www.ijiarec.com

ISSN:2348-2079 Volume 3 Issue 8

International Journal of Intellectual Advancements and Research in Engineering Computations

ROUTING AND MISBEHAVIOUR DETECTION MECHANISM IN DISRUPTION TOLERANT NETWORKS (WSN)

Manojkumar.K[1], A.Viswanathan[2]

ABSTRACT

Network security has focused primarily on protecting communication and network resources. It involves the authorization of access to data in a network which is controlled by a network administrator. Security incidents are rising at an alarming rate every year. As the complexity of the threats increase, so do the security measures required to protect networks. Denial of Service (DoS) attacks constitutes one of the major threats and among the hardest security problems in today's Internet. DoS are 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.

INTRODUCTION

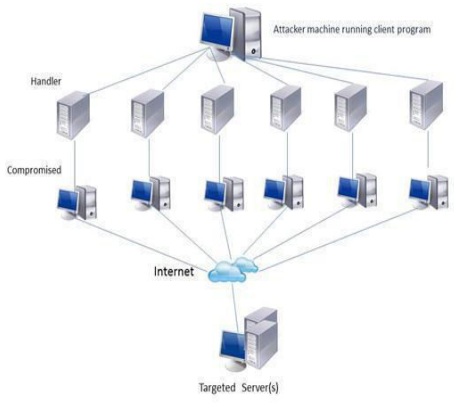
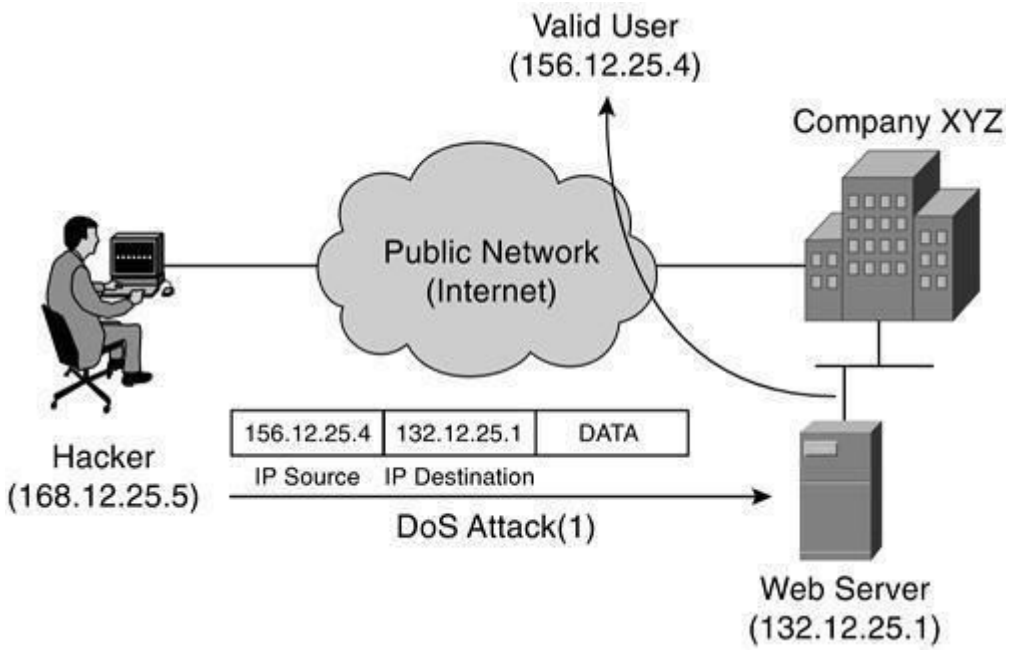


Fig 1.1 A conceptual diagram of DDoS attack

DDoS attacks are probably the most ferocious threats to the integrity of the Internet. It poses 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.

Author for Correspondence:
[1]Research Scholar, Annamalai University, Chidambaram, Tamilnadu, India. .Email: manojkumar.k@hotmail.com
[2]Professor, Annamalai University, Chidambaram, Tamilnadu, India. Email Idyoursvichu@gmail.com



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.

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 [6]. MaxProp is a good point of departure because it offers better throughput than several other strategieslike Random, FIFO, 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. Several techniques have been proposed to detect and alleviate the effects of such selfish nodes in MANETs [14], [10], [7], [13], [15], [11]. In [14] two extensions to the Dynamic Source Routing algorithm (DSR) [2] to mitigate the effects of routing behavior are proposed: watchdog and path rater. 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 . When a node forwards a packet, the node ś 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. 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.

2.1 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.

2.2 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[16], 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.

2.3 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.

2.4 Self-Organized Network-Layer Security

In SCAN [4], 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.

2.5 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 [5] 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.

2.6 2ACK Scheme

In 2ACK scheme [9] 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 seriousrouting misbehavior is the black hole attack

2.7 Social Selfishness Aware Routing (SSAR)

Social Selfishness Aware Routing (SSAR) [12] 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.

2.8 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.

PROPOSED SYSTEM

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.

3.3 MODULES

1 Userinterface Design

2 Routing Model
3 Security Model
4 Record Summary and Contact Record
5 Witeness Node-Misreporting Detection
6 Black List

3.3.1 Userinterface Design

The goal of user interface design is to make the user's interaction as simple and efficient as possible, in terms of accomplishing user goals—what is often called user-centered design. Good user interface design facilitates finishing the task at hand without drawing unnecessary attention to it. Graphic design may be utilized to support its usability. The design process must balance technical functionality and visual elements (e.g., mental model) to create a system that is not only operational but also usable and adaptable to changing user needs.

3.3.2 Routing Model

The routing protocol used in a DTN strongly influences the security properties of the system. We nominally identify two characteristics in routing protocols: criterion and style. The criterion refers to the process by which neighboring nodes are passed packets; specifically, we consider metric based and random criteria. The style indicates whether the protocol is replicative or forwarding.

3.3.3 Security Model

Our goal is to determine how the network performance ofa DTN degrades when no authentication protocol is used. This depends on starting with a set of assumptions about thesecurity model and what attacks we consider. We recognizethat one can construct a different set of assumptions thatwill cause the DTN to perform extremely poorly even witha small number of attackers. For instance, if node mobilityis extremely low, and one node forms a nexus for all routingpaths, the DTN will fail to deliver packets after corruptingthat node. Similarly, if one attacker can corrupt all nodesby flooding an area with RF noise, the DTN will also fail.Rather, it is our intention to show that at least some DTNshave mobility patterns that perform extremely well underattack, and before applying the complexity of an authorizationmechanism, one should consider whether the networkreally requires it.

We have chosen to use a security model that provides aconvincing case for the robustness of DTNs. This modelincludes several elements.Identity: In a DTN environment without authentication,no assumptions can be made about the identities or intentionsof other peers. Moreover, attackers can spoof their MAC layeraddresses to appear to be any node at any time, includingthe destination of packets.

Attack types: There are two forms of the parasite attack:node corruption and tailgating. Under node corruption, anattacker has completely taken over a node and can commandit to create and drop packets at will. In some settings, thisattack can include physical destruction of the target node.The tailgating attacker is external to the uncorrupted node,but can arbitrarily give it extra packets to forward, spoofoutgoing packets, or selectively interfere with the deliveryof packets during connection opportunities. The tailgatingattacker is as powerful as node corruption since the effect ofboth is identical.

Given this security model, a number of attacks are possible.To simplify analysis, we focus on a set of actions that are fundamentalto any attack. These four actions are detailed below in the context of DTN transfer opportunities: exchangingpackets, exchanging routing tables, and exchanging acknowledgments.When a network is restricted to authenticated,authorized participants, one would expect these attacks areavoided or at least attributable to some entity.

- Dropping all packets
- Flooding of packets
- Routing table falsification
- Counterfeit acknowledgments of delivery

3.3.4Contact Records

The two nodes also exchange their current vector of buffered packets (as a step of contact record generation). In this way, one node knows the two sets of packets the other node buffers at the beginning of the previous contact and the beginning of the current contact, which are denoted by and , respectively. It also knows the two sets of packets the other node sends and receives in the previous contact, which are denoted by and a misbehaving node may drop a packet but keep the packet ID, pretending that it still buffers the packet.

The next contacted node may be a better relay for the dropped packet according to the routing protocol, which can be determined when the two exchange the destination (included in packet ID) of the buffered packets. In this case, the misbehaving node should forward the packet to the next contacted node, but it cannot since it has dropped the packet. Thus, the next contacted node can easily detect this misbehavior and will not forward packets to this misbehaving node.

3.3.5 Witness Node

Detection: To detect the inconsistency caused by misreporting,for each contact record generated and received in a contact,a node selects random nodes as the witness nodes of thisrecord, and transmits the summary of this record to them whenit contacts them. It selects the witness nodes from the nodes thatit has directly contacted. Here, the nodes contacted a long timeago are not used since they may have left the network.

Alarm: After detection, the witness node floods an alarmto all other nodes. The alarm includesthe two inconsistent summaries. When a node receivesthis alarm, it verifies the inconsistency between the includedsummaries and the signature of the summaries. If the verificationsucceeds, this node adds the appropriate misreporting nodeinto a blacklist and will not send any packets to it. If the verificationfails, the alarm is discarded and will not be further propagated.A misreporting node will be kept in the blacklist for acertain time before being deleted.

A node deletes the record that it generates in a contact afterthe contact has been purged out of its report window, probablyafter a few contacts. It deletestherecordsreceivedfromthe contactednode right after this contact, since these received recordsare only used to check if the contacted node has dropped packetsrecently.The witness node should keep its collected record summariesfor a long enough time to detect misreporting. For simplicity,our scheme uses a time-to-live parameter, which denotesthe time for the collected summaries to be stored before beingdeleted

.

3.3.6 Black List

To mitigate routing misbehavior, we try to reduce the numberof packets sent to the misbehaving nodes. If a node is detectedto be misreporting, it should be blacklisted and should not receivepackets from others. We cannot simply blacklist it because it is droppingpackets, since a normal node may also drop packets due tobuffer overflow. In the following, we focus on how to mitigaterouting misbehavior without affecting normal nodes too muchwhen misbehaving nodes do not misreport.

Our basic idea is to maintain a metric *forwarding probability(FP)* for each node based on if the node has dropped, receivedand forwarded packets in recent contacts, which can be derivedfrom its reported contact records. The nodes that frequently droppackets but seldom forward packets will have a small FP andwill receive few packets from others. Our scheme borrows ideas from congestion control to update FP. More specifically, it combinesadditive increase, additive decrease, and multiplicativedecrease to differentiatemisbehaving nodes fromnormal nodes.

3.4 PROBLEMDEFINITION

To transfer the data packet from source to destination commonly user TCP/IP protocol in networking. In this TCP/IP process is before transfer the data the connection has been established. Each node forwards the query to the next node. During the lookup process no information is send back to the originator, resulting in less packet overhead. To make the routing strategy perform best, we present an efficient routing strategy, called tracer routing. Tracer routing enables the initiator to trace the whole routing process.

Disruption tolerant networks (DTNs) exploit the intermittent connectivity between mobile nodes to transfer data. Due to a lack of consistent connectivity, two nodes exchange data only when they move into the transmission range of each other (which is called a *contact* between them). 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. Routing misbehavior can be caused by selfish nodes that are unwilling to spend resources such as power and buffer on forwarding packets of others, or caused by malicious nodes that drop packets to launch attacks.

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.

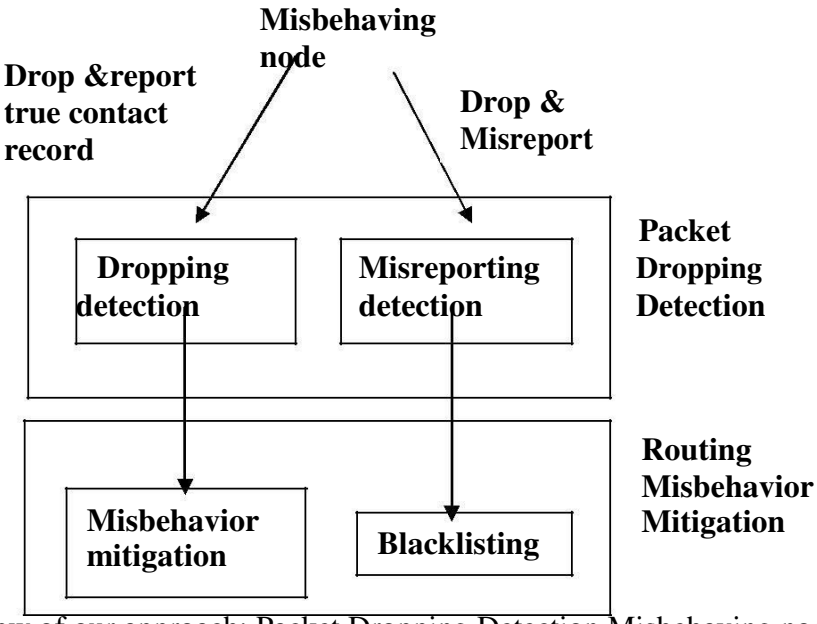


Fig 3.3 Overview of our approach: Packet Dropping Detection Misbehaving node M reports two forged contact records R and R‘ which are inconsistent

The misbehaving node [in Fig. 2.2] 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 misbehavingnode 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. The witness node [in Fig. 2.2] that collects two inconsistent contact records can detect the misreportingnode.

ALGORITHM FOR FORWARDING PROBABILITY

Algorithm 1 :FP Update (run by $N_i$when it contacts N_j)

Require: The gauge list *GL*that $N_i$maintains fromN_j

Require: The *r*nodes $N_x(1 \leq x \leq r)$ contacted by$N_j$in its report window

Require: *drop* = FALSE, *receive*= FALSE, *forward*= FALSE

Require: $0 < \delta < 1$, $0 \leq \rho < 1$

1: Delete the two oldest elements of*GL*

2: Insert $N_x(1 \leq x \leq r)$ into*GL*

3: **if** $N_x$is the most-frequent element of *GL*but notN_i itself **then**

4: Tag $N_x$as *special*

5: **else**

6: Tag $N_x$as *plain*

7**: end if**

8: **if**$N_j$has dropped packets in the report window **then**

9: *drop*= TRUE

10: **end if**

11: **if** $N_j$has received packets from a *plain* node (N_x)**then**

12: *receive*= TRUE

13: **end if**

14: **if** $N_j$has forwarded packets to a *plain* node (N_x)**then**

15: *forward*=TRUE

16: **end if**

17: **if***drop*== TRUE

18: $\gamma = \gamma . \rho$

19: **else if** *receive*== TRUEor*forward* ==TRUE

20: $\gamma = \min\{\gamma + \rho, 1\}$

21: **else**

22: $\gamma = \max\{\gamma - \rho, 0\}$

23: **end if**

CONCLUSION AND FUTURE SCOPE

CONCLUSION

In this project, we presented a scheme to detect packet dropping in DTNs. The detection scheme works in a distributed way; i.e., each node detects packet dropping locally based on the collected information. Moreover, the detection scheme can effectively detect misreporting even when some nodes collude. Analytical results on detection probability and detection delay were also presented. Based on our packet dropping detection scheme, we then proposed a scheme to mitigate routing misbehavior in DTNs. The proposed scheme is very generic and it does not rely on any specific routing algorithm. Trace-driven simulations show that our solution are efficient and can effectively mitigate routing misbehavior.

Peer-to-peer overlay networks, both at the network layer and at the application layer. We have shown how techniques ranging from cryptography through redundant routing to economic methods can be applied to increase the security, fairness, and trust for applications on the p2p network. Because of the diversity of how p2p systems are used, there will be a corresponding diversity of security solutions applied to the problems has presented the design and analysis of techniques for secure node joining, routing table maintenance, and message forwarding in structured p2p overlays. These techniques provide secure routing, which can be combined with existing techniques to construct applications that are robust in the presence of malicious participants.

REFERENCES

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

[3] F. Li, A. Srinivasan, and J. Wu, ―Thwarting blackhole attacks in distruption-tolerant networks using encounter tickets‖, in Proc. IEEE IN-FOCOM , pp. 24282436.2009

[4] 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.

[5]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.

[6] 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.

[7]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.

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

[9] 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. 536550, May 2007.

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

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

[12] 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.

[13]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.

[14] S. Marti, T. J. Giuli, K. Lai, and M. Baker, ― Mitigating routing misbehavior in mobile ad hoc networks‖, in Proc. ACM MobiCom,2000, pp. 255265.