A Survey On Detection And Mitigation Of Misbehavior In Disruption Tolerant Networks

Ardra. P. S,
Dept. of Computer Science and Engineering
K.S.R College of Engineering
Tiruchengode, India
ardraps@gmail.com

A. Viswanathan,
Dept. of Computer Science and Engineering
K.S.R College of Engineering
Tiruchengode, India
viswanathcse@yahoo.com

***Abstract*- Denial of Service (DoS) attack is one of the major problem in today's Internet. It constitutes the hardest security problems nowadays. Particularly Distributed Denial of Service (DDoS) attack have severe impact. The main aim of a DoS is the disruption of services by attempting to control access to a system or service instead of overthrowing the service itself. Disruption-Tolerant Networks (DTNs) deliver data in network environments composed of intermittently connected nodes. Malicious nodes within a DTN may attempt to delay or destroy data in transit to its destination. Such attacks include dropping data, flooding the network with extra messages, corrupting routing tables, and counterfeiting network acknowledgments. Packet dropping in DTNs can be detected in a distributed way by observing signed contact records. To mitigate such routing misbehavior a scheme is proposed in which the number of packets forwarded to the misbehaving nodes is limited. When one or more nodes are malicious, they may prevent correct message routing. Alternate routing paths can be used to circumvent them. In this paper attacks aimed at preventing correct message delivery in structured peer-to-peer overlays and defenses to these attacks are discussed. This survey entitles the above mentioned problem and solutions proposed.**

Keywords: Attack Mitigation; Peer-ID; Security; Tracer Routing.

I. INTRODUCTION

Denial of Service (DoS) attacks constitutes one of the major threats and among the hardest security problems in today's Internet. DoS is the disruption of services by attempting to limit access to a machine or service instead of subverting the service itself. The DDoS attack is the most advanced form of DoS attacks. It is distinguished from other attacks by its ability to deploy its weapons in a ‘‘distributed’’ way over the Internet and to aggregate these forces to create lethal traffic. DDoS attacks never try to break the victim's system, thus making any traditional security defense mechanism inefficient. The main goal of a DDoS attack is to cause damage on a victim either for personal reasons, either for material gain, or for popularity.

DDoS attacks are probably the most ferocious threats to the integrity of the Internet. It pose an ever greater challenge to the Internet with increasing resources at the hands of attackers. It is well known that it is rather easy to launch, but difficult to defend against, a DDoS attack. The underlying reasons include (1) IP spoofing; (2) the distributed nature of the DDoS attack (a huge number of sources generate attack traffic simultaneously); (3) no simple mechanism for the victim to distinguish the normal packets from the lethal traffic. It is most accurate to detect DDoS attacks closer to the victim, especially for flooding-style attacks. On the other hand, it is more effective to control the attack traffic closer to the attack sources. Hence, because of the distributed nature of DDoS problem, we need a distributed solution, in which detection and reaction components are deployed at multiple places throughout the Internet, and must cooperate with each other to mitigate attack effect.

Disruption of service caused by DDoS attacks is an increasing problem in the Internet world. Disruption Tolerant Networks (DTNs) [10] consist of mobile nodes which contact each other opportunistically. Due to the low node density and unpredictable node mobility, only intermittent network connectivity exists in DTNs. To transfer data DTNs exploit the intermittent connectivity between mobile nodes. Two nodes exchange data only when they move into the transmission range of each other. This is called a contact between those nodes. Thus, DTN routing usually follows store-carry-forward; i.e., when a node receives some packets, it stores these packets in its buffer, carries them around until it contacts another node, and then forwards the packet.

In DTNs, a node may misbehave by dropping packets even when it has sufficient buffers. Selfish

nodes misbehave by showing unwillingness to spend resources such as power and buffer on forwarding packets of others while the malicious nodes that drop packets to launch attacks. These will result in routing misbehavior in DTNs. There are several techniques proposed to detect and mitigate this routing misbehavior in network.

Several techniques have been proposed to detect and alleviate the effects of such selfish nodes in MANETs [5], [12], [13], [14], [15], [16]. In [5], two techniques were introduced, namely, watchdog and path rater, to detect and mitigate the effects of the routing misbehavior, respectively. The watch- dog technique identifies the misbehaving nodes by over-hearing on the wireless medium. The path rater technique allows nodes to avoid the use of the misbehaving nodes in any future route selections. The watchdog technique is based on passive overhearing. Unfortunately, it can only determine whether or not the next-hop node sends out the data packet. The reception status of the next-hop link's receiver is usually unknown to the observer. In order to mitigate the adverse effects of routing misbehavior, the misbehaving nodes need to be detected so that these nodes can be avoided by all well-behaved nodes.

Our approach consists of a packet dropping detection scheme and a routing misbehavior mitigation scheme. The misbehaving node is required to generate a contact record during each contact and report its previous contact records to the contacted node. Based on the reported contact records, the contacted node detects if the misbehaving node has dropped packets. The misbehaving node may misreport (i.e., report forged contact records) to hide its misbehavior, but forged records cause inconsistencies which make misreporting detectable. To detect misreporting, the contacted node also randomly selects a certain number of witness nodes for the reported records and sends a summary of each reported record to them when it contacts them.

We propose tracer routing, an efficient routing strategy designed to control the routing path while reducing the normal routing latency. Combined with a peer-ID based signature scheme, it can offer the initiator of each query to identify malicious nodes. A key feature of our scheme from other protocols is that alternate routing is constructed only detecting malicious nodes. We propose to address routing message attack by combined tracer routing with Peer-ID based signature scheme. Note that Peer- ID based signature scheme is not necessary. Any techniques of verifying the Peer-ID of remote peer can work with tracer routing. In our scheme, the initiator appends a signature to a query. When an intermediate peer x receives the message (including query and its signature), x verifies the message and discards the polluted or forged one using the initiators public key. Recall that the public key is the Peer- ID of initiator. Then x forwards the message it received to the next hop. At the same time, x sends an acknowledgement (including the Peer- ID of the next hop, query and the signature generated using the private key of x) to initiator. The process is repeated until the query reaches the target.

II. LITERATURE REVIEW

Disruption-tolerant networks (DTNs) provide communication in scenarios that challenge traditional mobile network solutions. DTNs use the inherent mobility of the network to deliver messages in the face of sparse deployments, highly mobile systems, and intermittent power. DTN routing differs from previous networking paradigms by assuming that connectivity will be unpredictable and poor, so information must be opportunistically routed toward the final destination.

In addition to those challenges, malicious adversaries may threaten connectivity in a DTN by inserting, flooding, corrupting, and dropping messages. In traditional, infrastructure based networks and manets, security is often provided by restricting participation to a specific set of authorized nodes, enforced with cryptographic keys and identity management. In such a system, an administrator certifies all nodes in the network and participants will only route messages through other authorized nodes.

The routing protocol used in a DTN strongly influences the security properties of the system. Two characteristics in routing protocols are : criterion and style. The criterion refers to the process by which neighboring nodes are passed packets; specifically, metric based and random criteria. The style indicates whether the protocol is replicative or forwarding. The performance when under attack of MaxProp(metric-based and replicative) to three other protocols: RandProp (random and replicative), MaxForw (metric-based and forwarding), and RandForw (random and forwarding) is compared in [7]. MaxProp is a good point of departure because it offers better throughput than several other strategies like Random, FIFO, MV, Djikstra with an oracle of future transfer opportunities, PROPHET, and Spray-and-Wait. They have shown that replication has a number of advantages over forwarding.

Routing misbehavior has been widely studied in mobile adhoc networks. Much work has been done to detect packet dropping and mitigate routing misbehavior. In [5] two extensions to the Dynamic Source Routing algorithm (DSR) [9] to mitigate the effects of routing behavior are proposed: watchdog and path rater. The watchdog identifies misbehaving nodes, while path rater avoids routing packets through these nodes. When a node forwards a packet, the node´s watchdog verifies that the next node in path also forwards the packet. The watchdog technique is based on passive overhearing. Unfortunately, it can only determine whether or not the next- hop node sends out the data packet. Path rater allows nodes to avoid the use of misbehaving nodes in any future routing selection.

A. Metric-based DTN routing protocols

DTNs attempt to route packets via intermittently-connected nodes. Most of the previous work on DTNs has been based on various assumptions regarding connectivity and the availability of environmental knowledge and control. Some of them even assume that nodes know all future contact information. Since the real mobility trace the recent experimental DTNs appear to be cyclic to a large extent, several recently-proposed routing protocols in DTNs designed metrics to summarize the information of contact history. These metric-based DTN routing protocols use history to predict the future and are widely applicable. However, all of them assume the truthfulness of the history information and omit the possibility of attacks by providing faked metrics.

B. Attacks with forged metrics in MANETs

The blackhole attack [3]and other attacks with forged metrics, such as wormhole attacks have attracted significant research interest in MANETs. When launching a wormhole attack[2], an adversary connects two distant points in the network using a direct low-latency communication link, known as the wormhole link. The attacker uses the wormhole link to claim and distribute falsified connectivity metrics in an effort to affect routing. The existing countermeasures to these attacks with forged metrics mainly focus on utilizing geometric properties and inherent restrictions of the network. Some of them consider geographical and temporal packet leashes. Others define forbidden substructures in the connectivity graph according to the underlying communication model and graph theory, and detect such substructures to decide whether attackers exist. Since the connectivity or other routing-related metrics comply to certain rules and restrictions in MANETs, these countermeasures are applicable.

However, in DTNs, such rules and restrictions of connectivity are invalid due to high mobility and a dynamic topology. Some routing metrics, such as the historical contact probability, are provided by the possible forwarder itself and are hard to verify. This makes the existing countermeasures inapplicable in DTNs.

C. Trust management systems

Various frameworks have been designed to model trust networks and have been used as trust management systems. Most trust management systems allow each node to build its own view of other nodes based on its own observations as well as on recommendations from others. Reputation systems, such as CONFIDANT and CORE, divide the trust opinion into belief and disbelief. In uncertainty is added and considered to be an important dimension of trust. In DTNs, nodes collect information through direct communication in a distributed manner and form trust opinions based on collected encounter evidence.

D. Self-Organized Network-Layer Security

In SCAN [6], they tackle an important security issue in ad hoc networks, namely the protection of their network-layer operations from malicious attacks. They focused on securing the packet delivery functionality since it is the premise for the multihop connectivity between two far away nodes. Without appropriate protection, the malicious nodes can readily function as routers and prevent the network from correctly delivering the packets. The malicious nodes can announce incorrect routing updates which are then propagated in the network, or drop all the packets passing through them.

In order to protect the packet delivery functionality, each SCAN node overhears the wireless channel in the promiscuous mode, and monitors the routing and packet forwarding behavior of its neighbors at all time. The monitoring results at different nodes in a local neighborhood are cross-validated. A malicious node is convicted when its neighbors have reached such a consensus, then it is deprived of the network membership and isolated in the network. In order to enforce the network access, each legitimate node carries a valid token which certified, unexpired, and not revoked, while any node without a valid token is denied of participation in the network operations. A legitimate node can always

renew the token from its neighbors before its current token expires. However, when a malicious node is convicted, its neighbors collectively revoke its current token and inform all other nodes in the network. The above SCAN framework which has the following three components:

- *Collaborative Monitoring*: all nodes within a local neighborhood collaboratively monitor each other.
- *Token Renewal:* all legitimate nodes in a local neighborhood collaboratively renew the tokens for each other.
- *Token Revocation:* the neighbors of a malicious node, upon consensus, collaboratively revoke its current token.

E. MaxProp: Routing For Vehicle-Based DTNs

DTNs can be based on moving nodes such as vehicles or pedestrians. Vehicles can provide substantial electrical supplies and transport bulky hardware, which may be inappropriate for use by non-mechanized peers. The disadvantage of a vehicle based network is that the nodes move more quickly, reducing the amount of time they are in radio range of one another. Accordingly, one limited resource in a vehicle-based DTN is the duration of time that nodes are able to transfer data between one another as they pass. Storage can be a limited resource as well.

The MaxProp protocol[11] uses several mechanisms in concert to increase the delivery rate and lower latency of delivered packets. MaxProp uses several mechanisms to define the order in which packets are transmitted and deleted. At the core of the MaxProp protocol is a ranked list of the peer's stored packets based on a cost assigned to each destination. The cost is an estimate of delivery likelihood. In addition, MaxProp uses acknowledgments sent to all peers to notify them of packet deliveries. MaxProp assigns a higher priority to new packets, and it also attempts to prevent reception of the same packet twice.

F. 2ACK Scheme

In 2ACK scheme [4] the sending node waits for an ACK from the next hop of its neighbor to confirm that the neighbor has forwarded the data packet. Such a 2ACK transmission takes place for only a fraction of data packets, but not all. Such a selective acknowledgment is intended to reduce the additional routing overhead caused by the 2ACK scheme. However, this technique is vulnerable to collusions, i.e., the neighbor can forward the packet to a colluder which drops the packet. Although end-to-end ACK schemes are resistant to such colluding attacks, the ACK packets may be lost due to the opportunistic data delivery in DTNs. In DTNs, one serious routing misbehavior is the black hole attack

G. Social Selfishness Aware Routing (SSAR)

Social Selfishness Aware Routing (SSAR) [8] algorithm to cope with user selfishness and provide good routing performance with low transmission cost. But it considers only selfish routing behavior. It does not consider the misbehavior of malicious nodes whose goal is not to maximize their own benefits but to launch attacks.

H. Mitigating Misbehavior Using Contact Records

In [1] the misbehaving node is required to generate a contact record during each contact and report its previous contact records to the contacted node. Based on the reported contact records, the contacted node detects if the misbehaving node has dropped packets. The misbehaving node may misreport to hide its misbehavior, but forged records cause inconsistencies which make misreporting detectable. To detect misreporting, the contacted node also randomly selects a certain number of witness nodes for the reported records and sends a summary of each reported record to them when it contacts them.

In our work we propose tracer routing combined with a peer-ID based signature scheme, it can offer the initiator of each query to identify malicious nodes. A key feature of our scheme from other protocols is that alternate routing is constructed only detecting malicious nodes.

III. CONCLUSION

DDoS attacks are probably the most ferocious threats to the integrity of the Internet. Selfish and routing misbehavior of nodes causes the most attack in DTNs. When one or more nodes are malicious, they may prevent correct message routing. Alternate routing paths can be used to circumvent them. The tracer routing, an efficient routing strategy designed to control the routing path while reducing the normal routing latency is proposed. We propose to address routing message attack by combined tracer routing with Peer- ID based signature scheme.

REFERENCE

[1] Qinghua Li, Guohong Cao, "Mitigating Routing Misbehavior in Disruption Tolerant Networks", IEEE Transactions On Information Forensics And Security, Vol. 7, No. 2, April 2012.

[2] Y. Ren, M. C. Chuah, J. Yang, and Y. Chen, "Detecting wormhole attacks in delay tolerant networks", IEEE Wireless Commun. Mag., vol. 17, no. 5, pp. 36-42, Oct. 2010.

[3] F. Li, A. Srinivasan, and J. Wu, "Thwarting blackhole attacks in distruption-tolerant networks using encounter tickets", in Proc. IEEE IN- FOCOM , pp. 2428-2436.2009

[4] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, " An acknowledgment-based approach for the detection of routing misbehavior in MANETs ", IEEE Trans. Mobile Comput. , vol. 6, no. 5, pp.536-550, May 2007.

[5] S. Marti, T. J. Giuli, K. Lai, and M. Baker, " Mitigating routing misbehavior in mobile ad hoc networks", in Proc. ACM MobiCom,2000, pp. 255-265.

[6] H. Yang, J. Shu, X. Meng, and S. Lu, "Scan: Self-organized network-layer security in mobile ad hoc networks", IEEE J. Sel. Areas Commun.,vol. 24, no. 2, pp. 261273, 2006.

[7] J. Burgess, G. D. Bissias, M. Corner, and B. N. Levine, " Surviving attacks on disruption- tolerant networks without authentication", in Proc. ACM MobiHoc,, 2007, pp. 6170.

[8] Q. Li, W. Gao, S. Zhu, and G. Cao, " A routing protocol for socially selfish delay tolerant networks", in Ad Hoc Networks, ,Aug. 2011, DOI: 10.1016/j.adhoc.2011.07.007.

[9] D. Johnson, D. A. Maltz, and Broch. "The Dynamic Source Routing Protocol for Mobile Ad Hoe Networks", Mobile Ad-hoc Network (MANET) Working Group, IETF, , October 1999.

[10] K. Fall, "A delay-tolerant network architecture for challenged internets", in Proc. SIGCOMM, 2003, pp. 2734.

[11] J. Burgess, B. Gallagher, D. Jensen, and B. Levine, "Maxprop: Routing for vehicle-based disruption-tolerant networks," in *Proc.IEEE INFOCOM*, 2006, pp. 1–11.

[12]L. Buttyan and J.-P. Hubaux, "Enforcing Service Availability in Mobile Ad-Hoc WANs," Proc. MobiHoc, Aug. 2000.

[13]J. P. Hubaux, T. Gross, J.-Y. LeBoudec, and M. Vetterli, "Toward Self-Organized Mobile Ad Hoc Networks: The Terminodes Project," IEEE Comm. Magazine, Jan. 2001.

[14]S. Buchegger and J.-Y. Le Boudec, "Performance Analysis of the CONFIDANT Protocol: Cooperation of Nodes, Fairness in Dynamic Ad-Hoc Networks," Proc. MobiHoc, June 2002.

[15]S. Zhong, J. Chen, and Y.R. Yang, "Sprite: A Simple, Cheat-Proof, Credit-Based System for Mobile Ad-Hoc Networks," Proc. INFOCOM, Mar.-Apr. 2003.

[16]M. Jakobsson, J.-P. Hubaux, and L. Buttyan, "A Micropayment Scheme Encouraging Collaboration in Multi-Hop Cellular Networks," Proc. Financial Cryptography Conf., Jan. 2003.