International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 03 | Mar -2017 www.irjet.net p-ISSN: 2395-0072

DETECTING MISBEHAVIOR NODES USING SECURED DELAY TOLERANT NETWORK

S.Aiswarya[1], G.Vanitha[2] , C.B. LogaPreethi[3], A.Monica[4]

[1]*Assistant Professor, Department of Computer Science and Engineering, Velammal Institute of technology, Chennai.*

[2,3,4]*UG Student, Department of Computer Science and Engineering, Velammal Institute of technology, Chennai.*

ABSTRACT - Delay Tolerant Networks (DTN) assumes that the network nodes voluntarily cooperate in order to work properly. This cooperation is a cost-intensive activity and some nodes can refuse to cooperate, leading to a selfish node behavior. Normally nodes are required to exchange their encounter data, in which malicious nodes are intentionally drop all or part.Thus the overall network performance could be seriously affected. Thus, we propose Statistical-based Detection of Blackhole and Greyhole attackers (SDBG to address both individual and collusion attacks. To detect the individual misbehavioring nodes As shown in the paper, detect the attacker node at a time and increases the precision when detecting selfish nodes. Extensive simulation shows that our solution can work with various dropping probabilities and different number of attackers per collusion at high accuracy and low false positive.

Keywords used: Delay Tolerant Network, Blackhole attack and Greyhole attack

1. INTRODUCTION

DTN makes use of hop-by-hop routing and the store-and-forward paradigm to overcome the lack of end-to-end paths. DTN is threatened by various attacks, including black- hole and greyhole. Blackhole attackers drops all the received messages even if they have enough buffer storage. Greyhole attackers drops received messages partially. The malicious nodes will decrease the overall message delivery and waste the resources of intermediate nodes.

[1], [2] require trusted ferries to check if nodes arbitrarily increase their delivery probabilities to absorb more data, which is preliminary to the dropping attack. [3] depends on a trusted authority to investigate nodes based on the evidences of forwarding tasks, contact opportunities and actual forwarding behaviors. [4] designs a trust-based framework in which the message forwarding behavior is acknowledged and rewarded with reputation. [5], [6], and [7] make use of node's encounter records to detect or mitigate the impact of the attack. In the above methods, only individual attackers can be found, they cannot handle multiple attackers. For example, in an individual detection method, is for each nodes, histories of encounters will be evaluated with other nodes, i.e., encounter records. A node is suspected as malicious if it's forwarding ratio is lower than a threshold. Forwarding ratio is the ratio between the total number of sent messages and receive messages. This method will work if attackers tend to drop received messages instead of sending them. If attackers cooperate with each other node and creates the forged encounter records by boosting the forwarding ratio. So, this kind of cooperative attacks can be detected by this method. This type of attack is called as collusion attack. In the proposed method, Statistical-based Detection of Blackhole and Greyhole (SDBG), which can detect both individual and collusion attacks with high accuracy is used. SDBG is designed based on the following observations. Forwarding ratio is used to find individual attack, attackers tend to send out their own messages rather than messages of other nodes. The individual detection accuracy can be improved by observing the number of self-sent messages. In collusion attacks, since attackers need to frequently create fake encounter records to boost the forwarding ratio metric, their number of sent messages can be high. This observation enables us to detect collusion attack.

2. RELATED WORK

Zhaoyu Gao*y* experimented with malicious and selfish behaviors represent a serious threat against routing in Delay or Disruption Tolerant Networks (DTNs). Due to the unique network characteristics, designing a misbehavior

detection scheme in DTN represents a great challenge. The basic idea of a probabilistic misbehavior detection scheme (PMDS) is introducing a periodically available Trusted Authority (TA), which judges the node's behavior based on the collected routing evidences. PMDS model is the Inspection Game and use game theoretical analysis to demonstrate that, by setting an appropriate investigation probability, TA could ensure the security of DTN routing at a reduced cost. To improve the efficiency of the scheme, correlate detection probability with a node's reputation, which allows a dynamic detection probability determined by a node's reputation. The extensive analysis and simulation results show that the scheme substantiates the effectiveness and efficiency of the scheme.

Qinghua Li worked in disruption tolerant networks (DTNs), selfish or malicious nodes may drop received packets. Such routing misbehavior reduces the packet delivery ratio and wastes system resources such as power and bandwidth. Although techniques have been proposed to mitigate routing misbehavior in mobile ad hoc networks, they cannot be directly applied to DTNs because of the intermittent connectivity between nodes. To address the problem, a distributed scheme is used to detect packet dropping in DTNs. In a scheme, a node is required to keep a few signed contact records of its previous contacts, based on which the next contacted node can detect if the node has dropped any packet. Since misbehaving nodes may misreport their contact records to avoid being detected, a small part of each contact record is disseminated to a certain number of witness nodes, which can collect appropriate contact records and detect the misbehaving nodes. A scheme to mitigate routing misbehavior by limiting the number of packets forwarded to the misbehaving nodes is used. Trace-driven simulations show these solutions which are efficient and can effectively mitigate routing misbehavior.

Yanzhi Ren found that the Disruption Tolerant Networks (DTNs) are vulnerable to insider attacks, in which the legitimate nodes are compromised and the adversary modifies the delivery metrics of the node to launch harmful attacks in the networks. The traditional detection approaches of secure routing protocols cannot address such kind of insider attacks in DTNs. A mutual correlation detection scheme (MUTON) for addressing these insider attacks. MUTON takes into consideration of the transitive property when calculating the packet delivery probability of each node and correlates the information collected from other nodes. To evaluate this approach through extensive simulations using both Random Way Point and Zebranet mobility models. The results show that MUTON can detect insider attacks efficiently with high detection rate and low false positive rate.

3. PROPOSED SYSTEM

Statistical-based Detection of Blackhole and Greyhole attackers (SDBG) to address both individual and collusion attacks to detect .A authority to reduce the time and improve the effectiveness of detecting selfish nodes, reducing the harmful effect of false positives, and malicious nodes. When a contact occurs between two or more collaborative nodes. We can thus enhance the individual detection accuracy by further observing the number of selfsent messages Each and every nodes updated to identify the authority. So easy to detect collusion and individual attack and we can produce high accuracy and low false positive.

3.1 Network Formation and Authority Creation

First we can create a Trusted Authority and then create network node assume the communication range of a node is finite. Thus a data sender out of destination node's communication range can only transmit packetized data via a sequence of intermediate nodes in a multi-hop manner. For the simplicity of presentation, we take a three-step data forwarding process as an example. Suppose that node A has packets, which will be delivered to node C. Now, if node A meets another node B that could help to forward the packets to C, A will replicate and forward the packets to B. Thereafter, B will forward the packets to C when C arrives at the transmission range of B. In this process, we define three kinds of data forwarding evidences. They are Delegation Task Evidence, Forwarding History Evidence and Contact History Evidence, Encounter Records, Message Records.

Fig- 1: Authority Details

3.1.1 First Contact Algorithm

First contact algorithm is used in the proposed approach. First contact algorithm is the algorithm is used to find the nearest neighboring node in the network. It is mainly used for hop-by-hop communication in Delay Tolerant Network. For example, let consider the three nodes a_1, a_2 and a_3. Using First contact algorithm, each node can find nearest node by creating a contact history will have the information (name of the nearest neighbour node, time of that node creation) about each and every nearest node. Thus, the neighbour node can be found.

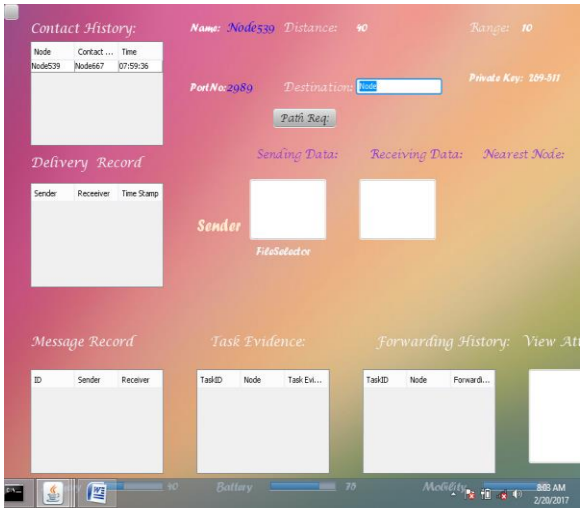

Fig-2: Contact History

3.2 Route Finding and Data Forwarding

A normal user will honestly follow the forwarding the messages as long as there are enough contacts. The requested message has been forwarded to the next hop, the chosen next hop nodes. We assume a trusted authority with the right to assign each node a unique identifier and a pair of public and private keys. Nodes are assumed to know the public keys of each other so that they can authenticate messages signed by others. we model the general behaviors of nodes as follows. When two nodes encounter and exchange messages, each of them generates an Encounter Record (ER) and stores it in its own storage. The ER includes the identities of two nodes, the ER sequence numbers assigned by them, the encounter timestamp and the lists of sent and received messages between the two parties and their signatures.

3.3 Detecting for colluding Attacks

When two nodes are communicating via intermediate node some time individuals adversaries launches an attacker first receives messages from other nodes but later drops them with a certain probability. Blackhole attacker drops all received messages (dropping probability = 100%) while greyhole attacker drops partially (dropping probability lower than 100 percent). The dropping occurs even if the attacker still has enough buffer to store messages , Introduces a SDBG, which could launch the trusted authority based watchdog for the target node and judge it by collecting the forwarding history evidence from its upstream and downstream nodes. Each node maintains a local black list which lists malicious nodes that it detects as blackhole or greyhole attackers If any node is detected as committing either misbehaviors, authority will punish it accordingly and then trusted authority add blacklist and send malicious node name to all nodes. . To further improve the performance of the proposed Statistical-based Detection on scheme, we introduce a reputation system, in which the inspection probability could vary along with the target node's reputation. Under the reputation system, a node with a good reputation will be checked with a lower probability while a bad reputation node could be checked with a higher probability.

4. RESULT AND ANALYSIS

Finding the route and detecting the black hole and grey hole attacks has been implemented and the results are shown below:

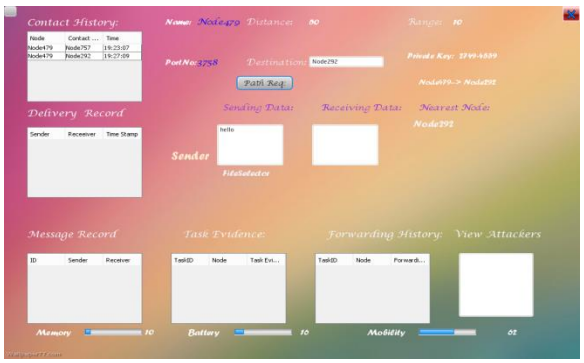

Fig-3: Finding the route

Fig-4: Detecting Greyhole and Blackhole Attacks

5. CONCLUSION AND FUTURE WORK:

We propose a method SDBG that can successfully prevent not only individual attackers but also cooperating attackers. The simulation results show that SDBG can detect colluding malicious nodes with high detection rate and low false positive rate when varying the number of colluding nodes and with a wide range of packet- dropping probability and different routing protocols.

REFERENCES

[1] M. Chuah, P. Yang, and J. Han, "A ferry-based intrusion detection scheme for sparsely connected ad-hoc networks," in Proc. 4th Annu. Int. Conf. Workshop Security Emerging Ubiquitous Comput., 2007.

[2] Y. Ren, M. Chuah, J. Yang, and Y. Chen, "MUTON: Detecting malicious nodes in disrupt-tolerant networks," in Proc. IEEE Wire- less Commun. Netw. Conf., 2010.

[3] Z. Gao, H. Zhu, S. Du, C. Xiao, and R. Lu, "PMDS: A probabilistic misbehavior detection scheme toward efficient trust establish- ment in Delay-tolerant networks," IEEE Trans. Parallel Distrib. Syst., Jan. 2014.

[4] N. Li and S. K. Das, "A trust-based framework for data forward- ing in opportunistic networks," Elsevier J. Ad Hoc Netw., 2013.

[5] F. Li, J. Wu, and A. Srinivasan,, "Thwarting blackhole attacks in disrupt-tolerant networks using encounter tickets," in Proc. INFOCOMM, 2009.

[6] Y. Guo, S. Schildt, and L. Wolf, "Detecting blackhole and greyhole attacks in vehicular delay tolerant networks," in Proc. IEEE 5th Int. Conf. Commun. Syst. Netw., Jan. 2013.

[7] Q. Li and G. Cao, "Mitigating routing misbehaviors in disruption tolerant networks," IEEE Trans. Inf. Forensics Security, Apr. 2012.

[8] J. Ott and D. Kutscher, "A disconnection-tolerant transport for drive-thru internet environments," in Proc. IEEE 24th Annu. Joint Conf. Comput. Commun. Soc., Mar. 2005.

[9] J. Burgess, B. Gallagher, D. Jensen, and B. N. Levine, "Maxprop: Routing for vehicle-based disruption-tolerant networks," in Proc. IEEE Int. Conf. Comput. Commun., Barcelona, Spain, Apr. 2006.

[10] M. J. Khabbaz, C. M. Assi, and W. F. Fawaz, "Disruption-tolerant networking: A comprehensive survey on recent developments and persisting challenges," in Proc. IEEE Commun. Surveys Tuts., 2012.