Consequently, this architecture does not suffer from the power and processing limitations discussed at the AB level.

Fixed or mobile networks play an increasingly vital role in modern day society; however, the security of these networks is always at risk. Therefore, there is a dire need to develop security assurance technology to protect these systems.

For both architectures, SZs are identified based on the physical limitations of the RF transmission range among ad hoc devices, and the density of these devices in a certain area at a given time. Taking into account both network density and RF range, this architecture can provide a scalable solution for monitoring vulnerability and processing network traffic within each zone. Note, these zones can be separated or overlapped. For both architectures, SZs report to a centralized manager that is responsible for communicating "clear virus" updates to all other SZs. This message is then distributed to devices in affected SZs.

The centralized security network system represents the aggregation at the GP level, in the sense it aggregates intrusion information from all IDSs. This system is ultimately in charge of generating and disseminating any global counter measure, such as a "clear virus" update message to all or specific SZs that have been "infected." Graphs similar to those shown in Fig. 3a can be applied to MANET networks to identify threshold levels at which decisions related to a "clear virus" update is communicated by the semi-distributed security architecture.

Conclusion

In this article, we discussed an SEIR based epidemic spread model for different levels of aggregation of population. Our objective was to analyze the dynamics of this model and the impact of the network topology on the behavior of the spread. SEIR model and its multilevel aggregation representation have been applied to ad hoc mobile networks (MANETs) to understand the dynamics associated with the virus spread in these networks. We have presented two security architectures for monitoring and responding to viruses for MANETs.

Acknowledgment

This research was supported by grants from Northrop Grumman Corporation (approved for public release, case #19-0397), and the U.S. National Science Foundation (NSF) Grant IIS-0964639.

References

[1] C. L. Barrett *et al.*, "EpiSimdemics: An Efficient Algorithm for Simulating the Spread of Infectious Disease over Large Realistic Social Networks," SC2008, Austin, Texas, USA, Nov. 2008.

[2] M. Opuszko and J. Ruhland, "Impact of the Network Structure on the SIR Model Spreading Phenomena in Online Networks," ICCGI 2013, pp. 22–28.
[3] D. Xu and X. Xu, "Modeling and Control of Dynamic Network SIR Based on Community Structure," *Proc. 26th CCDC*, 2014, pp. 4648–53.
[4] L. Perez and S. Dragicevic, "An Agent-Based Approach for Modeling Dynamics of Contagious Disease Spread," *Int'l. J. Health Graphics*, vol. 8, no. 50, 2009, pp. 1–17.
[5] E. Teweldemedhin, T. Marwalla, and C. Mueller, "Agent-Based Modelling: A Case Study in HIV Epidemic," *Proc. Fourth Int'l. Conf. Hybrid Intelligent Systems*, Washington, DC, USA, 5–8 Dec. 2004, pp. 154–59.
[6] M. Sahar *et al.*, *A Framework for Synthesizing Agent-Based Heterogeneous Population Model for Epidemic Simulation*, Purdue University, ProQuest Dissertations Publishing, 2014.
[7] R. Maciejewski *et al.*, "A Pandemic Influenza Modeling and Visualization Tool," *J. Visual Languages and Computing*, vol. 22, no. 4, 2011, pp. 268–78.
[8] H. Rahmandad and J. Sterman, "Heterogeneity and Network Structure in the Dynamics of Diffusion: Comparing Agent-Based and Differential Equation Models," *Management Science*, vol. 54, no. 5, May 2008, pp. 998–1014.
[9] D. Smith and L. Moore, "The SIR Model for Spread of Disease — Euler's Method for Systems," https://www.maa. org/press/periodicals/loci/joma, Mathematical Association of America (MAA),December 2004.
[10] M. Musolesi and C. Mascolo, "Controlled Epidemic-Style Dissemination Middleware for Mobile Ad Hoc Networks," *IEEE Mobile and Ubiquitous Systems*, San Jose, CA, 17–21 July 2006, pp. 1–9.
[11] P. Mell *et al.*, "A Complete Guide to the Common Vulnerability Scoring System (CVSS) Version 2.0, Forum of Incident Response and Security Teams," http://www.first.org/cvss/cvss-guide.html, June 2007.
[12] National Vulnerability Database, https://nvd.nist. gov/vuln-metrics/cvss/v2-calculator, 2016
[13] M. Vojnovic and A. Ganesh, "On the Race of Worms, Alerts, and Patches," *IEEE/ACM Trans. Networking*, vol. 16, no. 5, Oct. 2008.
[14] G. S. Dhillon, "Vulnerabilities & Attacks in Mobile Adhoc Networks (MANET)," *Int'l. J. Advanced Research in Computer Science*, vol. 8, 2017.

Additional Reading

[1] W. Li and A. Joshi, *Security Issues in Mobile Ad Hoc Networks–A Survey*, University of Maryland, Baltimore County, 2008, pp. 1–3.

Biographies

Nadra Guizani is a lecturer at Gonzaga University and a Ph.D. computer engineering student at Purdue University, completing a thesis on prediction and access control of disease spread data on dynamic network topologies. Her research interests include machine learning, mobile networking, large data analysis, and prediction techniques. She is an active member of both the Women in Engineering program and the Computing Research Association.

Ali Elghariani received the B.S. and M.S. degrees in electrical and electronic engineering from the University of Tripoli, Tripoli, Libya, and the Ph.D. degree in communications, networking, and signal processing from the School of Electrical and Computer Engineering, Purdue University of West Lafayette, West Lafayette, IN, USA, respectively. He worked in industry for several years before pursuing the Ph.D. degree. Currently, he is a visiting researcher at the school of Electrical and Computer Engineering, Purdue University. His research interests include network security, machine learning and signal processing for wireless communication

Jason Kobes works as a principal cyber architect and research scientist in Washington, DC for Northrop Grumman Corporation. He has over 20 years of experience concentrated in information systems design analytics, business/mission security architecture, enterprise risk management, information assurance research, and business consulting. He has an M.S. in information assurance (MSIA) and a B.S. in computer science from Iowa State University.

Arif Ghafoor is a professor in the School of Electrical and Computer Engineering at Purdue University. His research interests include multimedia information systems, database security, and distributed computing. He is a Fellow of the IEEE.