RESEARCH ARTICLE OPEN ACCESS

Detecting Selfish Nodes on Overlay Network and Optimizing the Network by Isolating Malicious Nodes Using Reputation-Based Mechanism

Naveen Kumar.B [1], Pampapathi.B.M [2], Mahantesh.H.M [3], Shivakeshi.C [4]
Assistant Professor [1], [2], [3] & [4]
Department of Computer Science and Engineering [1] & [2]
Department of Information Science and Engineering [3] & [4]
Rap Bahadur Y. Mahabaleswarappa Engineering College
VTU, Ballari
Karnataka - India.

ABSTRACT

The overlay networks to realize their potential in commercial deployments, it is important that they incorporate adequate security measures. Selfish behaviour of autonomous network nodes could greatly disrupt network operation. Such behaviour should be discouraged, detected, and isolated. In this paper, proposed reputation-based mechanism is to detect and isolate selfish nodes in an overlay network. Selfishness is usually passive behaviour. Additionally, malicious nodes may intentionally, and without concern about their own resources, attempt to disrupt network operations by mounting denial-of-service attacks or by actively degrading the network performance. For example, malicious nodes could disrupt routing operation by advertising non-existent routes or sub-optimal routes. Selfish and malicious behaviours are usually distinguished based on the node's intent. Network disruption is a side effect of the behaviour of a selfish node, while disrupting the network is the intent of malicious nodes. The focus is on detection and isolation of selfish nodes in overlay networks. So a reputation-based mechanism is proposed as a means of building trust among nodes. The mechanism relies on the principle that a node autonomously (i.e., without communicating with other neighbouring nodes) evaluates its neighbours based on the completion of the requested service(s).

Keywords:- Overlay network, Peer-to-Peer networks, load balancing, Internet Protocol (IP), cloud computing.

I. INTRODUCTION

An overlay network is a virtual network of nodes and logical links that is built on top of an existing network with the purpose to implement a network service that is not available in the existing network. An overlay network is a computer network which is built on the top of another network. Nodes in the overlay can be thought of as being connected by virtual or logical links, each of which corresponds to a path, perhaps through many physical links, in the underlying network. For example, distributed systems such as cloud computing, peer-to-peer networks, and client-server applications are overlay networks because their nodes run on top of the Internet. The Internet was built as an overlay upon the telephone network.

Overlay networks are distributed systems in nature, without any hierarchical organization or centralized control.

Peers form self-organizing overlay networks that are over layer on the Internet Protocol (IP) networks, offering a mix of various features such as robust wide-area routing architecture, efficient search of data items, selection of nearby peers, redundant storage, permanence, hierarchical naming, trust and authentication, anonymity, massive scalability, and fault tolerance. Over the Internet today, computing and communications environments are significantly more complex and chaotic than classical distributed systems, lacking any centralized organization or hierarchical control. There has been much interest in emerging Peer-to-Peer (P2P) network overlays because they provide a good substrate for creating large-scale data sharing, content distribution, and application-level multicast applications. These P2P overlay networks attempt to provide a long list of features, such as: selection of nearby peers, redundant storage, efficient search/location of data items, data permanence or guarantees, hierarchical naming, trust and authentication, and anonymity.P2P networks potentially offer an efficient

routing architecture that is self-organizing, massively scalable, and robust in the wide-area, combining fault tolerance, load balancing, and explicit notion of locality. We can view P2P overlay network models spanning a wide spectrum of the communication framework, which specifies a fully-distributed, cooperative network design with peers building a self-organizing system.

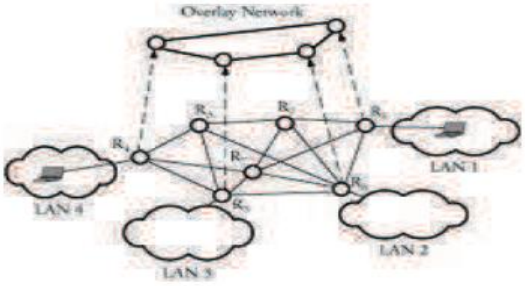

Fig 1: Overlay Network

II. RELATED WORK

For overlay networks to realize their potential in commercial deployments, it is important that they incorporate adequate security measures. Selfish behavior of autonomous network nodes could greatly disrupt network operation. Such behavior should be discouraged, detected, and isolated. For achieving that a reputation-based mechanism is used to detect and isolate selfish nodes in an overlay network. The proposed mechanism allows a node to autonomously evaluate the "reputation" of its neighbors based on the completion of the requested service.

The focus is on detection and isolation of selfish nodes in overlay networks. So a reputation based mechanism is used as a means of building trust among nodes. The mechanism relies on the principle that a node autonomously (i.e., without communicating with other neighboring nodes) evaluates its neighbors based on the completion of the requested service(s). This principle, in general, can be applied to operations that involve cooperation among nodes in an overlay network.

III. OVERLAY NETWORK

Overlays are easy to deploy and flexible, and can be resilient to faults. To achieve desired properties, however, most overlay systems assume that nodes cooperate with one another by following well-defined protocols, regardless of the costs incurred.

In reality, however, nodes may behave selfishly—seeking to maximize their own benefit. For instance, when parties in different domains utilize their own resources (overlay nodes) to participate in an overlay network, they have clear incentives to create links that maximize the benefit to their domain, possibly at the expense of globally optimum behavior. It is an open question whether these networks can have desirable global properties, in spite of the distinct local interests of the participating nodes. Inspired by the game theoretical model, selfishly constructed networks by modeling network formation as a non-cooperative game are studied. In this game, each node chooses its overlay neighbors to maximize its benefit and to minimize its linking cost. Consequently, nodes can have conflicting goals: on the one hand, they want to have low cost paths to other nodes in the network by establishing more links, and on the other hand, they may not want to establish many links, which may turn out to be costly.

Overlay network protocols based on TCP/IP include:

- Distributed hash tables (DHTs), such as KAD and other protocols based on the Kademlia Algorithm, for example.
- JXTA
- Many peer-to-peer protocols including Gnutella, Gnutella2, Freenet and I2P. (Examples: Lime wire, Shareaza, u torrent, etc.)
- PUCC
- Solipsis: a France Telecom system for massively shared virtual world

Overlay network protocols based on UDP/IP include:

- Real Time Media Flow Protocol - Adobe Flash

Overlay routing networks have become increasingly popular over the last few years. They form supporting technology for diverse application domains such as multicast, object location, and secure data dissemination. Overlays are easy to deploy and flexible, and can be resilient to faults. To achieve desired properties, however, most overlay systems assume that nodes cooperate with one another by following well-defined protocols, regardless of the costs incurred.

Selfish Nodes:

In an overlay network, the transmission range of mobile nodes is limited due to power constraint. Hence communication between two nodes beyond the transmission range relies on intermediate nodes to forward the packets. But sometimes these intermediate nodes do not work as expected, in order to conserve their limited resources such as energy, bandwidth etc. Such nodes are called non cooperative nodes or misbehaving nodes.

Selfish nodes are one type of non cooperative nodes which work in an overlay network to optimize their own

gain, with neglect for the welfare of other nodes. Selfish nodes disturb the performance of overlay network to a great extent. When a node becomes selfish it does not cooperate in data transmission process and causes a serious affect on network performance. It simply does not forward packets of other nodes to conserve its own energy, bandwidth.

One immediate effect of node misbehaviors and failures in wireless ad hoc networks is the node isolation problem due to the fact that communications between nodes are completely dependent on routing and forwarding packets. In turn, the presence of selfish node is a direct cause for node isolation and network partitioning, which further affects network survivability. Traditionally, node isolation refers to the phenomenon in which nodes have no (active) neighbors; however, a node can be isolated even if active neighbors are available.

Mechanisms

For the security problem and the misbehavior problem of overlay networks, various techniques have been proposed to prevent selfishness in MANETs. Most of the existing solutions are based on following mechanisms:

- Reputation Based
- Credit Based and
- Reputation Cum Credit Based Mechanism

Reputation Based

Reputation systems are used to keep track of the quality of behavior of other nodes. Basically reputation is an opinion formed on the basis of watching node behavior by direct and/or indirect observation of the nodes, through route or path behavior, number of retransmissions generated by the node, through acknowledgement message and by overhearing node's transmission by the neighboring nodes.

One of the main goals/reasons for using reputation systems in a network of entities interacting with each other is to provide information to help assess whether an entity is trustworthy. This helps in detection of selfish and malicious nodes. Another goal is to encourage entities to behave in a trustworthy manner, i.e. to encourage good behavior and to discourage untrustworthy entities from participating during communication.

Credit Based

Credit based mechanisms reward nodes for forwarding by giving them credits. Without credit, a node cannot transmit self-generated data packets. The basic idea of credit-based schemes is to provide incentives for nodes to faithfully perform networking functions. In order to achieve this goal, virtual (electronic) currency or similar payment system may be set up. Nodes get paid for providing services to other nodes. When they request other nodes to help them for packet forwarding, they use the same payment systemto pay for such services.

Buttyan and Hubaux used the concept of nuggets (also called beans) as payments for packet forwarding. They proposed two models: the Packet Purse Model and the Packet Trade Model. In the Packet Purse Model, nuggets are loaded into the packet before it is sent. The sender puts a certain number of nuggets on the data packet to be sent. Each intermediate node earns snuggest in return for forwarding the packet. If the packet exhausts its nuggets before reaching its destination, then it is dropped. In the Packet Trade Model, each intermediate node buys the packet from the previous node for some nuggets, and sells. It to the next node for more nuggets. Thus, each intermediate node earns some nuggets for providing the forwarding service, and the overall cost of sending the packet is borne by the destination.

Each node maintains a counter termed nuglet counter. The counter is decreased when the node sends packets of its own, but increased when it forwards packets for the other nodes. The counter should be positive before a node is allowed to send its packet. Therefore, the nodes are encouraged to continue to help other nodes. Tamper resistant hardware modules are used to keep nodes from increasing the nuglet counter illegally.

Reputation cum Credit Based

Secure and Objective Reputation–based Incentive (SORI) scheme encourages packet forwarding and disciplines selfish behavior in a non cooperative overlay network. Reputation of the node is used as an incentive for cooperate among nodes. Authors are able to design a punishment scheme to penalize selfish nodes. ARM selects low mobility nodes as reputation management nodes and is responsible for managing reputation values. ARM uses locality aware Distributed Hash Table for efficient reputation information collection and exchange. Advantage of using ARM is that ARM builds a hierarchical structure to efficiently manage the RVs of all nodes, and release the reputation management load from individual high mobility nodes. This enables low overhead and fast global reputation information accesses. Also ARM does not require currency circulated in the system.

IV. IMPLEMENTATION

Implementation of any software is always preceded by important decisions regarding selection of the platform, the language used, etc. these decisions are often influenced by several factors such as real environment in which the system works, the speed that is required, the security concerns, and other implementation specific details. There are three major implementation decisions that have been made before the implementation of this project. They are as follows:

1. Selection of the platform (Operating System).
2. Selection of programming language for the development of the application.
3. Coding guideline to be followed.

Most protocols used for implementing overlay routing or content sharing impose hard constraints on the maximum number of overlay neighbors. For example, in popular versions of Bit Torrent a client may select up to 50 nodes from a neighbors' list provided by the Tracker of a particular torrent file. In overlay routing systems, the number of immediate nodes has to be kept small so as to reduce the monitoring and reporting overhead imposed by the link-state routing protocol implemented at the overlay layer. Hard constraints on the number of first hop neighbors are also imposed in most P2P systems to address scalability issues, up-link fragmentation, and CPU consumption due to contention.

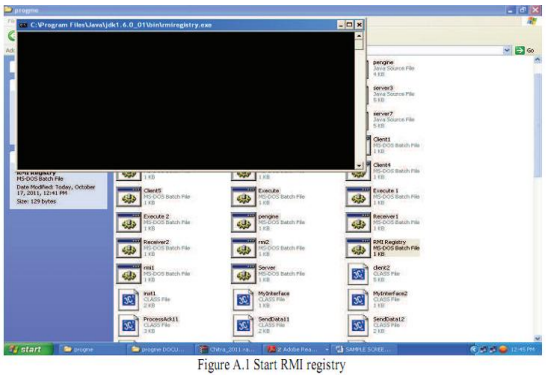

Figure A.1 Start RMI registry

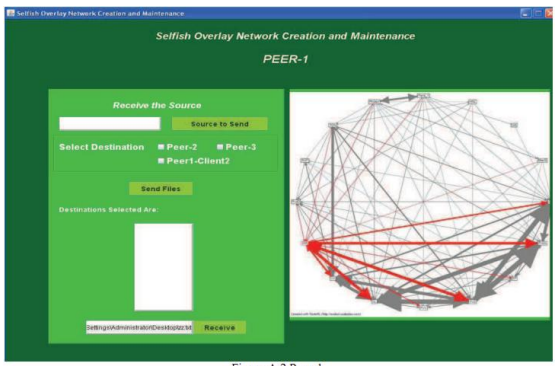

Figure A.2 Peer-1

V. CONCLUSION

In this paper, the design and evaluation of a reputation-based mechanism that isolates selfish nodes in an overlay network has been proposed. The results indicate that the mechanism is successful in achieving fast isolation of selfish nodes. Selfish and malicious behaviors are usually distinguished based on the node's intent. Network disruption is a side effect of the behavior of a selfish node, while disrupting the network is the intent of malicious nodes. The focus is on detection and isolation of selfish nodes in overlay networks. A reputation-based mechanism has been proposed as a means of building trust among nodes. The mechanism relies on the principle that a node autonomously (i.e., without communicating with other neighboring nodes) evaluates its neighbors based on the completion of the requested service(s).

REFERENCES

[1] [N. Laoutaris, G. Smaragdakis, A. Bestavros, and J. W. Byers, "Implications of Selfish Neighbor Selection in Overlay Networks," in Proc. IEEE INFOCOM'07.

[2] G. Smaragdakis, V. Lekakis, N. Laoutaris, A. Bestavros, J. W. Byers, and M. Roussopoulos, "EGOIST: Overlay Routing using Selfish Neighbor Selection," in Proc. ACM CoNEXT'08.

[3] D. Andersen, H. Balakrishnan, F. Kaashoek, and R. Morris, "Resilient Overlay Networks," in Proc. ACM SOSP'01.

[4] L. Qiu, Y. R. Yang, Y. Zhang, and S. Shenker, "On Selfish Routing in Internet-like Environments," in Proc. ACM SIGCOMM'03.

[5] T. Roughgarden and ´Eva Tardos, "How Bad is Selfish Routing?" Journal of the ACM, vol. 49, no. 2, pp. 236–259, 2002.

[6] P. Dewan, P. Dasgupta and A. Bhattacharya, "On using reputations in ad hoc networks to counter malicious nodes," Proceedings of the 10th Intl. Conference on Parallel and Distributed Systems, July 2004, pp. 665-672.

[7] S. Buchegger and J.Y. LeBoudec, "The effect of rumor spreading in reputation systems for mobile ad hoc networks," Proceedings of the Workshop on Modeling and Optimization in Mobile, Ad hoc and Wireless Networks, March 2003.

[8] Z. Despotovic and K. Aberer, "A probabilistic approach to predict peers' performance in P2P networks," Proceedings of the Intl. Workshop on Cooperative Information Agents, September 2004.

[9] C. Perkins, E. Belding-Royer and S. Das, "Ad hoc Ondemand Distance Vector (AODV) routing," IETF RFC 3561, July 2003; www.faqs.org/rfcs/rfc3561.html.

[10] P. Michiardi and R. Molva, " Simulation based analysis of security exposures in mobile ad hoc networks," Proceedings of the European Wireless Conference, February 2002.