Behavior Analysis of Flooding Attacks in Sparse Mobile Ad-Hoc Networks

Takuya IDEZUKA, Tomotaka KIMURA, and Masahiro MURAGUCHI
Faculty of Engineering, Tokyo University of Science

***Abstract*-- In recent years, many store-carry-forward routing schemes have been proposed for sparse mobile ad-hoc networks, which are the most representative networks in delay/ disconnected tolerant network environments. In general, store-carry-forward routing schemes are designed under the assumption that all nodes in the network are good and cooperative. Therefore, they are highly vulnerable to malicious attacks. To eliminate these vulnerabilities, we need to clarify the characteristics of such malicious attacks. In this paper, we focus on analyzing the behavior of flooding attacks in which malicious nodes generate unnecessary messages to exhaust network resources. Through simulation experiments, we reveal how flooding attacks affect the system performance.**

I. INTRODUCTION

Sparse mobile ad-hoc network is a typical example of DTNs (Delay/Disconnected Tolerant Networks) [1, 2, 3, 5, 6]. In sparse mobile ad-hoc network, nodes are disconnected at almost any time, because the density of nodes is sparse. The nodes, however, can move around the field, occasionally leading to encounters. When two nodes encounter each other, they can communicate with each other. Under these situations, store-carry-forward routing is used for delivering messages [2, 3, 5, 6]. In this routing, when a node generates or receives a message, it stores the message, and then carries the message. When the node with the message encounters another node, the message is forwarded to the encountered node. By repeating this procedure, the destination node eventually receives the message.

To make it easier to deliver messages, multi-copy routing schemes have been developed [2, 3, 5, 6]. Epidemic routing is an example of a multi-copy routing scheme [6]. In Epidemic routing, when a node with a message encounters another node, it always forwards a copy of the message to the encountered node. If the network resources are sufficient, then it is possible to achieve the smallest delivery delay among multi-copy routing schemes, though the network resource is largely consumed in the process.

In most of the existing store-carry-forward routing schemes, it is assumed that all nodes in the network are good and cooperative. Therefore, if there are malicious nodes in the network, these routing schemes are vulnerable to attack. To effectively deliver messages using store-carry-forward routing schemes, it is necessary to eliminate such vulnerability as much as possible.

In this study, we focus on flooding attacks, in which malicious nodes generate unnecessary messages to exhaust network resources [4]. Because sparse mobile ad-hoc networks have limited resources, they can be instantly exhausted through dissemination of unnecessary messages, majorly affecting their system performance. In this paper, we analyze how a flooding attack affects the system performance. To the best of our knowledge, this is the first work to analyze the behavior of flooding attacks in DTN environments.

II. SYSTEM MODEL

The network comprises $N+1$ mobile nodes, including a malicious node. Let V denote the set of nodes in this network. We assume that encounters between two nodes v, w $(v, w \in V)$ follow a Poisson process, with a rate of $\lambda_{v,w}$. Each node has a buffer that can store B different messages. Except for the malicious node, each node generates Λ messages per unit time on average. Each message is delivered to its destination node using Epidemic routing. After message delivery, copies of the message are removed using VACCINE recovery scheme [1]. To cause buffer overflow, the malicious node $m \in V$ generates Λ_M messages per unit time on average, according to a Poisson process, where $\Lambda_M \geq \Lambda$.

III. ANALYSIS OF FLOODING ATTACKS

We investigate how the system performance is affected by the message generation rate Λ_M of the malicious node. Our analysis is an expansion of previous work [5], in which the authors estimated the buffer size B, for which buffer overflow rarely occur under assumptions that nodes are collaborative and homogeneous $(\lambda_{v,w} = \lambda\ (v, w \in V))$. Let $X(t)$ $(t \geq 0)$ denote the number of copies of a message in the network for a message generated at time 0 $(X(0) = 1)$. The time-average of the total number of message copies $E[Q]$ is given by [5]:

$$E[Q] = \frac{E[\int_0^{T_E} X(t)dt]}{E[T_E]},$$

where $E[T_E]$ is the mean extinction time, when all message copies are removed from the network $(X(T_E) = 0)$. Moreover, we denote O_L as the node load incurred by generating the message. O_L is given by:

$$O_L = \frac{E[Q]E[T_E]}{N+1} = \frac{E[\int_0^{T_E} X(t)dt]}{N+1}.$$

Let K denote the total number of messages that a node randomly chosen from the set of nodes has. Because we assumed that each node generates Λ messages per unit time on average, $E[K]$ can be obtained using Little's law for a G/G/∞ queuing system:

This work was supported by JSPS KAKENHI Grant Number 17846116.

$$E[K] = (N+1)\Lambda O_L.$$

Furthermore, through simulation experiments [5], it can be shown that the coefficient of the variation of $E[K]$ is low. Therefore, these authors concluded that buffer overflows rarely occur, when the buffer size is about twice $E[K]$.

In our model, the malicious node generates Λ_M messages per unit time on average. In this case, $E[K]$ is given by:

$$E[K] = (N\Lambda + \Lambda_M)O_L.$$

Here, we consider two scenarios: *the rare generation scenario* ($\Lambda = 0.01$) and *the frequent generation scenario* ($\Lambda = 0.05$). In both scenarios, $N = 100, \lambda_{v,w} = \lambda\ (v, w \in V)$, and $B = 10$. In [2], for $\lambda = 0.01$, it is shown that $O_L \approx 4.19$ [3]. In the rare generation scenario, when the malicious node does not launch the flooding attack ($\Lambda_M = 0.01$), $E[K] = (100+1) \times 0.01 \times 4.19 = 4.23$. This indicates that buffer overflow rarely occurs in the network. Therefore, to cause buffer overflows, the malicious node largely generates unnecessary messages. Specifically, the message generation rate is set to $\Lambda_M = (B/2 - N\Lambda)/O_L = 0.19$. At this setting, Λ_M is much greater than Λ. Therefore, we can easily identify the malicious node among other nodes.

In the frequent generation scenario, $E[K] = (100+1) \times 0.05 \times 4.19 = 21.2 > B/2$. This indicates that buffer overflows occur, even when the malicious node does not launch the flooding attack. Therefore, when Λ_M is set only slightly larger than Λ, buffer overflows frequently occur, but it is difficult to identify the malicious node in this scenario.

IV. Evaluation

A. Simulation model

Through simulation experiments, we investigate the effect of flooding attacks in sparse mobile ad-hoc networks. In our simulation experiments, $N = 100$, $\lambda_{v,w} = 0.01$ $(v, w \in V \setminus \{m\},\ v \neq w)$, $\lambda_{v,m} = \lambda_{m,v} = \lambda_M \in \{0.01, 0.1\}$, and $\lambda_{v,v} = 0$ $(v \in V)$. Note that an increase in the rate λ_M of encountering the malicious node implies that the malicious node moves faster than other nodes. In our simulation, each good node generates messages according to a Poisson process, with a rate of $\Lambda = 0.01$. Meanwhile, the malicious node makes unnecessary messages according to a Poisson process, with a rate of Λ_M. The buffer size B is set to be 10. We use *the loss probability* L as a performance metric. The loss probability is defined as the ratio of the number of unreachable messages to the number of messages that the good nodes generated.

B. Results

Figure 1 shows the loss probability L as a function of the message generation rate Λ_M of the malicious node. When the rate λ_M of encountering the malicious node is small ($\lambda_M = 0.01$), even if Λ_M is set considerably high, L is not large. For example, when $\Lambda_M = 3$ and $\Lambda = 0.05$, only about 20% of messages are unreachable. In contrast, when λ_M is large, i.e., $\lambda_M = 0.1$, most messages cannot be delivered for large Λ_M. Clearly, when only one node launches the flooding attack, and the moving speed of the malicious node is about the same as that of other nodes, the effect of the flooding attack is small. In contrast, if the malicious node is faster than other nodes, then it encounters other nodes more frequently, causing the flooding attack to decrease system performance markedly. Moreover, these results imply that when there are multiple malicious nodes in the network, the effect of flooding attacks is large, especially if the malicious node moves faster than the other nodes. Therefore, it is necessary to implement countermeasures to flooding attacks in networks that have a malicious node that moves fast and/or multiple malicious nodes.

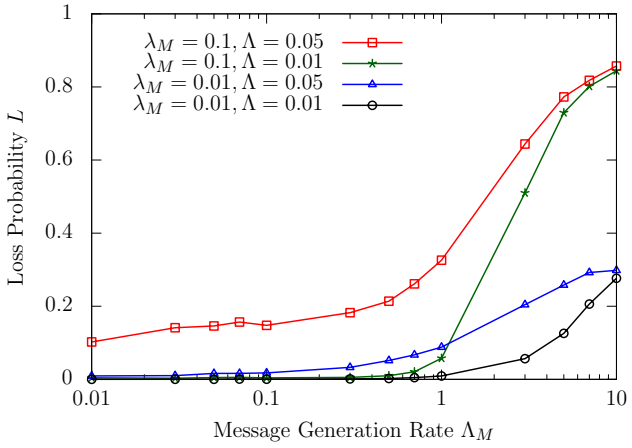

Fig. 1. Loss probability as a function of the malicious message generate rate.

V. Conclusion

In this paper, we analyzed the behavior of a flooding attack in sparse mobile ad-hoc networks. We identified the characteristics of flooding attacks using queuing theory and simulation experiments. These characteristics are useful for designing countermeasures against flooding attacks to be undertaken in future work.

References

[1] Z. Haas and T. Small, "A new networking model for biological applications of ad hoc sensor networks," *IEEE/ACM Transactions on Networking*, 2006.

[2] T. Kimura, T. Matsuda, and T. Takine, "Multi-spreader routing for sparsely populated mobile ad hoc networks," *Wireless Networks*, vol. 20, no. 1, 2014.

[3] T. Kimura, Y. Kayama, and T. Takine, "Home base-aware store-carry-forward routing using location-dependent utilities of nodes," *IEICE Transactions on Communications*, vol. E100-B, no. 1, 2017.

[4] Q. Li, W. Gao, S. Zhu, and G. Cao, "To lie or to comply: Defending against flood attacks in disruption tolerant networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 10, no. 3, 2013.

[5] T. Matsuda and T. Takine, "(p,q)-Epidemic routing for sparsely populated mobile ad hoc networks," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 5, 2008.

[6] A. Vahdat and D. Becker, "Epidemic routing for partially connected ad hoc networks," Duke Technical Report, 2000.