ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014

Secured Data Forwarding Technique in Disruption Tolerant Networks-Survey

D.S.Delphin Hepsiba[1], S.Simla Mercy[2], S.Prabu[3]

PG Scholar, Computer Science and Engineering, S.A.Engineering College, Chennai, India[1,2]

Senior Lecturer, Computer Science and Engineering, S.A.Engineering College, Chennai, India[3]

Abstract: Disruption Tolerant Network is a different type of wireless network. It is a intermittently connected mobile network. Here, at maximum time there does not exist a clear way from source to the destination. It also has a limitation in network resources. The DTN allows transmission only if it is in the transmission range. Because of this limitation there is a chance of dropping the received packets by the selfish or malicious nodes. Finally this leads to attacks. Many approaches are proposed to solve the problems which are occurred in DTN. A survey is proposed by referring some approaches that are used to overcome different problems in the Disruption Tolerant Network.

Index Terms: Disruption Tolerant Networks, Attack, Malicious nodes, Wireless Network.

I. INTRODUCTION

Disruption Tolerant Networks utilize the mobility of nodes. The nodes can move anywhere at any time. Due to the intermittent connectivity it is very difficult to maintain end-to-end connections. This allows the forwarding of data, only if it is in contact with other nodes. So many traditional protocols and conventional routing schemes are failed under this long propagation delay. Because this schemes tries for creating complete path definition to transmit data. This network performs a type of table namely routing table. This routing table is updated at every transmission. Various methods are involved in this type of network. This network is also known as Delay-Tolerant Networks. This network usually follows the "store-carry-forward" scheme.

Whenever the node obtaining the messages, it store it into one buffer and carry it until it gets contact with other node. After this it forward to the specified destination. Examples of wireless networks are military networks, mobile adhoc networks, vehicular ad hoc networks and sensor networks. For establishing routing between the sender and receiver flooding related method is used. In flooding related method large energy will be wasted. It reduces the Disruption Tolerant Networks Performance. Packet Delivery ratio will be reduced by the selfish or malicious nodes. DTN use the method store carry method to exchange the data. In the DTN security model nodes are classified as two types such as misbehaving nodes and normal nodes.

Delay Tolerant Networks getting disconnection because of low node density and mobility. In the DTN data forwarding metric is used to exchange the data. This allows more step-by-step process to improve the forwarding performance. Based on the infrastructure and application security related problems may arise in the Disruption Tolerant Networks such as authorization and data confidentiality obstacles. In a Disruption Tolerant Networks all devices search for nearer visible devices.

II. SECURING METHODS

The methods which are used in DTN is surveyed as given below.

A.Transient Contact Patterns

In [2] a technique is adopted for improve the performance of data forwarding. This consists of three perspectives. They are Transient contact distribution, Transient connectivity, and Transient community structure. By exploiting these perspectives the data forwarding technique can be improved. To find the capability of the nodes in the given period, the first two perspectives are proposed. The final one is for evaluation of exact scope. Here the forwarding of data consists of two stages. They are global scope centrality and local scope centrality. In the first stage, all the nodes in the networks are considered as nodes for forwarding the messages. This stage is used to ensure the carrying and forwarding of data. After finishing this stage the second stage is performed. This is to forward the data directly to the destination. This is done between the nodes in the local network.

B.Social-Aware Multicast

In [3] obtaining of the forwarded data to the Single destination is focused by more forwarding schemes in this network. But this multicast is very effective than the previous schemes. Because it dealts with multiparty communication effectively. To achieve this, the social network concepts such as centrality and community are exploited. These are mainly used for the maintenance of global network knowledge.The basic idea in this is to establish the social-based metrics. This can be done for the selection of relay. This aims to select the minimum relays to satisfy the forwarding performance.

C.Mitigating Routing Misbehavior

In [2] technique allows to mitigate the misbehavior of routing. For that it needs to answer for two questions. They are dealt with detection of packet dropping and limitation of traffic flow. This can be achieved by maintaining a node which acts as a record. It only keep the

signed contacts and that are informed to next node. This helps to detect the packets which are dropped from the network. After this, the limitation is adopted to the number of packets that are forwarded to the misbehaving nodes. Some works which are related to this use the neighborhood detection to find the packets that are dropped by various nodes. This tries to avoid the misbehaving nodes in the selected path. But this approach is not directly applied to DTN. For this problem, routing behavior is proposed.

D.Bubble

In [4] because of the partial capture of transient network, many previous approaches ended with effectiveness cost. Behavior The hierarchical community structure can be performing well with this bubble algorithm. It is a novel social-based forwarding algorithm. This are improved the forwarding performance by comparing the number of already existing algorithms. They also proposed two methods. They are community and centrality. This community refers only the popularized people and the centrality refers to the people who have more interaction than others. This bubble algorithm combines the nodes of the community and centrality. This observes both the human and physical aspects of mobility information.

E.Social Network Analysis Metrics

In [7] Social Network Analysis Metrics is used as a practical forwarding solution for providing an efficient message delivery during the disconnection of network. This metrics are on the basis of the previous interaction of the node. It used the concepts of combination of centrality, strong ties and prediction of tie. This used the theory of network that are allowed to apply with the social network. The information flow graph was proposed by this scheme. These metrics are based on the path information

F.Spray Routing

In [6] whenever the network is disconnected, the transmission becomes faster than the action of the node. For this problem, the spray routing is proposed. Spray and Wait is the first scheme which allows a small number of copies for distribution. This is one of the unaware flooding schemes. This consists of two phases. They are spray phase and wait phrase. The phase which is used for initiating each message at the source, some assumed number of copies are originally spread and allows to sent by this originating nodes. These spreaded messages are possibly spreaded to other nodes. This phase is known as spray phase. The wait phase is used when the destination is not detect in the first phase, that means spray phase. In this phase, a direct transmission is performed by the possible nodes. The second scheme is Spray and Focus. The advantage of the high localization nodes are again considered by this second type of scheme. But this was considered only a limited number of copies. The limitation is applied by itself.

G.Claim-Carry-Check

The limitation of the Disruption Tolerant Network leads to many problems [8]. They are named as an attack. This considered two types of attacks. Packet and Replica attack. These are commonly referred as flood attacks. This problem was solved by the Rate limitation and Claim-Carry-Check techniques. This scheme provides the facility of calculating the packet count by itself. This scheme uses the pigeonhole principle. Using this principle count of flooded packets can be detected. Rate limitation limits over the two types of attacks such as packet flood attack and replica flood attack.

III. CONCLUSION

These are some of the existing problems and solutions that are proposed by different users. These all are almost related with the disruption tolerant networks. These methods are implemented to improve the performance of forwarding techniques and reduce the end to end delay. But some solutions cannot directly apply to overcome the flood attack in DTN. It is observed that claim carry check method is designed to overcome the flood attack in DTN. This is adopted to work in a distribution manner. Generally the social network concept is used here for finding the solution. However, the work which was applying in this type of network is still a challenging one.

REFERENCES

[1] W. Gao and G. Cao, “On Exploiting Transient Contact Patterns for Data Forwarding in Delay Tolerant Networks,” Proc. IEEE 18th Int’l Conf. Networks Protocols (ICNP), 2013.

[2] Q. Li and G. Cao, “Mitigating Routing Misbehavior in Disruption Tolerant Networks,” IEEE Trans. Information Forensics and Security, vol. 7, no. 2, pp. 664-675, Apr. 2012.

[3] Wei Gao, Li Quinghua, Bo Zhao, and Guohong Cao, “Social-Aware Multicast in Disruption-Tolerant Networks”, IEEE/ACM TRANSACTIONS ON NETWORKING, vol.20, No.5, 2012.

[4] Pan Hui, Jon Crowcroft, and Eiko Yoneki, “BUBBLE Rap: Social-Based Forwarding in Delay-Tolerant Networks” IEEE TRANSACTIONS ON MOBILE COMPUTING,VOL.10,NO.11,2011.

[5] W. Gao and G. Cao, “On Exploiting Transient Contact Patterns for Data Forwarding in Delay Tolerant Networks,” Proc. IEEE 18th Int’l Conf. Networks Protocols (ICNP), 2010.

[6] Thrasyvoulos Spyropoulos, Konstantinos Psounis, Cauligi S.Raghavendra, “Efficient Routing in Intermittently Connected Mobile Networks: The Multiple-Copy Case” IEEE/ACM TRANSACTIONS ON NETWORKING, VOL.16, NO.1, 2008.

[7] M. Elizabeth, Daly, and Mads Haahr, “Social Network Analysis for Information Flow in Disconnected Delay-Tolerant MANETs” IEEE, vol.8, 2009.

[8] Qinghua Li, Wei Gao, Sencun Zhu and Guohong Cao, ”To Lie or Comply: Defending against flood attacks in Detail”, IEEE Transaction on Dependable and Secure Computing, Vol 10, 2013.