Blackhole Detection and Prevention Strategies in DTN

[1]Rakhi Sharma and [2]Dr D.V Gupta

[1]Assistant Professor, Jmit, Radaur

[2]Professor, College of Engg., Roorkie

ABSTRACT: Delay Tolerance Network (DTN) is a network which is used for sparse networks where network connectivity is not possible between two nodes so for this number of intermediate nodes is used to transfer messages. These intermediate nodes may cause network so security in DTN is a very difficult task. In this paper blackhole attack and its various detection techniques are presented with literature review of different research papers that covers black hole detection and prevention mechanism. A blackhole node behaves maliciously in network and provides wrong data routing information or may drop the messages receives from other nodes. So it is difficult to find black hole attack and prevent network from them. These techniques are used in the prevention of network from blackhole attack.

Keywords: DTN, Security, Blackhole Attack, Reputation, Routing and Movement model etc.

I. Introduction

DTNs are wireless networks designed for the environment where end to end connectivity is not possible between nodes. DTN provides special kind of routing protocols that provides routing between nodes where no direct contact is presented between nodes [1].

DTN routing protocols use store carry and forward mechanism to transmit messages between intermediate nodes. In store carry and forward mechanism nodes store data coming from source into buffer and carrying this data to forward it to destination when it comes in the range of destinations they forward messages to destination [2]. In DTN transmission of messages through intermediate nodes is a difficult task because intermediate nodes may behave as maliciously by either dropping the message or not forwarding messages. There are number of attacks presented in networks like Black hole attack, selfish node attack, Sybil attack, wormhole attack an jellyfish attack. In this paper main focused on black hole attack and various prevention techniques [3].

I. Challenges in DTN

In this section various challenge are discussed that are occurred during data transmission in DTN. These are as follows:

i. Encounter Schedule: With a specific end goal to send the information from source to destination, the node can hold up till it experiences the destination node and after that straightforwardly convey the message to the destination.

ii. Network Capacity: Limit of basic system is likewise a crucial element for deciding the measure of information that can be conveyed. On the off chance that amid experience different nodes tries to forward information, the system may get to be congested. Accordingly, this element figures out if a message should be divided or not with a specific end goal to send it from source to the destination.

iii. Storage Capacity: The capacity limit of nodes is confined. At whatever point an experience happens, the nodes attempt to swap every one of the information they right now keep with them. In this manner, if the nodes have capacity appreciative the node supports will flood and it will come about into message adversity [3].

II. DTN Architecture

The DTNRG has created engineering for Delay-Tolerant Networking that has risen up out of the endeavours on Inter Planetary Internet (IPI)[4]. The essential ideas discover their application in sensor systems, interpersonal correspondence (individuals or "pocket-exchanged" systems), and in versatile Internet access.

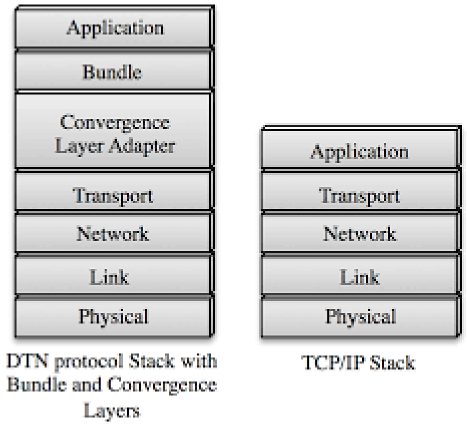

Fig1 DTN bundle layer Architecture

i. Link Layers: In link layers same lower level Layers are available which are available in TCP/IP i.e. Information join layer, Internet Layer, Transport Layer. The capacity of these layers is same as in TCP/IP convention suite.

ii. Bundle Layer: Bundle Layer gives join between lower level connection Layers and Application layer. Information is transmitted in system in type of packs and is transmitted by Bundle Layer.

iii. Application Layer: Application Layer gives interface to the end clients. End clients can impart to different Layers through Application Layer. In application Layer different conventions are available like FTP, Telnet, and DNS and so on.

III. DTN Routing protocols

i. Epidemic routing: In epidemic routing number of replication of messages are send in network in the hop that at least one copy of message is received towards destination. In this routing delivery ratio is high but due to replication of message overhead ratio also increases [5].

ii. Spray and Wait: In SAW routing source messages in two phases. In first phase it replicate messages and waits for a time for the acknowledgement from any other intermediate nodes which are in the range of destination node. In second phase source sends messages only to those intermediate nodes through which it receives acknowledgment. In this routing delivery ratio and overhead ratio is slightly lower than epidemic routing [6].

iii. Prophet routing: In prophet routing source node sends messages through the node having highest chances of message delivery to next node. This intermediate node is chosen by computing the probability of message delivery of node. In this routing mechanism delivery ratio is constant while overhead ratio decreases [7].

IV. Black Hole Attack

Black hole is a network layer attack [8]. At the point when a source node sends a Route Request (RREQ) to its neighbour nodes, then all nodes answer in an approved way however the attacker node answers with smallest metric quality. Source node supposes this node has the most restricted path to the destination. In black hole attack, an attacker node utilizes its directing convention to advertise that it has the most limited path from source to the destination node or to the bundle it needs to capture. This antagonistic node promotes its accessibility of new and briefest paths without looking in its directing table. Along these lines attacker node will dependably have the accessibility in answering to the course demand and accordingly block the information bundle and hold it.

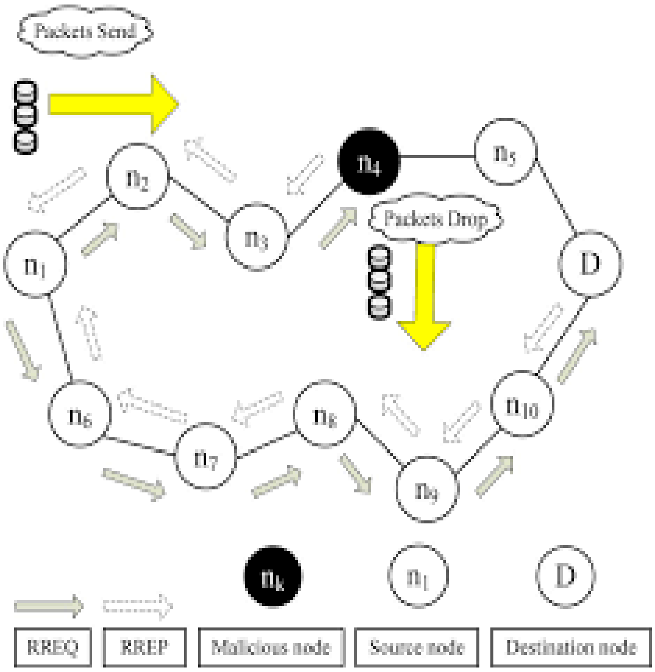

Fig 2: Black Hole Attack in DTN

Black Hole attack has two properties:

- First, it sends the wrong directing data to the source node.
- Second, it blocks or drops the bundles which are bound to destination node through itself.

II. Literature Review

Fu et al. [9] utilized an information steering data (DRI) table at every node and cross checking strategy to recognize the helpful black hole nodes in the system. The adjusted AODV directing convention was utilized to accomplish this approach. The analysis results demonstrate that this arrangement performs superior to anything different arrangements.

Tao and Bharat [10] displayed the most vital types of attacks and talk about conceivable cooperation among different attackers and show how different sign preparing and neural learning can help in discovery and barrier of collective attacks in such situations. They similarly demonstrated how collective attacks can bring about a more terrible impact on remote than on a wired system. Analysis results show the acceptance and viability of the model proposed by minimizing the communitarian attacks and vaccinating the portable specially appointed systems.

Yi Hu et al. [11] tended to the issue of cooperative insider attacks where basic information inside the data frameworks is traded off by two or more insiders cooperating. Authors initially talked about different relations among illegal data stream outline and data framework parts. At that point after, different attributes of information gets to outlined by the common get to record's likelihood regard and the exchange separation to information thing are displayed. Subsequently the calculation is presented for distinguishing community oriented insider attacks.

Sanjay et al. [12] proposed a system to keep it by occupying movement from the Black Hole nodes. The MANETs so talked about make utilization of the AODV steering convention and the strategy so proposed depends on sending confirmation messages that are confirmed by the destination to check for the Black Hole nearness in the GAODV directing convention so proposed.

Liu et al. [13] proposed a theory that adjusted Collaborative attackers can pass trusted nodes help techniques which are regularly utilized as a part of existing secure strategy. On the premise of theoretical investigation, the reports so framed between BC assailants have the most significant likenesses amount. They proposed a calculation to check irregularity discovery and to distinguish BC attackers. The Numerical results demonstrate that the proposed method can without much of a stretch recognize and discover BC aggressors obviously.

III. Existing techniques

i. Reputation Based System: In this system every node gives response of its neighbour node by checking its reputation value and order whether it is deadly node or normal node. The disadvantage of this technique was that measuring reputation of node is a difficult assignment as a result of element nature of nodes [14].

ii. CORE: In this strategy, node advances the bundle by monitoring different nodes and their development. Drawback of technique was that the sender node relies on upon another node and if another node is destructive then transmission is modified [15].

iii. Buddy System: This strategy depends on social structure, implies how one node relies on upon another node. In light of this it is to be chosen whether node advances the bundles or not. Disadvantage of this technique was measuring the contact between two nodes as a result of aspect nature of nodes [16].

iv. ERS: Event-based reputation system (ERS) in which presence of activity occasions was resolved in view of its perception by other neighbor nodes. Association of certainty neglected for every node was an issue with ERS [17].

IV. Conclusion and future work

In this paper DTN and its various challenges, its architecture and its routing protocols are presented. Blackhole attack and its requirement are also discussed. After that detailed review of blackhole detection techniques has been provided with their pros and cons. In future it is intended to propose a new methodology that detects blackhole nodes and prevent network from blackhole node.

References

[1] K.Fall, "A Delay-Tolerant Network Architecture or Challenged Internets," In Proceeding of ACM SIGCOMM, 2003, Pp. 27–34.

[2] F. Warthman, "Delay-Tolerant Networks (DTNs): A Tutorial," 2003, Version13 Mar 2013.

[3] Maurice J. Khabbaz, Chadi M. Assi and Wissam F. Fawaz,"Disruption-Tolerant Networking. A Comprehensive Survey on Recent Developments and Persisting Challenges", IEEE Communications Surveys & Tutorials, Vol. 14, No.2, Second Quarter 2012.

[4] V. Cerf, S. Burleigh, A. Hooke, L. Torgerson, R. Durst, K. Scott, E. Travis and H.Weiss,"Interplanetary Internet (IPN): Architectural Definition," Available Online: Http://Www.Ipnsig.Org/Reports/ Memo-Ipnrg-Arch-00.Pdf.

[5] Vahdat, A. & Becker, D. (2000), "Epidemic routing for partially-connected ad hoc networks", Proceedings of the 2005 ACM, New York, NY, USA, pp. 229–236.

[6] Thrasyvoulos, KonstantinosPsounisand Cauligi S. Raghavendra, "Spray and Wait: An Efficient Routing Scheme for Intermittently Connected Mobile Networks", 2005 ACM.

[7] Anders Lindgren, Avri Doria, and Olov Schel´en, "Probabilistic routing in intermittently connected networks", In Proceedings of The First International Workshop on Service Assurance with Partial and Intermittent Resources (SAPIR 2004), August 2004.

[8] Sonika Gandhi, A.N. Jaiswal, "A Method for Detecting Attacks on Delay Tolerant Network",International Journal of Advanced Computational Engineering and Networking, Issn: 2320-2106, Volume-2, Issue-6, June-20.

[9]S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard, "Prevention of Cooperative Blackhole Attack in Wireless Ad-hoc Networks", *International Conference on Wireless Networks (ICWN)*, 2003.p.1-7.

[10]Tao Gong1 and Bharat Bhargava, "Immunizing mobile ad-hoc networks against collaborative attacks using cooperative immune model", article published in Wiley Online Library (*wileyonlinelibrary.com*), *Issue: Security and Communication Networks*, 2013.p.58-68.

[11]Khanh Viet, Brajendra Panda, Yi Hu Korea, "Detecting Collaborative Insider Attacks in Information Systems", *IEEE International Conference on Systems, Man, and Cybernetics*, Seoul; 2012.p.502-507.

[12]Sanjay K. Dhurandher, I. Woungang, R. Mathur, P. Khurana, "GAODV: A Modified AODV against single and collaborative Blackhole attacks in MANETs", *IEEE 27th International Conference on AINA Workshops*, Barcelona; 2013.p.357-362.

[13]Mingchen Wang, Bin Liu and Chi Zhang "Detection of Collaborative SSDF Attacks using Abnormality Detection Algorithm in Cognitive Radio Networks", *IEEE International Conference on Communications*, Budapest; 2013.p.342 – 346.

[14] GianlucaDiniand Angelica Lo Duca, "Towards A Reputation-Based Routing Protocol to Contrast Blackholes in A Delay Tolerant Network".Ad Hoc Netw. (2012).

[15] Michiardi P, Molva R. Core: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks. In *CMS*. 2002.

[16] Fahnrich S, Obreiter P. *The Buddy System: A Distributed Reputation System Based on Social Structure.* Universitat Karlsruhe, Faculty of Informatics, Tech. Feb 2004.

[17] Schmidt RK, Leinmuller T, Schoch E, *et al.* Vehicle Behavior Analysis to Enhance Security in VANETS. In *Workshop on Vehicle to Vehicle Communications, V2VCOM*. 2008.