IJCSN International Journal of Computer Science and Network, Volume 3, Issue 1, February 2014
ISSN (Online) : 2277-5420
www.IJCSN.org

A Survey on Malicious Node Detection Method for Delay Tolerant Network

[1] A.N. Jaiswal, [2] Sonika gandhi

[1] Department of Computer Science and Engineering, GHRIETW, RTMNU
Nagpur, India

[2] Department of Computer Science and Engineering, GHRIETW, RTMNU
Nagpur, India

Abstract - Delay tolerant network s (DTNs) is the one of the areas in the field of wireless communication, where in delay is particularly high. They are promising technology in vehicular, disaster response, under water and satellite networks. Delay tolerant networks characterized by large end to end communication latency and the lack of end to end path from a source to its destination and they pose several challenges to the security of DTNs. Daley and disruption tolerant network is a new communication field that can have multiple networks and internet model. After few years there are numbers implementation and application have performance and application domain. In this survey, we can conclude that the recent developments in the field and high potential for future development.

Keywords - *Delay Tolerant Networking, Disruption Tolerant Networking, attacks, DTN platforms*

.

1. Introduction

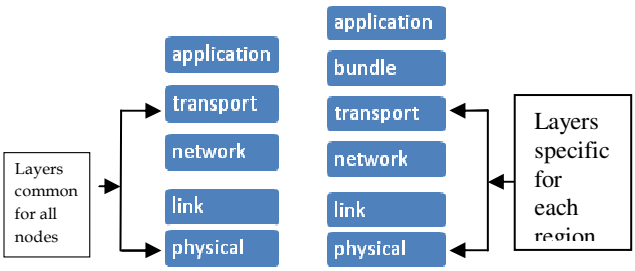
Daley tolerant network is a network where Daley is particularly high. In a mobile ad-hoc network, misbehavioring of the nodes that creates a Daley in network and they form a Daley tolerant network. In a mobile ad-hoc network due to mobility the path will be disrupted, the disruption is temporary and require for a fixed infrastructure in which nodes can communicate with each other via wireless links either directly or relying on other nodes as routers. The operation of MANETs does not depend on base stations. In MANETs, network nodes are move randomly. Therefore, topology of MANET may change rapidly and unpredictably. All the activities of network such as delivering data packets and discovering the topology have to be executed by the nodes themselves. Depending on its application, the structure of a MANET may vary from a small static network to dynamic network. MANETs are special types of DNTs. If compared to MANETs, common problems in packet communication, such as routing, uncasting, broadcasting and multicasting. It becomes sufficiently harder in DTNs even with lossless links. Depending upon the model for mobility, efficient communication schemes for stationary ad-hoc network can be extended partially or wholly to DTNs.

For DTN, a new communication model work in the IPN project spawn with emphasis on communication. So we can realize that networking is the challenging environment for the terrestrial application and both for civilian and military application. So in this setting, Delays are not due to large propagation delay but by communication disruption, intentional or not. In year 2002, the IETF formed the DTN research group which is help in the DTN and with the objective concept into architecture for delay and disruption tolerant networks. The space and terrestrial environment have difference that is the space contacts are schedule and predictable while terrestrial once are more opportunistic in nature.
Some previous survey on DTN, they are focus on mainly an architecture and routing issues in the network. In this survey, we can review the recent advance in the DTN potential for terrestrial application.

2. Review

2.1 Delay Tolerant Network Architecture

A delay tolerant network is a regional network including the internet. The DTN have communication characteristic in a communication region. Wireless DTN technologies include not only ratio frequency but also ultra wide band, acoustic technologies. DTN gateway having membership in a two or more region for only passing a message between regions. Each region has unique ID.



Original five layer of TCP DTN protocol bundle layer

Fig 1: DTN specific task

2.2 Attacks on DTN

In MANET, adversary may mount several threats against DTNs to reduce the performance of the network. There are several attacks in ad-hoc network. Attacks are classified into two types: external attacks and internal attacks. In external attacks, the attacker cause congestion in routing information and disturb nodes from providing services. In internal attacks the adversary wants to gain normal access to the network activates using it as basis to conduct its malicious behavior. Attacks can also be classified into two categories:

A. Attacks on routing protocols
B. Attacks on packet forwarding

An ad-hoc network can be attacked from any direction at any node in the network which is different from the fixed hardwired networks. The every node should be equipped to meet an attacker directly or indirectly. In network mobile node may attempt to benefit from other nodes, but refuse to present its own resources. Such nodes are called malicious nodes. Malicious node attack from both inside and outside of the network. In ad-hoc network it is very difficult to track a specific node in large ad-hoc networks and it is more dangerous and much difficult to detect the attacks from an affected node. It denotes that every node should be prepared to work in a way that it should not trust on any node immediately. The attacks on the route loop, resource deprivation and route hijack is brought influences in the network. Due to mobility and constantly changing the topology of the mobile ad-hoc network, it is difficult to validate all the route information as a result of impersonating another node to spoof route message, flooding route discovery, modifying route message, suppressing route error to mislead others may occur. In this the attacks can be classified as impersonation, modification, fabrication, wormhole and lack of cooperation.

2.2.1 Attacks using Modification

In DTNs, the modification is a type of attack when the malicious node can redirect the network traffic and conduct DOS attacks by modifying message fields or by forwarding route message.

2.2.2 Attacks using Impersonation

Malicious node lunch many attack in the network due to no authentication of data packets in ad-hoc network by masquerading as another node that is spoofing. Spoofing is occurring in the network when the malicious node misreprensts its identity in the network such as MAC or IP address.

2.2.3 Attack through Fabrication

In the DTNs, fabrication is used to refer the attacks by generation false routing message in the MANETs.

2.2.4 Wormhole Attacks

It is also known as tunneling attack. In a tunneling attack two or more than two nodes are collaborate to encapsulate and exchange message between them along existing data routes.

2.2.5 Lack of Cooperation

A selfishness node wants to preserve own resource by using the serves of their resource. In mobile ad-hoc network the cooperation of all the participating nodes to transfer traffic, the more powerful a MANET gets. The most serious attack in the network is byzantine attack which is in the insider network.

The behavior of Byzantine attack in the network as follow:

1. In the network there is a selfish node means not forwarding the data packets to others and change the transmitting data packet and to destroy the operation of the AODV in MANET, by advertising shorter routes to a destination.

2. To disturb the communication of other nodes in the network, without regard to its own resource consumption. These cause Byzantine failures which include the omission failures for example crash, failing to receive a request or failing to send a response and the Commission failures for

example processing a request incorrectly or sending an incorrect or inconsistent response to a request.

3. If two nodes are compromised means malicious node receives packets at one location in the network and tunnels them to the network, where the packets in the network are resent into the network.

2.3 DTN Platforms

DTN implementation having platform, system needs, and processing architecture. On the basis of survey, DTN can be implemented on the Linux, win 32, Mac OSX, free BSD, C++. As a survey of DTN platforms, the DTN-reference platform evolved into the DTN2. DTN2 is a open source license and it is written in C++, and Linux. DTN 2 is hosted on source forge code. DTN2 also supported external routing via XML messaging. The current version of DTN2 is supported the TCP, UDP, AX.25 and Bluetooth convergence layers. In DTN, the ION is software that is implemented on the bundle protocol stack and routing functionality environment. Another protocol that is IBR-DTN is a very portable, slim and extensible protocol that is implemented on C++.

2.4 Performance Analysis

The DTN implementation gives a large delay and disruption. As a survey, the performance of the DTN built in accordance to network performance tools and supported many DTN options like, sent window, volume and file transfer, custody transfers. The traffic analysis tools can be help for a developer for example, when DTN software on different architecture, convergence layer and testing for interpretability. A survey of the entire platform like IBR-DTN, ION and DTN2 we can conclude that they all software is a memory base storage. Their performances are limited by the bundle frequency and the amount of data must be moved in high speed like vehicular nodes joining a Wi-Fi network. The DTN2 is a very low cast and low power computer. The effects of security in performance of DTN2. For the security they used the android platform and used the bound-castle library for cryptography operation. The is implementation required the encryption algorithm. In the smart phone performance analysis describe the small transmission overhead of only 0.007 seconds. So there was large battery overhead for encryption and decryption operation due to cryptography. So in this, bundle security required small transmission overhead.

2.5 Emulation and Simulation

The emulation and simulation is very necessary activity for testing and validating new ideas in the network and their operation. So, as a survey of simulation in DTN, it is focus on each environment, complexity of the network and their needs. In this survey we find there are four main stream simulation are used in the DTN routing: NS2, OMNET++, DTNsim and ONE. The NS2 and OMNET++ are used in general purpose in the DTN for extended to a degree for supporting DTN. The OMNET++ and DTNsim are supported only in two situation routing in a remote village and network to a city bus. ONE simulator is used such a low degree accuracy of time slot, lack of supporting for lower level protocol.

3. Conclusion

In this survey, we reviewed developing DTN software, services and application. DTN starting from the deep space communication and then it is evolved in architecture for any networking environment. The DTN provide the sufficient condition for the implementation and their performance. We can conclude from software, simulation, emulation, the DTN can be implemented on the complex scenarios and pursue even harder problem. For the more application more and more application cope with disruptions in the internet domain.

References

[1] Erman Ayday, and Faramarz Fekri "*An Iterative Algorithm for Trust Management and Adversary Detection For Delay-Tolerant Networks*" IEEE trans. on mobile computing, VOL. 11, NO. 3, SEP 2012.

[2] Z. Zhang, "*Routing in intermittently connected mobile ad hoc networks and delay tolerant networks: overview and challenges*," IEEE Communications Tutorials & Surveys, vol. 8, no. 1, quarter 2006, pp. 24–37.

[3] K. Fall, "*A Delay-Tolerant Network Architecture for challenged internets*," in Proceedings of the 2003 conference on protocols, architectures, technologies and application for computer communications. ACM, 2003, pp. 27–34.

[4] Z. Zhang and Q. Zhang, "*Delay/disruption tolerant mobile ad hoc networks: latest developments: Research articles*," Wireless Communication Mobile Computer, vol. 7, no. 10, Dec. 2007, pp. 1219–1232.

[5] J. Crowcroft, E. Yoneki, P. Hui, and T. Henderson, "*Promoting tolerance for delay tolerant network research*," SIGCOMM Computer Communi. Rev., vol. 38, no. 5, Sept. 2008, pp. 63–68.

[6] A. Lindgren and P. Hui, "*The quest for a killer app for opportunistic and delay tolerant networks*," in

Proceedings of the ACM workshop on Challenged networks (CHANTS '09). New York, USA: ACM, 2009, pp. 59–66.

[7] W. D. Ivancic, "*Security analysis of DTN architecture and bundle protocol specification for space-based networks*," in 2010 IEEE Aerospace Conference, NJ, USA: IEEE, 2010, pp. 1–12.

[8] S. Domancich, "*Security in delay tolerant networks for the Android platform*," Master's thesis, Royal Institute of Technology (KTH), Sweden, June 2010.

[9] M. Loubser, "*Delay tolerant networking for sensor networks,"* Swedish Institute of Computer Science, Kista, Sweden, Tech. Rep. T2006:01, 2006.

[10] M. Liu, Y. Yang, and Z, "*A survey of routing protocols and simulations in delay-tolerant networks*," in Proceedings of the international conference on Wireless algorithms, applications, and systems. Berlin, Heidelberg on IEEE, 2011, pp. 243–253.

[11] J. Morgenroth, T. Poegel, "*Delay-tolerant networking in restricted networks*," in Proceedings of the 6th ACM seminar on Challenged networks. New York, NY, USA: ACM, 2011, pp. 53–56.

First Author Sonika Gandhi has received her B.E. degree in Electronics & Instrumentation Engineering from Chhatrapati shivaji institute of technology Durg (C.G), CSVTU University in 2012. She is pursuing M.E. in Wireless Communication and Computing from G.H.Raisoni Institute of Engineering and Technology for Women Nagpur. Her research interests include Detection of Malicious node in DTNS.

Second Author Anil Jaiswal , Professor in Department of Computer Science and Engineering @ G.H. Raisoni Institute of Engineering and Technology for Women Nagpur.