Analysis of packet dropping, storage issue, security Issue and routing misbehaviour in Disruption Tolerant Networks

R.Sangeetha[1], Dr.R.Vijayabhasker[2]

[1]*Ph.D Scholar, Faculty of information and Communication Engineering, Anna University, Chennai, India*
[2]*M.E.Ph.D, Assistant Professor, Department of Electronics and Communication Engineering, Anna University, Regional centre, Coimbatore, India*

[1]sangeetha.sivakumar13@gmail.com
[2]kaviji04@gmail.com

***Abstract*—Disruption tolerant networks (DTN) are built in such a way that the connection between source and destination does not exist for a long time. DTN transfers the message using store-carry-forward method. When a connection is established between the nodes, the message is forwarded. The four main issues in DTN are identified and the respective approaches are applied inorder to overcome the issues. The four main issues include packet dropping, storage, security and routing misbehaviour. The best approach among the various are identified and implemented. Techniques are identified to balance the buffer in each node. By applying the various techniques, the packet delivery ratio is increased. More number of misbehaving nodes are identified and blacklisted. The storage cost and communication cost is reduced. The system resources are not wasted. Overall the performance of the network is increased.**

Keywords-Disruption Tolerant Networks, Misbehaving node, Blacklist, Packet dropping.

I. INTRODUCTION

Disruption tolerant network(DTN) does not provide end –to-end connectivity between the nodes in the network. The connection between the source and destination does not last for a long time. When the connection is established at a particular time, the packets are exchanged. DTN provides store-carry-forward method. When a node receives a packet it stores the packet in the buffer and then it carries the packet around until the connection is established. Finally the packet is forwarded to the node which is in contact.

The nodes in disruption tolerant network forwards the messages in an open network. Hence security has become the major issue in DTN. The nodes that are compromised can easily drop the packets. The node misbehave by sending the false report. The false report describes that the particular compromised node had sent the packet in the disruption tolerant network. Automatically the number of compromised node increases and thereby decreasing the packet delivery ratio. The solution for decreasing the number of compromised nodes in the DTN network is by generating contact records. The contact records contains information that includes the packets sent, packets received, the sequence number and many other information. The contact records itself becomes false by sending false report to the other nodes. In this case the part of the contact records are sent to the neighbour witness nodes which monitors the network.

Storage is one of the major issue in Disruption Tolerant Network. Each time when a particular node receives a packet, it has to store in its buffer until the node comes in contact with another node. Only when two node contacts each other, the data is forwarded. Normal nodes drop the packet when its buffer is full. The compromised node drops the packet even though it has space in its buffer by acting selfish. The compromised nodes even make changes in the message and then forward them.

The storage overhead can be reduced by detecting the compromised nodes and blacklisting them. The blacklisting stores the packet that cannot participate in the network. The nodes remain ideal and can be permanently deleted after blacklisting them. The messages can be encrypted and forwarded thereby avoiding the message alteration in the network.

Security is also one of the major problem in DTN network. The communication between the nodes are much safer when the technique called Public Key Infrastructure is used. PKI verifies the authenticity of the original sender, the intermediate nodes and the receiver. PKI also verifies the integrity of the message. Although PKI provides good security , it cannot be used where there is no continuous connectivity between the nodes .

Routing misbehaviour is another major issue in DTN networks. Misbehaviour in routing occurs when a node is compromised. The misbehaving node agrees to send the packet but does not send the packet and drops it.

To avoid routing misbehaviour watchdog and pathrator are used. The protocols that includes MAXPROB and ProPHET are used to make effective routing. Though they provide effective routing the network overhead is increased and delivery rate is decreased. The performance of the disruption tolerant network decreases.

II. RELATED WORK

A.Packet dropping:

1.Encounter based routing:

Packet dropping is the most occurring issue in Disruption Tolerant Network. Here the compromised node appears like the better node so that it can reach the destination faster. Encounter based routing protocol has been used to detect the packet dropping. In EBR ,the encounter tickets are exchanged. Each node verifies weather encounter has really occurred by using encounter tickets and the tickets are verified in the network.

2.Ferries:

Ferries are trusted third parties. Ferries are used as monitors that move around the network to monitor the activities of the nodes.

3.Contact records:

Contact records are also used in detecting packet dropping. The contact record is generated by each node in the Disruption Tolerant Network. The contact record contains informations that includes packets sent, packets received, sequence number. The signed contact records are used to verify the authenticity of the message. The false contact records that are generated by each node may be detected by selecting the neighbour witness nodes in the network. The witness nodes receives a part of the contact record and verifies it. It acts as a monitor in the network.

4. Misbehaviour Detection scheme:

Misbehaviour Detection scheme not only detected blackhole attacks but also greyhole attacks. The Blackhole attacks drop the entire message and the Greyhole attack drops only a part of the message which is much more difficult to find. When the two nodes come in contact,the detection scheme is chosen with high detection rate and low false records. Trust based approach is used in detecting the Greyhole attacks. The misbehaving node can be detected by distributing and combining the information from the previous encounters in the network.

5. Packet exchange recording:

When two nodes come in contact, they validate the records by exchanging them. The history of the packet delivery is recorded at each contact of the nodes. By analysing the packet delivery records the blackhole attacks and be detected. Here two approaches are used. One is the Random Way Point and the other is the Zebranet mobility. Both the approaches reduce the misbehaving node. They increase the packet delivery ratio.

B.STORAGE

1.Stream-check method:

Stream-check method is a intrusion detection method used to monitor the network. Flood attack causes the major problem in storage. The method contains two tables that include RATE-LIMIT and DPT-TAB.
The RATE-LIMIT contains the list of certificates of each node. The DPT-TAB helps us to identify weather the attack has occurred or not. The Flood attack can be identified using Streaming method.

The main function of the streaming node in the network is to provide the secret message for decryption process. The packet rate is limited using Rate limit. Request-Response method is used in Rate limit scheme. The DPT-TAB contains the information about the current delivery probability rate.

2.Claim-carry-and-check method:

Network resources are limited in Disruption Tolerant networks. The compromised node causes flood attack by forwarding the packets without any limit. The packets are also replicated without limit by increasing the resource. Claim-carry method sets the limit for each node to forward the packets and sets the limit for replicas it can generate. Detection scheme is proposed to check the rate limit of each node. In this method each node counts the number of packets it has forwarded and the number of replicated packets it has sent. It then claims the count to the other node. The receiving node carries the count until it reaches the destination.

C. Security:

1.µDTNSec: A security layer

µDTNSec layer provides full security to the network. Man-in –the-middle attack and eavesdropping can be avoided and the network can be protected against them.
Asymmetric encryption, signature, elliptic curve cryptography and advanced encryption standards are together implemented.

µDTNSec provides end to end security between the sender and receiver. It provides two important operations that includes Signature only mode for authenticity and sign-then-encrypt mode for both authenticity and confidentiality.

2. Bundle protocol:

Bundle protocols are used in Disruption Tolerant Networks for transferring bundle of data.The protocol is implanted using RFC 5050. Bundle protocol involves more number of nodes in the network that work together to forward large number of data within less time.

D.Routing misbehaviour

1.Onion based anonymous routing:

Onion based routing protocol unables us to protect few informations that includes nodes identities,the location of the destination and routing path which are very sencetive. All the layers in onion protocol are encrypted with secret keys which can be decrypted .

To support limited forwarding of message,the group onions are introduced. Here a group of nodes form a onion group. Any node in the onion group can either encrypt or decrypt the corresponding layers in the network.

2. 2ACK scheme:

In 2ACK scheme, a two hop acknowledgement packet is sent in the opposite direction of the routing path. Here the source node forward the packet to its neighbour node and waits until it receives an acknowledgment stating that the other node had received it and also had forwarded the packet to its corresponding node.

The 2ACK scheme detects the misbehaving node that agrees to forward the packet but does not forward it after receiving the packet.

.

3. Routing algorithms:

SIMBET: It is a forwarding based algorithm. The packets are forwarded based on certain metrics that includes packet delivery ratio, number of wasted transmissions, detection delay and detection rate.

DELEGATION: It is a replication based algorithm where the packet has multiple replicas. The packets are replicated based on the usage of the nodes. By replicating the packets the communication cost can be reduced and packet delivery rate can be increased.

4. Transient contact patterns:

Transient contact patterns are formed when the two nodes come in contact with each other at a specific period of time and exchange messages. For example, the student in the class remains connected with his classmates and they form a Transient contact pattern. The vehicle remains connected with the traffic light and forming transient contact patterns.

5.MAXPROB:

MAXPROB is a protocol used for effective routing. The packets are scheduled first for forwarding and according to the priority,the packets are forwarded. In the same way the packets to be dropped first are scheduled and according to the priority the packets are dropped.The prioritization is based on the historical data, acknowledgments and the list of previous intermediaries. The protocol is based on the hop counts.

The packets with hop count less than the threshold value has the high priority and are transmitted first. The packets with hop count greater than and equal to the threshold value have the low priority and are deleted.

E. Best approach:

The best method among the approaches for overcoming packet dropping is the generation of contact records. The contact records provide high packet delivery ratio when compared to other methods since it provides required information to detect packet dropping.

The best approach for reducing the storage space is to blacklist the packets as it can remain ideal and cannot participate in the network. When the packets are not needed ,they can be permanently deleted. Hence the storage overhead can be reduced.

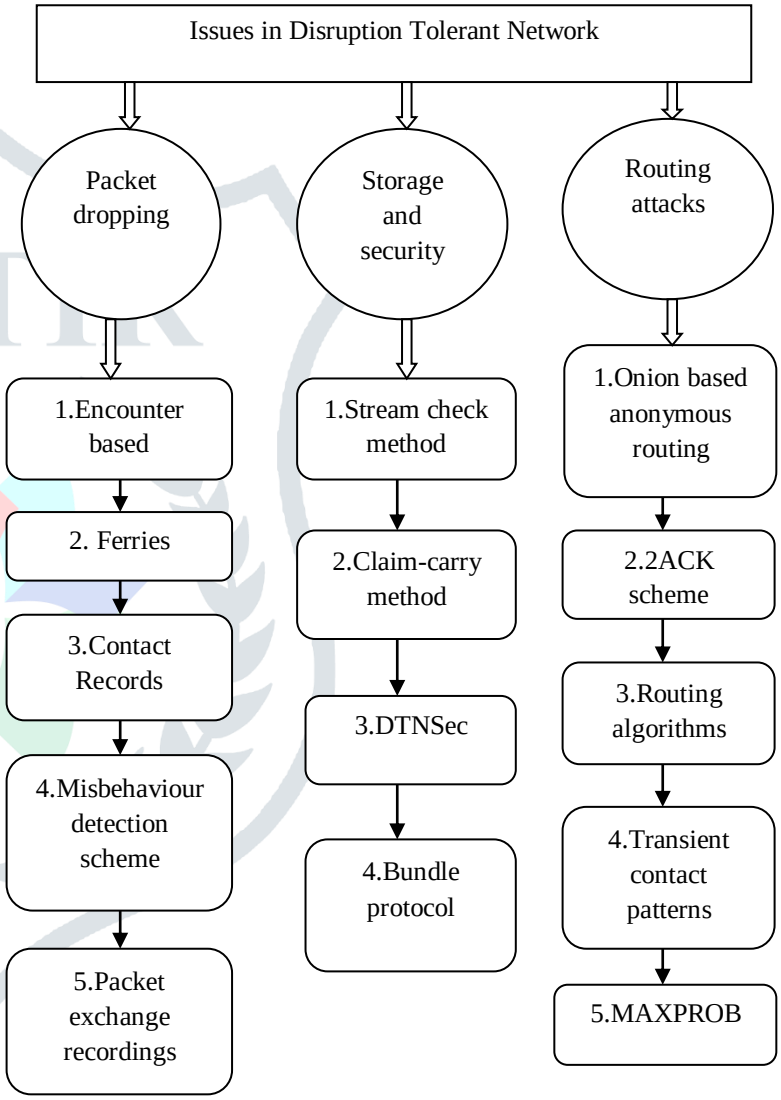
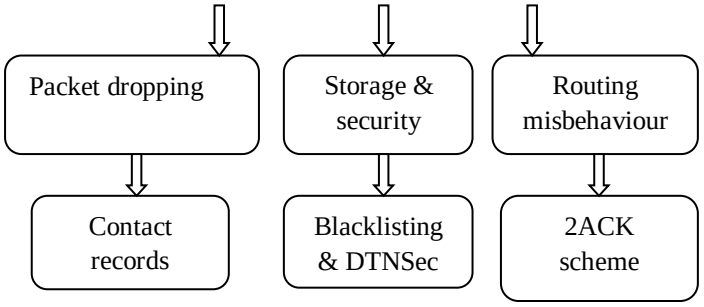


Fig 1: Issues in Disruption Tolerant

The recent best approach for security among them is the µDTNSec that provides maximum security when compared to other techniques. The technique consists of various other security machanisms and also avoids various attacks. Therefore the maximum security can be provided by µDTNSec. The recent best approach for solving routing misbehavior is the 2ACK approach. This method finds out the maximum misbehavior in routing since it follows two hop acknowledgment scheme where each node can receive acknowledgment

packet. The scheme can identify weather each node had forwarded the packet or had dropped the packet.



III. CONCLUSION

The main four issues in Disruption Tolerant Network (DTN) includes packet dropping, storage, security and routing misbehavior. Various new approaches have been identified in recent years to overcome the issues. Approaches that support in reducing the packet dropping includes encounter based routing, ferries, contact records, misbehavior detection scheme and packet exchange record. The best approach among them is contact records since it provides high packet delivery ratio, less number of malicious nodes participating in the network. A new scheme is introduced in detecting the false contact records that includes the selection of witness nodes. The other approaches that avoid storage overhead includes stream-check-method and claim-carry-check method. Both the methods work hard in maintaining the storage issue in DTN. The methods are more helpful in finding out the selfish nodes that do not provide space for the packet in their buffer even though they have enough space in the buffer. Blacklisting provides good result in reducing the storage overhead. The misbehaving nodes are identified and are blacklisted. The nodes in blacklist cannot participate in the network and they do not disturb the network. The issues in providing security to the network can be reduced by applying the techniques that include µDTNSec and the bundle protocol. All the security mechanisms are included in this technique and provides full security. The issues in routing misbehavior can be reduced by applying the approaches that include onion-based anonymous routing, 2ACK scheme, routing algorithms and Transient contact patterns. 2ACK scheme by providing 2 hop acknowledgement, it increases the packet delivery ratio and detects the misbehaving node. Thus the best approaches are identified that improves the performance of the network.

IV. REFERENCE

[1] Dominic Schurmann, "µDTN, A security layer for Disruption tolerant networks in Microcontrollers," in Proc. SIGCOMM, 2017, pp. 27–34.

[2] Kazuya Sakai, B. Gallagher, D. Jensen, and B. Levine, "Performance and security analysis of onion based anonymous routing for delay tolerant networks," in Proc. IEEE INFOCOM, 2015, pp. 1–11.

[3] Kazuya Sakai and Min-Te-Sun, "An analysis of onion basd routing protocol for delay tolerant networks," in Proc. IEEE INFOCOM, 2016, pp. 3119–3127.

[4] Ms Divya Kurikose and Mr.D.Daniel,"Effective defending against flood attack using stream-check method in tolerant networks," in Proc. ACM MobiHoc, 2014, pp. 32–40.

[5] Felipe garay, Erika Rosas,M. Crovella, and C. Diot, "Reliable routing protocol for delay tolerant networks," in Proc. ACM MobiHoc, 2015, pp. 251–260.

[6] Qinghua Li and Wei Gao, "To lie or to comply-Defending against flood attacks in tolerant networks," Pers. Ubiquitous Comput., vol. 10, no. 4, pp. 255–268, 2014.

[7] Yinghui Guo, Sebastain Schildt, M. Corner, and B. N. Levine, "Detecting blackhole attacks and greyhole attacks in delay tolerant networks," in Proc. ACM MobiHoc, 2013, pp. 61–70.

[8] K.Devi, P.Damodharan, K. Lai, and M. Baker, "Detecting misbehavior routing and attacks in delay tolerant networks," in Proc. ACM MobiCom, 2013, 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, 2017.

[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, 2016, 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 2015.

[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, 2012, 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, 2013.