International Journal of Engineering and Applied Physics (IJEAP)
Vol. 1, No. 3, September 2021, pp. 272~277
ISSN: 2737-8071

Comparative Analysis of Attack Detection Methods in Delay Tolerant Network

Rajashri Chaudhari[1], Manoj Deshpande[2]
[1,2]Dept. of Computer Engineering, ACPCE, Kharghar, Navi Mumbai, Maharashtra, India.

Article Info

Article history:

Received
Revised
Accepted

Keywords:

Delay Tolerant Network
Blackhole attack
Greyhole attack
security
Flooding attack

ABSTRACT

Delay Tolerant Network is a new kind of wireless network which includes Radio Frequency (RF) and acoustic (sonar) technologies. DTN developed for an interplanetary network where the speed of light is slow. DTN is derived from deep space communication. DTN is distinguished as long delay and intermittent connectivity. The Delay Tolerant Network is more vulnerable to different kinds of attacks like flooding attack, blackhole and greyhole attacks, due to limited connectivity. There is no end-to-end connectivity between source & destination in DTN. So that it uses a store, carry and forward mechanism to transfer the data from one node to another node. The Delay Tolerant Network was developed to solve technical problems in the end-to-end network. DTN is becoming more and more important because communication networks are ubiquitous today. It provides automotive communication solutions. DTN is a decentralized and self-managed system with unique network attributes; however, attributes such as high mobility nodes, network uplinks and downlinks, and separate routing can cause network vulnerabilities. These vulnerabilities include the host being compromised, which in turn will bring security risks, because the compromised host may destroy the routing protocol in the network. This article analyses the various types of attack detection methods.

Corresponding Author:

Rajashri Chaudhari,
A.C. Patil College of Engineering,
Kharghar, Navi Mumbai, Maharashtra, India.
Email: rajashri.c93@gmail.com

1. INTRODUCTION

In Mobile Adhoc Network (MANET) packets can be transferred only if a link between the nodes is established. If a link is not established then packets will be lost. So, the packet delivery ratio will be decreased in MANET. To defeat this problem, Delay Tolerant Network (DTN) is used. Figure 1 shows the architecture of DTN. In DTN, each node has some storage buffer. So, if the links of nodes are not established then packets will be stored in the storage. Communication services in unreachable & unfriendly environments are provided by DTN [19].

In recent years, the number of online threats has increased significantly. DDoS attacks and flood attacks are the main types of these threats. The purpose of these attacks is to prevent legitimate users from accessing Internet services. DDoS attacks act as a serious threat to the availability of Internet services. This attack forces multiple agents to send a large number of data packets to the victim, which easily consumes the victim's resources. A delay network is purposely designed to operate efficiently over extremely long distances (i.e., space communications). In these surroundings, a delay plays an important role in affecting network quality.

Delay-tolerant network addresses the issues regarding heterogeneous networks that may lost network connection continuity. Examples are those networks operating in mobile or extreme terrestrial environments, or planned networks in space. A series of network data bundles that are defined by a new kind of network that enables applications. In DTN, there is no end-to-end path between source and destination. DTN is characterized by long propagation delay and intermittent connectivity [18]. DTN consisting of a set of protocols that acts together to enable a standardized method of performing store-carry-forward mechanism shown in fig.1.

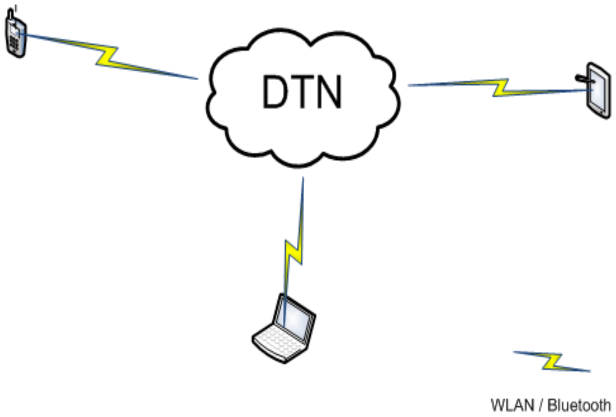

Figure 1.DTN Architecture

2. SECURITY MEASURES

- **Authentication**
  For every intermediate DTN node, it is essential to have the ability to check the data sent by an authorized node. The requirement of authentication depends on goals of security design and provided either on a hop-by-hop or end-to-end basis.

- **Confidentiality**
  Confidentiality requirement is to ensure that sensitive information is not revealed to unauthorized third parties during the bundle propagation process over DTN links.

- **Integrity**
  Integrity requirements should ensure that the transmitted messages cannot be altered during the propagation process. Due to shortage of integrity protection could result in many attacks including message modification, falsification, or replay attacks.

- **Privacy**
  The network should not disclose the location of the user, nor the party with which she communicates.

3. METHODS FOR ATTACK DETECTION

i. **Queuing mechanism**
This queuing mechanism is based on the Radia Perlman’s network design with byzantine robustness that can withstand malicious routers as well as alleviate the effect of flooding attacks through fair allocation of resources. This queuing policy is slightly different from Radia Perlman’s design in terms of allocation of resources. It involves a drop tail queue management technique using a distinctive formula for the selection of the preferred message to be dropped when the buffer is full. It is used for determining which message to remove when the storage is full. A metric is used as the determinant of which message to drop in queuing policy [6].

ii. **Mutual Correlation Detection Scheme (MUTON)**
In MUTON, each node will gather the packet distribution probabilities of any node that it encounters with and the past encounter history of that node. The gathered information is used for estimating the changes in the delivery probabilities to other nodes due to the transitivity property [20]

iii. **Claim-Carry-Check method**

In this method, each node itself counts the amount of packets or replicas that it's sent out, and claims the count to other nodes; the receiving nodes carry the claims around once they move, exchange some claims once they contact, and cross-check if these claims are inconsistent. If an attacker floods more packets or replicas than its limit, it's to use an equivalent count in additional than one claim consistent with the pigeonhole principle and this inconsistency may lead to detection[11].

iv. Stream-Check Method

In this scheme use a streaming node to perform the intrusion detection function. At every beacon of time the streaming node travelled along the path of the packet. Main function of streaming node is to provide a secret message for decryption of the claim generated by node. Rate limiting is a mechanism used to limit the packet rate. Setting of the rate limit is performed during a request-response style. When a user joins into the network it requests a rate limit from a trusted authority, which acts as operator[9].

v. Flooding Detection based on Encounter Record (FDER)

This method aims at detecting flooding attacks in DTN without imposing a strict rate limit on a node’s message generation rate. Each node’s normal traffic pattern is still mannered by a rate limit but the node is allowed to have a small and short burst of new messages which exceeds the rate limit. If the node generates an outsized burst for an extended period, it is considered as a flooding attacker and will be detected by FDER[1].

4. LITERATURE REVIEW

J. Cho et al [22] this article shows DTNs are common in the military environments, where network connectivity is not secure or guaranteed due to disconnection or delay of frequency level. They propose a trust framework based on provenance which is called PROVEST, they are working to achieve the increase in the correct message delivery received by destination nodes with peer-to-peer trust networks. This work acquires a model-based technique to estimate the PROVEST performance.

W. Khalid et al [21] Delay tolerant network (DTN) is a special type of intermittent connection network (ICN), which is characterized by variable delays, frequent failures, asymmetric data rates, and high error rates. A new resource-efficient algorithm (distributed and based on an intrusion detection system) is proposed to mitigate flood attacks.

Gideon Rajan et al [23] this paper proposed a new secure key management framework for the security of DTN. The system distributes cryptographic keys which securely represent the nodes. These distributed keys are used to reduce public-key cryptography to reduce during network attacks.

Yanzhi Ren, et al [20] developed the Mutual correlation detection scheme (MUTON) to address insider attacks. MUTON is examined when calculating the packet delivery probability of each node and correlates the information collected from other nodes. The collected information is employed for estimating the changes within the delivery probabilities to other nodes. During detection, when the ferry come up against a node, it uses a self-examination approach.

Mythili M., Renuka K.[24] developed a scheme that determines different forms of attack on DTN such as blackhole and greyhole attacks using fuzzy rule. This detection system is evolved from Fuzzy Logic. An IDS system is boosted by making use of two factors i.e., packet loss rate, data rate. They use both factors with fuzzy logic to solve problems using problem solving control systems. In this, a fuzzy algorithm is used to detect attacks.

Table 1. Comparison between attack detection methods in DTN

YEAR	AUTHOR	CONTRIBUTION	ATTACKS DETECTED
2010 [6]	Feng Cheng Lee, Weihan Goh, Chai Kiat Yeo	Introduced new queuing mechanism that can defend against the possible flooding attacks in DTN	Flooding attack
2010 [20]	Y. Ren, M. Chuah, J. Yang, and Y. Chen	Mutual correlation detection scheme (MUTON) introduced	Blackhole attack
2013 [11]	Qinghua Li, Wei Gao, Sencun Zhu, and Guohong Cao	A new technique was proposed, which exploits claim-carry-and-check to detect the violation of rate limit in DTN.	Packet Flood and Replica Flood attacks
2013 [17]	Dhiraj kr. Mishra, Meenu Chawla	Minimax Theory Based Scheme was proposed to distribute credits among non-selfish nodes	Detect Selfish nodes
2014 [9]	Divya Kuriakose,D. Daniel	Stream-Check Method is used to detect Flood attacks	Flood attack
2015 [3]	Pham Thi Ngoc Diep, Chai Kiat Yeo	The piggyback allows to incorporate two schemes into a single robust misbehaviour detection system.	blackhole, greyhole and flooding attack
2015 [4]	Preeti Nagrath, Sandhya Aneja, G.N.Purohit	A new scheme was introduced which uses a modified secure metric called reputation to distinguish a node in contact between malicious node and legitimate node.	Packet Flood attack
2017 [1]	Thi Ngoc Diep Pham, Chai Kiat Yeo, Naoto Yanai, Toru Fujiwara	A new scheme Flooding Detection based on Encounter Record (FDER) was developed that detects flood attacks.	Flood attack
2017 [8]	Zhicheng Liu and Junxing Zhang	A new scheme OSO, an improved Wi-Fi offloading architecture to mitigate data flooding attack.	Data flooding attack
2018 [2]	Zhaoxu Wang, Huachun Zhou, Bohao Feng, Wei Quan and Shui Yu	MTF targets the AS level traffic behaviour differences before and after the beginning of LFA	Link flood attack
2018 [7]	Keisuke Arai, Shuichiro Haruta, Hiromu Asahina, Iwao Sasase	An ER reduction scheme based on theoretical contact probability for flooding attack mitigation was introduced.	Flooding attack
2018 [10]	Takuya Idezuka, Tomotaka Kim Ura, And Masahiro Muraguchi	The theory focuses on analysis of the behaviour of flooding attacks in DTN environments.	Flooding attack
2016 [18]	Thi Ngoc Diep Pham and Chai Kiat Yeo	forwarding ratio metrics designed that can distinguish the behaviour of attackers from normal nodes.	Detect Blackhole and Greyhole attack
2021 [16]	Quisar Ayub, Sulma Rashid	An Intelligent buffer management policy has been designed that detects and drops messages those are destined to dead nodes.	Detects inactive nodes.

5. CONCLUSION

Delay tolerant networks are constructed networks. Security is the main concern of the Delay-Tolerant network. This paper compares different attack detection methods in DTN. In particular, flood attacks can slow down the network speed and abuse network resources. Most of the methods are able to detect flood attack efficiently. So that it reduces traffic in network.

REFERENCES

[1] Thi Ngoc Diep Pham, Chai Kiat Yeo, Naoto Yanai, Toru Fujiwara,"Detecting Flooding Attack and Accommodating Burst Traffic in Delay Tolerant Networks,"IEEE Transactions on Vehicular Technology, pp.1-14, 2017

[2] Zhaoxu Wang, Huachun Zhou, Bohao Feng, Wei Quan and Shui Yu"MTF: Mitigating Link Flooding Attacks in Delay Tolerant Network, "IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, cloud & Big Data Computing, Internet of People and Smart City Innovations, pp. 1532-1539,2018

[3] Pham Thi Ngoc Diep, Chai Kiat Yeo,"Detecting Flooding Attack in Delay Tolerant Networks by Piggybacking Encounter Records, " IEEE, 2015

[4] Preeti Nagrath, Sandhya Aneja, G.N.Purohit,"Defending Flooding Attack in Delay Tolerant Networks, " IEEE, ICOIN 2015, Vol. 15, pp. 40-45, 2015

[5] D.S.Delphin Hepsiba, S.Prabhu,"Enhanced Techniques to Strengthening DTN against Flood Attacks, "IEEE,2014

[6] Feng Cheng Lee, Weihan Goh, Chai Kiat Yeo,"A Queuing Mechanism to Alleviate Flooding Attacks in Probabilistic Delay Tolerant Networks," Sixth Advanced International Conference on Telecommunications, Vol.78,pp. 329-334, 2010

[7] Keisuke Arai, Shuichiro Haruta, Hiromu Asahina, Iwao Sasase,"Encounter Record Reduction Scheme based on Theoretical Contact Probability for Flooding Attack Mitigation in DTN," 24th Asia-Pacific Conference on Communications (APCC), Nov.2018

[8] Zhicheng Liu and Junxing Zhang,"OSO: Mitigating Data Flooding Attack in Wi-Fi Offloading," 6th International Conference on Computer Science and Network Technology (ICCSNT),IEEE. pp.400-404,Oct 2017

[9] Divya Kuriakose, D. Daniel,"Effective defending against flood attack using stream-check method in tolerant network," 2014 International Conference on Green Computing Communication and Electrical Engineering (ICGCCEE) ,Oct 2014

[10] Takuya Idezuka, Tomotaka Kim Ura, And Masahiro Muraguchi,"Behavior Analysis of Flooding Attacks in Sparse Mobile Ad-Hoc Networks,"IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW),2018

[11] Qinghua Li, Wei Gao, Sencun Zhu, and Guohong Cao,"To Lie or to Comply: Defending against Flood Attacks in Disruption Tolerant Networks, "IEEE Transactions on Dependable and Secure Computing, VOL. 10, NO. 3, pp, 168-182, May/June 2013

[12] Manghui Tu, Kyle W. Riordan, Geyang Xie , Shuhui Yang , "A Secure Contact Protocol for Delay Tolerant Networks, " IEEE ICIS 2017, Vol. 17, pp.5-11, May 2017

[13] Shuang Ding, Xin He, Jicheng Wang, And Junan Liu,"Pre-Decoding Recovery Mechanism for Network Coding Opportunistic Routing in Delay Tolerant Networks, " IEEE Access, Vol.6, pp.14130-14140, March 2018

[14] Hezhe Wang, Huiqiang Wang, Jing Tan, Hongwu Lv, And Meijin Zhu,"A Delay Tolerant Network Routing Policy Based on Optimized Control Information Generation Method, " IEEE Access, Vol. 6, pp.51791-51803, Oct 2018

[15] WANG Rong, WU Yahui, HUANG Hongbin, and DENG Su,"Cooperative transmission in delay tolerant network, " Journal of Systems Engineering and Electronics, Vol. 30, No. 1, pp.30 – 36, February 2019

[16] Ayub, Q., Rashid, S. “Energy Efficient Inactive Node Detection Based Routing Protocol for Delay Tolerant Network”. Wireless Personal Communications, vol. 116, pp. 227–248 (2021).

[17] Dhiraj kr. Mishra, Dr. Meenu Chawla, "Minimax Theory Based Scheme to Detect Selfish Node and Reduce Latency in Delay Tolerant Network", Conference on Advances in Communication and Control Systems, pp. [78-82],2013.

[18] Thi Ngoc Diep Pham and Chai Kiat Yeo, "Detecting Colluding Blackhole and Greyhole Attacks in Delay Tolerant Networks," in IEEE Transactions on Mobile Computing, vol. 15, no. 5, pp. 1116-1129, 1 May 2016

[19] (2014, february) ijareeie. [Online]. https://www.ijareeie.com/upload/2014/february/13l.html

[20] M. Chuah, J. Yang, Y. Chen, Y. Ren, "MUTON: Detecting malicious nodes in disrupt-tolerant networks," in Proceeding IEEE Wireless Communication Networking Conference, 2010, pp. 1-6.

[21] W. Khalid, N. Ahmed, M. Khalid, A. Ud Din, A. Khan and M. Arshad, "FRID: Flood Attack Mitigation Using Resources Efficient Intrusion Detection Techniques in Delay Tolerant Networks," in IEEE Access, vol. 7, pp. 83740-83760, 2019

[22] J. Cho and I. Chen, "PROVEST: Provenance-Based Trust Model for Delay Tolerant Networks," in IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 1, pp. 151-165, 1 Jan.-Feb. 2018

[23] Gideon Rajan and Gihwan Cho, "Applying Security Architecture with Key Management Framework to the Delay/Disruption Tolerant Networks", IJSIA, Vol-9, pp [327-336], 2015.

[24] Mythili M., Renuka K., “An Efficient Black Hole and Gray Hole Detection Using Fuzzy Probabilistic Detection Scheme in DTN”, International Journal of Advanced Research in Computer and Communication Engineering, vol. 5, no. 10, pp. 123-127, Oct. 2016

BIOGRAPHIES OF AUTHORS

	Rajashri Chaudhari is a research scholar and currently pursuing a Ph.D. in Computer Engineering from ACPCE, Kharghar, Navi Mumbai, Maharashtra, India. She earned her M.E. degree in Computer Science and Engineering in 2017 and completed B.E. degree in Computer Engineering in 2014 from SSVPSCOE, Dhule affiliated to North Maharashtra University, Jalgaon, Maharashtra, India.
	Dr. Manoj M. Deshpande has obtained his M.Tech and PhD from Indian Institute of Technology Bombay, Mumbai in 2002 and 2009 respectively from IDP in Systems and Control Engineering. Currently he is working as Professor and Dean at A. C. Patil College of Engineering Navi Mumbai, Maharashtra, India.