{tag} {/tag}International Journal of Computer Applications
Foundation of Computer Science (FCS), NY, USA

Volume 171
-
Number 4

Year of Publication: 2017

Authors:

Chaudhari Rajashri M., Patil Manesh P.

10.5120/ijca2017915008

{bibtex}2017915008.bib{/bibtex}

Abstract

DTN (Delay Tolerant Network) is a new kind of wireless technologies which includes Radio Frequency (RF) and acoustic (sonar) technologies. DTN developed for interplanetary use where the speed of light is slow. DTN is a new kind of network derived from deep space communication. DTN is characterized as long delay and intermittent connectivity. The Delay Tolerant Network (DTN) is more vulnerable to different kinds of attacks like blackhole and greyhole attacks, due to limited connectivity. There is no end to end connectivity between source & destination in DTN. So that it uses store, carry and forward mechanism to transfer the data from one node to other node. Delay tolerant networks (DTNs) are characterized by delay and intermittent connectivity, due to this, malicious nodes drops all or a part of the received messages. This dropping behavior is known as blackhole and greyhole attacks respectively. Existing research scheme can detect individual attackers well but they cannot handle the case where attackers cooperate to avoid the detection. So that SDBG scheme implements an algorithm to detect individual attacks with collusion attack. The simulation result shows the protocol reduces the delivery delay using RAPID protocol by detecting collusion attacks that is

simulated using the ONE simulator.

References

1. Thi Ngoc Diep Pham and Chai Kiat Yeo, "Detecting Colluding Blackhole and Greyhole Attacks in Delay Tolerant Networks," IEEE Transactions on Mobile Computing, vol. 15, no. 5, pp. 1116-1129, May 2016.
2. M. Chuah, P. Yang, and J. Han, "A ferry-based intrusion detection scheme for sparsely connected ad hoc networks," in In Proceeding 4th Annu. Int. Conf. Workshop Security Emerging Ubiquitous Computing, 2007, pp. 1-8.
3. F. Li, J. Wu, and A. Srinivasan, "Thwarting blackhole attacks in disrupt-tolerant networks using encounter tickets," In Proceeding INFOCOMM, pp. 2428–2436, 2009.
4. Y. Ren, M. Chuah, J. Yang, and Y. Chen, "MUTON: Detecting malicious nodes in disrupt-tolerant networks," in in Proceeding IEEE Wireless Communication Networking Conference, 2010, pp. 1-6.
5. Q. Li and G. Cao, "Mitigating routing misbehaviors in disruption tolerant networks," IEEE Transaction on Information Forensics and Security, vol. 7, no. 2, pp. 664-675, April 2012.
6. Y. Guo, S. Schildt, and L. Wolf, "Detecting blackhole and greyhole attacks in vehicular delay tolerant networks," in In Proceeding IEEE 5th international conference on Communication System and Networking, 2013, pp. 1-7.
7. N. Li and S. K. Das, "A trust-based framework for data forwarding in opportunistic networks," Elsevier J. Ad Hoc Networking, vol. 14, pp. 1497–1509, 2013.
8. Z. Gao, H. Zhu, S. Du, C. Xiao, and R. Lu, "PMDS: A probabilistic misbehavior detection scheme toward efficient trust establishment in Delay-tolerant networks," IEEE Transaction on Parallel and Distributed System, vol. 25, no. 1, pp. 22-32, Jan 2014.
9. Mythili M. and 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, october 2016.
10. A. Keranen, J. Ott, and T. Karkkainen, "The one simulator for dtn protocol evaluation," in Proc. 2nd Int. Conf. Simul. Tools Tech., Rome, Italy, March 2009.
11. (2014, february) ijareeie. [Online]. https://www.ijareeie.com/upload/2014/february/13l.html
12. Thi Ngoc Diep Pham and and Chai Kiat Yeo. (2016, May) Detecting Colluding Blackhole and Greyhole attacks in Delay Tolerant Networks. ACM Digital Library.

Index Terms

Computer Science Wireless

Keywords

Delay Tolerant Network, Blackhole attack, Greyhole attack, Collusion, Detection Accuracy, and Delivery Delay.