ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

SPYWARE PROPOSAL IN WIRELESS AD HOC NETWORKS

R.Sudha, B.Suguna, V.Bhuvani, G.Shobikha
*Assistant Professor, A.V.C.College of Engineering
UG Students, A.V.C.College of Engineering
UG Students, A.V.C.College of Engineering
UG Students, A.V.C.College of Engineering

DOI: 10.5281/zenodo.400979

ABSTRACT

Accurate malware propagation modeling in wireless ad hoc networks (WANETs) represents a fundamental and open research issue which shows distinguished challenges due to complicated access competition, severe channel interference, and dynamic connectivity. As an effort towards the issue, in this paper, we investigate the malware propagation under two spread schemes including Unicast and Broadcast, in Spread Mode and Communication Mode, respectively. We highlight our contributions in three-fold in the light of previous literature works. First, a bound of malware infection rate for each scheme is provided by applying the wireless network capacity theories. Second, the impact of mobility on malware propagations has been studied. Third, discussion of the relationship between different schemes and practical applications is provided. Numerical simulations and detailed performance analysis show that the Broadcast Scheme with Spread Mode is most dangerous in the sense of malware propagation speed in WANETs, and mobility will greatly increase the risk further. The results achieved in this paper not only provide insights on the malware propagation characteristics in WANETs, but also serve as fundamental guidelines on designing defense schemes.

KEYWORDS: malware propagation, wireless ad hoc networks, modeling.

INTRODUCTION

MALWARES such as worm and virus have always been great security threats accompanying the development of networks. The Code Red [1], for example, infected hundreds of thousands of hosts and cost over billions in damage to networks.

The last few years have seen a new type of malwares which targets mobile terminals. They can spread from device to device using wireless communication channels, which brings severe security challenges to the applications of wireless networks.

Malware attacks in Internet have long been a topic of extensive studies [2] [3]. And most of the related works are based on the study of epidemic propagation. In this framework, malware propagation models are constructed according to the state transitions of each node, which include Susceptible-Infectious (SI) models [4], Susceptible-Infectious-Susceptible (SIS) models [5],and Susceptible-Infectious-Recovered (SIR) models [6]. In the fundamental SI framework, each node has only two possible states: susceptible or infectious. Based on the simple yet efficient model, a multitude of works [7], [8], [9], [10], [11] have been developed for investigating the propagation of scan-based and topology-based worms. These works also provide a comprehensive approach to enable the research on the fundamental spreading patterns that characterize malware outbreaks.
The lack of any centralized control and possible node mobility in wireless networks raise the risks on the propagation of malicious attacks, which has no counterparts in the wired networks.

SYSTEM MODEL

In this section, we provide an overview of the random network model for the WANET, the protocol model for wireless transmissions, and the epidemic propagation model.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

Random Network Model

First, we consider a random network model with the following settings and notations in this paper:

- The WANET consists of *n* nodes which are randomly located in a unit area.
- Each node chooses the same transmission range *r* or powerlevel *p*.
- *Xi* is used to denote the location of node *i*.
- The total bandwidth of wireless channel is*W*(*Hz*), which can be divided into *M* subchannels and each node can transmit at *Wm* bits per seconds over any *m* channels,where 1< *m* < *M*, and Σ*M* *m*=1*Wm* = *W*.

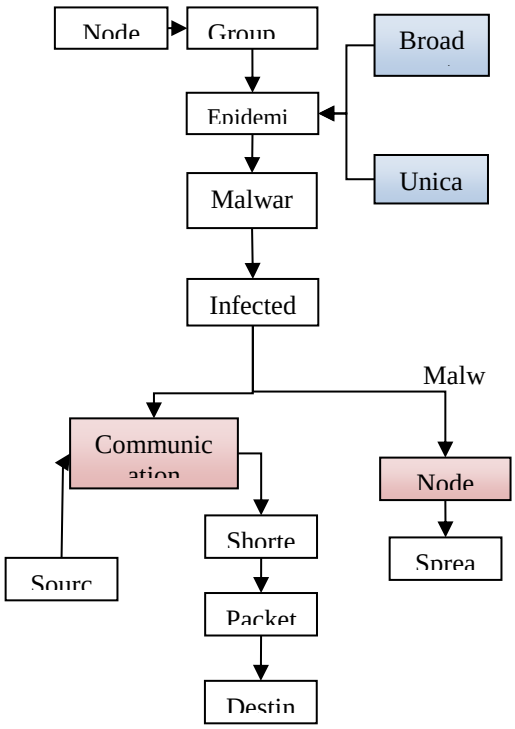
The Epidemic Propagation Model

The Classical Simple Epidemic Model [4] is an *SI* model. In this model, there are only two states for any node in the network susceptible (*S*) and infectious (*I*). Moreover, a node remains in the infectious state forever once it has been infected by a malware.

Before we present the model, we first list some important notations which will be used in the rest of the paper.

- *n*: the number of nodes in the WANET.
- a small time interval.
- *I*(*t*): the number of infected nodes at time *t*.
- [*n* □ *I*(*t*)]: the number of susceptible (uninfected) nodes at time *t*. the infection rate in epidemiology studies which represents a ratio of infection from an infectious node to susceptible nodes among all nodes in the network within a unit time.
- *Tn*: the network infected time.

ARCHITECTURAL REPRESENTATION



MODULES

Malware Propagation:

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

a) **Early stage**: An early stage of the breakout of a malware means only a small percentage of vulnerable hosts have been compromised, and the propagation follows exponential distributions.

b) **Final stage**: The final stage of the propagation of a malware means that all vulnerable hosts of a given network have been compromised.

c) **Late stage**: A late stage means the time interval between the early stage and the final stage.

Network Formation:

Research on complex networks has demonstrated that the number of hosts of networks follows the power law.People found that the size distribution usually follows the power law, such as population in cities in a country or personal income in a nation

Node clustering mechanisms

Select the Cluster Heads node of each groups based on the energy and capacity. The data cluster node handling inter-cluster and intra-cluster data forwarding.

Communication

All nodes in the network are in communication status, competing for transmissions at the same time.The available communication channels is controlled by the Medium Access Control (MAC) protocol.The WANET communications are based on the neighbor node/cluster head.

Performance evolution

Analyze the impact of the mobility on malware propagations is evaluated. Analyze the network Packet arrival rate, Average end-to-end delay, and through put. There are some parameters which will affect the malware propagation, including the number of nodes in the network, the transmission ranges, and the mobility.

MALWARE PROPAGATION MODELS IN WIRELESS AD HOC NETWORKS

In this section, the theoretical models of malware propagation in WANETs are provided, which are based on the classic *SI*.epidemic propagation model [4]. The main work will focus on identifying the infection rate with different propagation schemes by taking the contentions an interferences between nodes into consideration.First of all, we present the definition of two different malware propagation schemes and two network modes.

Malware Propagation Scheme I Unicast: The malware propagates through unicast messages, which means it can infect one of its neighbors at a time.

Malware Propagation Scheme II- Broadcast: The malware is designed to be propagated through broadcast messages, which means it can infect all its neighbors at the same time.

Network Mode I- Spread Mode: Only infectious nodes in the network compete for transmission, and all the susceptible nodes do not compete for transmission. This is an approximate model of
the case when the communication load in the network is light and nodes do not communicate with each other frequently.

Network Mode II- Communication Mode: All nodes in the network are in communication status, competing for transmissions
at the same time.

PERFORMANCE ANALYSIS AND DISCUSSIONS

Simulation Setups

In order to unveil the features of malware propagation in WANETs, we run a comprehensive simulation campaign and analyze the impacts of different parameters. To facilitate the simulations, we developed a dedicated Python simulation program using the NumPy/SciPy/Networkx packages. All simulation results are averaged over 100 runs. The critical features of the simulation are described as follows.

Network model: The random network model is presented by a two-dimensional random geometric graph (RGG) [32], which has been recently used for modeling WANETs [12]. In our simulation it is constructed by first generating nodes with random positions in the unit flat square [0, 1] and then creating an edge between any two nodes which are within each other's transmission range.

Critical transmission range: Critical transmission range *rc* is the transmission radius for each communicating node to achieve a connected network with minimum power consumption and communication interference.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

Medium Access Control: In practical WANETs such as WiFi, a node's access to the available communication channels is controlled by the Medium Access Control (MAC) protocol, whose function is to ensure interference-free wireless transmissions of data packets in the network. The MAC protocol used by WiFi-based wireless devices follows the carrier sense multiple access with collision avoidance (CSMA-CA) scheme, which specifies a set of rules that enable nearby devices to coordinate their transmissions in a distributed manner. CSMA-CA uses Request to Send/Clear to Send (RTS/CTS) schemes to guarantee that no other nodes transmit at the same time within the range of the communicating nodes pair, which satisfies the requirement of our protocol model in Subsection.

CONCLUSION

A generalized WANET structure is studied for the propagation model analysis, considering the features of wireless interference and terminal mobility. First, we have investigated two malware propagation schemes with two different network modes and provided their bounds of infection rates, respectively. Detailed performance analysis shows that the Broadcast Scheme with Spread Mode is most dangerous among the four different conditions. In addition, the impact of the mobility on malware Propagations is evaluated. Based on these analyses, we discuss the malware propagation issues in practical applications and the possible countermeasures.

There are several interesting directions for future works. First, we can consider the network model with node clusters, which means the nodes in the network are not equal. Second, other mobility models with unique characteristics such as temporal dependency, spatial dependency or geographic restriction can be
Considered under certain specified applications. Third, factors such as hardware and software platforms could be added to provide a more comprehensive risk evaluation for different systems. Finally,it is also interesting to further investigate corresponding defense strategies for different propagation models.

REFERENCES

[1] Yini Wang, Sheng Wen, Yang Xiang, and Wanlei Zhou,"Modeling the Propagation of Worms in Networks" A Survey ,2014.
[2] Cliff Changchun Zou, Weibo Gong, Don Towsley, Code Red Worm Propagation Modeling and Analysis,2002.
[3] Hossein ajorloo, s.hashem maddahhosseini, Nasser yazdani, and abolfazl lakdashti, Critical transmission range for connectivity ,In ad-hoc networks ,2007.
[4] M. Roberts and J. Heesterbeek, "Mathematical models in epidemiology,"*Encyclopedia of Life Support Systems (EOLSS)*, 2003.
[5] R. Pastor-Satorras and A. Vespignani, "Epidemic spreading in scale-free networks," *Physical review letters*, vol. 86, no. 14, p. 3200, 2001.