The International Journal of Engineering And Science (IJES)
||Volume|| 2 ||Issue|| 1 ||Pages|| 67-75 ||2013||
ISSN: 2319 – 1813 ISBN: 2319 – 1805

Detection of Routing Attacks in Disruption Tolerant Networks

[1]Sangeetha.R, [2]Krishnammal.N

[1]Department of Computer Science, Sri Shakthi Institute of Engineering and Technology, Coimbatore, India
[2]Department of Information Technology, Sri Shakthi Institute of Engineering and Technology, Coimbatore, India

ABSTRACT

Disruption tolerant networks (DTN) differ from other networks in such a way that they provide inconsistent connectivity between the nodes in order to exchange the data. Due to the inconsistent connectivity the data is exchanged only when the nodes come in contact with each other. DTN performs store-carry-forward method. When a node receives a packet it stores the packet first in the buffer and then carries until it contacts another node. After the two nodes are in contact the packet is forwarded to the next node. This system detect the packet dropping and to limit the traffic flowing to the misbehaving node. To detect the packet dropping in DTN the distributed scheme is introduced in which a node is selected that contains the signed contact records of its previous contact. Based on this record the next node in contact can detect the node that had dropped the packet. Also a node that is compromised may misreport a false record so that the packet dropping cannot be detected. In order to avoid this, the contact record is distributed to few witness nodes which then can detect the node that has dropped the packet. SimBet is a forwarding-based algorithm where a packet only has one replica. A packet is forwarded to a node if that node has higher metric than the current node. Delegation is a replication-based algorithm where a packet may have multiple replicas. The packet is replicated based on the usage of the neighbour node. The communication cost can be reduced. Such routing misbehavior can increase the packet delivery ratio and does not waste system resources such as power and bandwidth.

Keywords— *Disruption tolerant network, Routing , Attacks, Security, Detection.*

Date of Submission: 19, December, 2012 ⟺ Date of Publication: 05, January 2013

I. INTRODUCTION

Disruption tolerant network (DTN) do not provide continuous connectivity between the nodes in the network. Due to the lack of connectivity the nodes are unable to exchange the packets frequently. The nodes can transfer the packet only when two nodes come in contact with each other. Disruption tolerant network usually follows store–carry-forward method.

The nodes in disruption tolerant network misbehaves by dropping the packet it receives and informs that it has not received any packets. Otherwise the selfish nodes do not spend the available resources such as buffer and power in forwarding the packets of the previous nodes. Routing misbehaviour occurs by dropping the packets even if the node has sufficient power and buffer to store.

The routing misbehavior can be detected by introducing two algorithms. SIMBET AND DELEGATION are the two algorithms in which the misbehavior in routing can be detected. Simbet is the algorithm based on forwarding. Delegation is the algorithm based on replication.

In this paper the packet dropping is detected and the misbehaving nodes are blacklisted such that they do not receive any packet nor send any packet. The packet dropping is detected by the contact records that contains the information about the nodes previous contacts and the information about the node that it is going to contact and many other information. The contact records itself may contain false records. The misbehaving contact record can be detected by sending the part of contact record to the randomly selected nodes.

In disruption tolerant networks the packet may be dropped if the buffer is full. In order to identify the difference between the packet dropped due to the buffer overflow and the packet dropped due to the misbehavior , the contact records are used. The contact record contains the information like the packets sent, packets received, the sequence number and transmission options.

In mobile and ad-hoc networks the packet dropping is detected by monitoring the neighbour nodes and acknowledgment schemes. The packet dropping is detected in a distributed manner.

In distributed scheme the node that contains the previous contacts are forwarded to the next node that comes into contact. The information about the buffer and the packets sent and received are transmitted to the next node.

If the contact record is being attacked then the part of it are stored randomly and finally the node that is misbehaving is pushed into the blacklist such that it neither receives any packet nor can transmit and packet. A node generates a contact record and reports its previous contact to the next contacted node. If misbehavior happens in contact record ,the copy of the contact record is sent to the witness nodes.

II. Related Work

Routing misbehavior takes place in mobile ad hoc networks when the node agrees to forward the packet but does not. In order to avoid this misbehavior two approached are applied. They are watchdog and path rater. The watchdog monitors the neighbour nodes weather they forward the packet or not. The path rater finds the best path and also avoids the misbehaving nodes from forwarding packets.

Routing in disruption tolerant network is very difficult. In order to make routing effective a protocol called MAXPROB is proposed. The protocol is based on priority wise. The prioritization is based on the duration, storage, message delivery, history of the nodes etc. Priority is also based on scheduling of packets to be transmitted and scheduling of packets to be dropped.

Detecting the wormhole attacks in delay tolerant networks is a tedious process. Wormhole attack refers to the malicious node that forwards the packet to the next colluding node and damages the network. In order to detect the wormhole attack two schemes were proposed. They are Random Way Point and Zebranet mobility models.

The node replication attacks in sensor networks are detected in distributed manner. The node replication attacks are attacks that replicate the node and produces in the network. It also causes more disconnections in the network. Two algorithms are proposed to detect this attack. They are Randomized Multicast distributes node location information to randomly-selected witnesses, exploiting the birthday paradox to detect replicated nodes.

Data forwarding in delay tolerant networks is very challenging. Data forwarding is not much effective in delay tolerant networks. To efficiently forward the data we exploit transient contact patterns. Some nodes in DTNs may remain connected with each other during specific time periods to form transient connected subnets despite the general absence of end-to-end paths among them.

For example, a student remains connected with his classmates during the class and they form a TCS during that time period. Similarly, vehicles also form a TCS when they are waiting for the traffic light at the cross roads .

Mobile Ad-hoc networks are self-configuring and self-organizing multi hop wireless networks where, the network structure changes dynamically. To detect the routing misbehavior in MANETS, 2acknowledgement based approach is used. In this approach when a data travels for two hops ,acknowledgement is sent.

Data is disseminated based on the interest of the node in delay tolerant mobile networks. The interest of a node may be weather forecast, event alerts, commercial advertisement, movie trailers, blog updates, and various news. The source interest refers to generating the data messages that match the corresponding interest. A sink of an interest is a node that wishes to acquire and consume data messages that match the corresponding interest. Lack of continuous connectivity of the network is one of the major problem in delay tolerant networks.

Multicasting the data is very difficult in delay tolerant networks due to frequent partitioning. In this paper they have proposed a forwarding algorithm called delegation forwarding to handle the delay tolerant networks multicast and develop several multicast forwarding algorithms. The delegation forwarding algorithm is also compared with the single copy multicasting and multiple copy multicasting.

III. Preliminaries

A. Network and routing model

The nodes in disruption tolerant network contains two buffers in which one buffer stores its own packets and the other buffer is used for storing the packets from other nodes. The network is synchronized loosely such that the nodes can come into contact for a short period of time.

When the nodes come in contact they exchange messages .The network is designed in such a way that the nodes come in contact exchange the packets.

B. Security model

The malicious nodes drops the packet even if they have enough space in memory. The normal nodes will drop the packet only if the buffer if full. The misbehaving node will not allow to drop its own packets. Each node in DTN has a certain lifetime. If the lifetime of the packet has expired then the packet has to be dropped. The expired packets can be detected if the source specifies the lifetime of the packet along with the packet it sends.

C. Overview of the approach

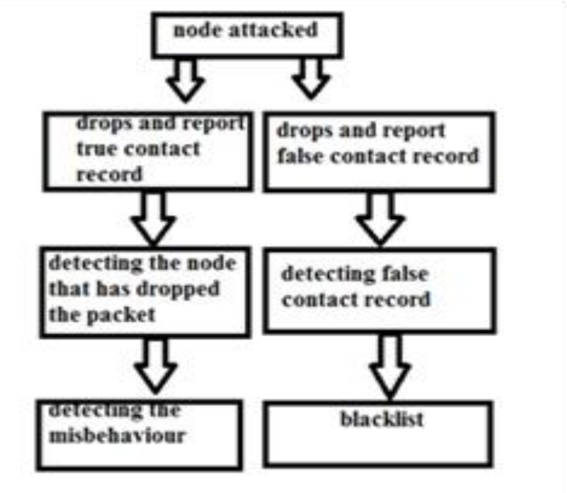
node attacked
drops and report true contact record
drops and report false contact record
detecting the node that has dropped the packet
detecting false contact record
detecting the misbehaviour
blacklist

Fig1. Packet Dropping Detection

The approach has two schemes. Packet dropping detection and routing attacks are detected in our scheme. The packet is detected by generating the contact records.

A node generates its previous contact records and reports it to the other node. The contact record itself generates a false records .The false records will be detected by the witness nodes where the part of the contact record is distributed randomly to the set of nodes.

A misbehaving node may drop the packet and report a true contact record or drop the packet and report the false contact record. A misbehaving node that reports the true contact record is detected and the misbehaviour is detected. A node that reports false contact record is blacklisted. The part of the contact record is reported to the witness nodes if a node is being detected.

The contact record contains the information like when the contact record had happened and the packets sent ,packets received and the sequence number . A misbehaving node drops the packet but keeps the ID of it in order to show that they have forwarded the record. Two algorithms are used to detect the misbehavior. The summary of the contact record is generated to the witness nodes.

By detecting the nodes the network performance can be increased and message delay also can be reduced. The packet delivery ratio can be increased. The misbehaving node overhead can be reduced. The node that has been attacked either drop and report true contact record or drop and report false contact record. The node that drops and report the true contact record is detected by analyzing the contact record details. Thus the misbehavior is detected.

The node that drops the packet and report the false contact record is detected and blacklisted such that they do not receive any packets and neither send packets.

IV. Packet Dropping Detection

Each node contains its own buffer. The node when received the packet it stores in its buffer. The malicious node drops the packet but it informs the next contacted node that it had not received any packets. Detecting the misbehavior is done by simbet and delegation algorithms. The simbet is a forwarding based algorithm and delegation is a replication based algorithm. The packet is forwarded according to the metrices like packet delivery ratio number of wasted transmissions, bytes transmitted per packet, detection rate, detection delay.

1. Packet delivery ratio:
Packet delivery ratio deals with number of packets delivered.

2. Number of wasted transmissions:
Deals with wastage of power and other resources

3. Bytes transmitted per packet:
Deals with number of bytes transmitted per packet

4. Detection rate:
It deals with the number of malicious node detected.

5. Detection delay:
The delay in sending and receiving the packets are detected.

V. Analysing The Conact Record

The contact record is analyzed by viewing the details in it. The misbehavior in contact record can be detected by sending the part of contact record to the witness nodes who are responsible for viewing the activities in the network. If the details in forged contact record and the details in contact record stored in witness nodes differs, then the forgery in contact record can be detected.

VI. Routing Algorithms

When the routing algorithm simbet is used , it decreases the delivery ratio as the number of malicious nodes increases. The number of packets used for forwarding are less when simbet is used. When the number of malicious nodes increases then more number of packets are dropped. The number of hops traversed by the packet becomes less.

When the routing algorithm delegation is used, the packet delivery ratio increases as the number of malicious node increases. In this algorithm the nodes are replicated such that the communication cost can be reduced. When the replicated packet is passed to the malicious node then the probability of replicating the packets gets reduced.

The destination node can easily receive the packets when it is replicated.

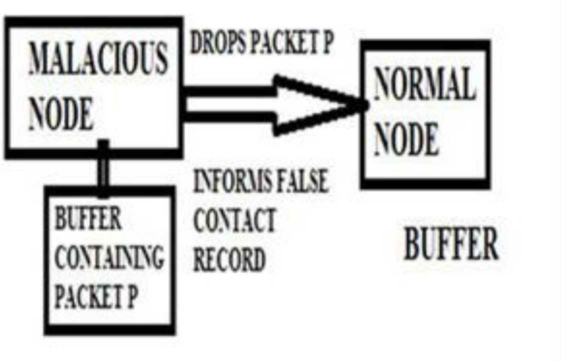

Fig 2. Analyzing the Contact Record

When the routing algorithm delegation is used, the packet delivery ratio increases as the number of malicious node increases. In this algorithm the nodes are replicated such that the communication cost can be reduced. When the replicated packet is passed to the malicious node then the probability of replicating the packets gets reduced.

The destination node can easily receive the packets when packets are replicated. The storage cost can be reduced by deleting the packets when not necessary. Thus the algorithm increases the performance by reducing the number of malicious nodes as possible and blacklisting them. Detecting the false records can be done by analyzing the sequence numbers whether they are in proper order.

VII. False Reporting Detection

A. Reproduction of the old record

A malicious node cannot forge the contact record when there is no collision. Only when collision occurs the false record can be reported . The compromised node cannot modify the true contact record since it is signed by the previous node that was in contact.

B. Selection of Witness node

Due to false reporting, the inconsistency is caused. In order to avoid the inconsistency that has been caused the witness nodes are selected in random where the whole information about the misbehaving node is sent and analysed. The witness nodes that are directly in contact are selected. The old witness nodes are not selected because they might have left the network. The witness node by receiving the information will compare it with the already existing information and verify whether the signer has involved in violation by not following the rules.

C. Rules to avoid inconsistency

1. The inconsistency can be avoided by assigning the sequence numbers to each contact record. The first generated contact record can be given the sequence number initially.
2. The record that has less contact time will also have smaller sequence number.

D. Alarm

The witness node upon sending the alarm signal to the corresponding nodes, the nodes verify it by comparing the included information and signature information. Upon verification of the information by the nodes, the nodes come to the conclusion that the node is a malicious node and sends it in to the blacklist and the blacklisted node cannot receive any more messages and neither can send messaged to the other nodes. Thus the misbehavior can be detected. The node will be kept in the blacklist for certain amount of time and then deleted in order to avoid less memory space.

VIII. Collision Avoidance

A. False report with collision

The malicious node drops the packet and reports the true contact record. The misbehavior of such nodes can be detected. If the node reports false record inorder to avoid the detection of dropping, it forwards the packet to the next colluder. Both the colluding nodes can hide the dropping from being detected in several ways The dropping can be detected by analyzing the sequence number. When two nodes come into contact they exchange the information through a contact record and detect the misbehavior.

A node may drop a packet if the buffer becomes full. A node may drop a packet when the lifetime of the network is over. These dropping cannot be misbehavior.

B. Duplicate buffer

The forge buffer is used to hide the packet being dropped. When a normal node comes in contact with the misbehaving node and colluder node, the colluder cannot view the long history of the previous records. In order to overcome this problem, each node has to report more than one previous contact records to the next node.

C. Duplicate Not active

In duplicate inactive the node is allowed to forward the packet only to an active node. The active node is a node that behaves normal. When this rule is not followed by a particular node, the node is considered to be malicious node and placed inside the blacklist where it remains idle and later deleted from it.Each node maintains an active table that contains the list of active nodes that it knows from its local knowledge.

D. Duplicate transactions

The node deletes the contact record as soon as the record reaches its destination. Therefore the packet delivery ratio can be increased and inconsistencies can be reduced and the collision can be avoided. The destination node can easily receive the packets when packets are replicated. The storage cost can be reduced by deleting the packets when not necessary.

The algorithm increases the performance by reducing the number of malicious nodes as possible and blacklisting them. Detecting the false records can be done by analyzing the sequence numbers whether they are in proper order.

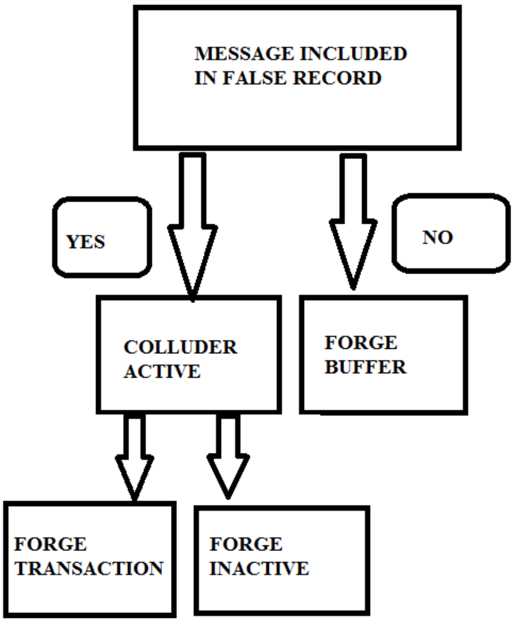

Fig 3. Detection of Colluder

IX. Conclusion

Due to the inconsistent connectivity the data is exchanged only when the nodes come in contact with each other. DTN performs store-carry-forward method. When a node receives a packet it stores the packet first in the buffer and then carries until it contacts another node. After the two nodes are in contact the packet is forwarded to the next node. This system detect the packet dropping and to limit the traffic flowing to the misbehaving node. To detect the packet dropping in DTN the distributed scheme is introduced in which a node is selected that contains the signed contact records of its previous contact. Based on this record the next node in contact can detect the node that had dropped the packet. Also a node that is compromised may misreport a false record so that the packet dropping cannot be detected. In order to avoid this the contact record is distributed to few witness nodes which then can detect the node that has dropped the packet. SimBet is a forwarding-based algorithm where a packet only has one replica. A packet is forwarded to a node if that node has higher metric than the current node. Delegation is a replication-based algorithm where a packet may have multiple replicas. The packet is replicated based on the usage of the neighbor node. The communication cost can be reduced. Such routing misbehavior can increase the packet delivery ratio and does not waste system resources such as power and bandwidth.

X. References

[1] K. Fall, ―A delay-tolerant network architecture for challenged internets,‖ in Proc. SIGCOMM, 2003, pp. 27–34.

[2] 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.

[3] W. Gao and G. Cao, ―User-centric data dissemination in disruption tolerant networks,‖ in Proc. IEEE INFOCOM, 2011, pp. 3119–3127.

[4] E. Daly and M. Haahr, ―Social network analysis for routing in disconnected delay-tolerant manets,‖ in Proc. ACM MobiHoc, 2007, pp. 32–40.

[5] V. Erramilli, A. Chaintreau,M. Crovella, and C. Diot, Delegation forwarding,‖ in Proc. ACM MobiHoc, 2008, pp. 251–260.

[6] N. Eagle and A. Pentland, ―Reality mining: Sensing complex social systems,‖ Pers. Ubiquitous Comput., vol. 10, no. 4, pp. 255–268, 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. 61–70.

[8] 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.

[9] 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. 261–273, 2006.

[10] S. Buchegger and Y. L. Boudec, ―Performance analysis of the confidant protocol (cooperation of nodes: Fairness in dynamic ad-hoc networks),‖ in Proc. MobiHoc, 2002, pp. 226–236.

[11] 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.

[12] B. Awerbuch, D. Holmer, C.-N. Rotaru, and H. Rubens, ―An on-demand secure routing protocol resilient to byzantine failures,‖ in Proc. ACM WiSe, 2002, pp. 21–30.

[13] Y. Xue and K. Nahrstedt, ―Providing fault-tolerant ad-hoc routing service in adversarial

environments,‖ Wireless Pers. Commun., vol. 29, no. 3-4, pp. 367–388, 2004.

[14] P. Hui, J. Crowcroft, and E. Yoneki, ―Bubble rap: Social-based forwarding in delay tolerant networks,‖ in Proc. ACM MobiHoc, 2008, pp. 241–250.

[15] F. Li, A. Srinivasan, and J. Wu, ―Thwarting blackhole attacks in distruption- tolerant networks using encounter tickets,‖ in Proc. IEEE INFOCOM, 2009, pp. 2428–2436.

[16] Y. Ren, M. C. Chuah, J. Yang, and Y. Chen, Detecting wormhole attacks in delay tolerant networks,‖ IEEEWireless Commun.Mag., vol.17, no. 5, pp. 36–42, Oct. 2010.

[17] U. Shevade, H. Song, L. Qiu, and Y. Zhang, Incentive-aware routing in dtns,‖ in Proc. IEEE ICNP, 2008, pp. 238–247.