International Journal of Computer Science and Engineering Open Access
Survey Paper Volume-2, Issue-4 E-ISSN: 2347-2693

Black Hole Attack in Delay Tolerant Networks: A Survey

Shikha Jain[1]

[1]Department of Computer Science, Delhi University, India

www.ijcseonline.org

Received: 22/03/2014 Revised: 12/04/2014 Accepted: 26/04/2014 Published: 30/04/2014

***Abstract*—** Delay-Tolerant Network is a network above networks having unique characteristics like intermittent connectivity, longer delays and constraints on resources. DTN have the capability to survive long delays to achieve interoperability between the regional networks. Since nodes are intermittently connected with each other some new future prediction based routing protocols like Prophet, MaxProp have been proposed in this emerging areas for communication purposes. These future prediction based routing protocols depends on some easily modifiable metrics; attackers can easily forge these parameters to attack the network. This paper discusses one such popular Black-Hole attack on these routing protocols and some of the proposed solutions to mitigate their effect in the network.

***Keywords/Index Term*—** Wireless Networks, Delay Tolerant Networks, Security, Black Hole Attack

I. INTRODUCTION

A delay tolerant network (DTN) is an overlay on heterogeneous networks formed by overcoming all the technical hurdles between them. It is a new store, carry, forward network architecture and protocol suite designed to communicate among nodes when there is no continuous network connectivity. The main architectural layer that supports DTN is bundle layer having capabilities to store-and-forward messages [1]. Absence of end to end connectivity between nodes or disconnection of nodes due to less power, node mobility, sparse node density, and equipment failures creates a need for a DTN network. These DTN networks look out for the temporal paths created in the network as nodes discover their neighbors and exchange messages. Thus DTN can withstand long delays to achieve interoperability between the regional networks. Applications like satellite communication, undersea communication, e-governance, telemedicine, citizen journalism etc can take advantages of DTN characteristics. Another application is rural area DTNs, which help in connecting rural areas for developing regions using conventional transportation mediums, like buses. Therefore, security and privacy are critical for DTNs. The rest of the paper is organized as follows. Section II discusses the routing in DTNs. Section III introduces the security needs in DTN. Section IV describes the blackhole attack and Section V discusses the proposed solutions. Section VI concludes the paper.

II. ROUTING IN DTNS

Routing in DTNs is active research area. Ad hoc routing protocols do not suits to DTNs due to high node mobility which results in unstable paths. A low node density and short radio ranges also make it difficult to establish an end-to-end connectivity between the source and the destination. The routing table is also formed dynamically.

Corresponding Author: *Shikha Jain*
Department of Computer Science, Delhi University, India

Based on the applications, the links are categorized into three types:

- *Opportunistic* – These are the most random links. They are active when there is any node in the connection vicinity of the gateway or router. Examples of some routing protocols using opportunistic links are epidemic routing [2], spread and erase routing [3] etc.
- *Scheduled* – Contacts are scheduled in a specific context such as the bus schedule between two cities to carry the packets or for communication between Mars Rover Satellite and NASA labs. One such example is given in [4]
- *Probabilistic* – Contacts are based on the probability of the node which depends on the movement of the node in the direction of the destination. This contains routing protocols like MaxProp [5] and Prophet [6].

Real objects' movements usually follow repetitive patterns in UMass DieselNet [7] which is a practically existing DTN. Due to this repetitive nature, future encounters can be estimated based on the gathered history.

III. SECURITY REQUIREMENTS IN DTN

The present and the future envisioned capabilities of DTN networks are being implemented on a wide scale of applications such as Rural-Area DTNs, Airborne Networks, Sparse Mobile Networks and many more. All these applications are prone to security threats. Therefore security and privacy constraints are, considered to be important and demanding aspects of DTNs. When DTNs are used for communication, it invites many opportunities for security attacks. The attackers can compromise the information integrity, authenticity, user privacy and system performance of the network. For example, malicious nodes can arbitrarily

insert false information into the messages in DTNs. If these false messages are propagated, it results in generation of large amounts of unwanted network traffic. Due to the resource-scarcity characteristic of DTNs, the extra traffic may pose a serious threat on the operation of DTNs. Further, unauthorized access and utilization of DTN resources are another serious concern in terms of DTN security.

The nodes in DTNs are basically of two types:

- Selfish: These nodes minimize their contributions to the network community and maximize their own gains by placing conniving nodes into the network community to grab information.
- Malicious: These nodes attack proper network operations and do not consider their own gains.

DTNs security protocols have to be more invulnerable and powerful to handle these nodes. Also public key management including key distribution and revocation issues serves the foundation of any security algorithms/protocols in any wireless networks. However, public key revocation is widely recognized as an open problem in DTN due to its unique characteristics including long round-trip delay, lack of end-to-end connections and limited storage space.

IV. BLACKHOLE ATTACK IN DTN

Routing protocols belonging to the probablistic group like Prophet, Maxprop require each node to store packets and selectively transmits them when it encounters other nodes based on various metrics including the numbers of previous encounters, the last encounter time, and the estimated packet delivery, probability values to other nodes etc. However, these probabilities are provided by the mobile nodes and it is difficult to verify them due to the network non-connectivity. The malicious nodes may disseminate false delivery probabilities in undetectable way to surreptitiously increase, or decrease, their chances to be selected as next-hop nodes. For example, a node may share large delivery probability to increase its chance to be chosen, thus increasing its ability to attract messages to gain more credits, or to launch Black-Hole attacks by dropping the messages. The Black-Hole attackers aim to destruct network services by causing a severe drop in the message delivery rate or to launch Eavesdropping or Selective-Forwarding attacks. On other hand without using incentive protocol, the selfish nodes may disseminate low delivery probabilities so that they never get chosen in message forwarding to save their resources. Therefore, in DTNs, it is important to secure the contact evidence to prevent malicious nodes from providing false contact information.

V. SOLUTIONS PROPOSED TO BLACKHOLE ATTACKS IN DTN

Various solutions have been proposed to address the problem of blackhole attacker in DTNs.

Authors in [8] have proposed an Encounter-Based Routing (EBR) protocol which achieves 40% improvement in message delivery over the current state-of-the-art along with 145% increase in good put. EBR optimizes the message passing by locally observing the node's environment and using encounter-based metric. This maximizes message delivery ratio and minimizes the overhead by limiting the number of replicas of any message in the system. These message replicas are further eliminated by the security component which protects against denial-of-service attacks in the system. The routing decisions of EBR are based on the nodes' rates of encounters giving preference to the message exchanges with nodes that have high encounter rates. This results in higher probability of message delivery thus avoiding routes that may never result in delivery and so reducing the total number of message exchanges. Since the information about a node's rate of encounter is based on a local metric be tracked using a small number of variables. Therefore, EBR is able to maintain very low state overhead, as compared to other protocols that can require up to O(n) routing messages exchanged during every contact connection, and O(n2) routing state locally stored. The appropriate fraction of message replicas the nodes should exchange during the contact opportunity depends on the relative ratio of their past rates of encounter. Therefore, a malicious node can convince a node following the protocol to transmit virtually any percentage of replicas to it by advertising an ultra-high encounter value, causing all contacts to send almost all replicas to them. It then simply deletes these messages, attempting to stop, or at least slow the message delivery. The authors used Opportunistic Network (ONE) simulator [9] for evaluation.

Advantages

It achieves up to 40% improvement in message delivery over the other proposed protocols along with 145% increase in the value of good put. Moreover, it proposed simple and easy to implement rules for message replication in comparison to the complex rules found in many protocols, minimizing the chance of bugs and reducing computational complexity.

Disadvantages

This method did not reduce the packet dropping in the black hole attack. It only prevented the attackers from claiming the non-existent encounters.

Metrics used for evaluation are message delivery ratio, good put, and end-to-end delay.

In [10], the authors proposed a mutual correlation detection scheme (MUTON) for addressing the insider attacks. MUTON uses the ferry node and makes the use of the transitive property while calculating the packet delivery probability of each node. This result is then correlated to the information collected from other nodes. The authors have demonstrated the efficient detection of insider attacks. The results showed high detection rate and low false positive rate. The protocol works by making each node collects the packet delivery probabilities and the past encounter history

of any node that it discovers. The collected information is then used for estimating the changes in the delivery probabilities to other nodes due to the transitivity property. MUTON routing protocol is different from FBIDM [11] in the sense that when in MUTON, the ferry discovers a node, it uses a self-examination approach instead of cross-checking the delivery probabilities between a pair of nodes as in FBIDM. In MUTON, in order to determine the judgment of the node, the ferry only examines the node itself and compares the calculated packet delivery probability to the asserted probability by the node. A compromised node uses on and off periods to perform attacks in order to disguise its malicious behavior. During the on period, the compromised node will attack other nodes by declaring a higher random packet delivery probability to those nodes, which is larger than a threshold whereas during the off period, the compromised node behaves honestly and uses its true packet delivery probability. Such actions will increase the chance of a compromised node being selected as the next hop node for relaying packets to the nodes that are being attacked. Once selected as the next hop node, the compromised node will drop some percentage of the data it receives and undermine the normal data delivery process in the network. At every beacon time, the ferry moves along a set route and broadcast a secret inquiry message that each regular node knows to interpret. The information regarding packet delivery probabilities of the encounter node and all other nodes that the encountering node previously encountered is collected by that time. When a node receives the inquiry message from the ferry, it will share this information with the ferry secretly. The ferry then obtains the correlated information to make an educated guess about the delivery probability value and compares the estimated value to the value asserted by the node itself to determine the sanity of the node. The authors used Ns-2 [12] for simulation purposes along with RWP and Zebranet mobility model. They moved the ferry node on a fixed route at a speed of 20m/s.

Advantages

The paper achieved better detection performance than FBIDM by making use of the transitive property to calculating the delivery probability. MUTON succeeded in reducing the average detection time by 7%, which is about 100 seconds shorter than the FBIDM.

Disadvantages

It cannot stimulate the nodes' cooperation. Also it depends upon the trusted examiner called ferry node for detecting the blackhole attackers. Thus additional devices need to be deployed in the network which may not be feasible.

Prophet was used as a routing protocol. Metrics used for evaluation are false positive rate and detection time.

In [13], a method is proposed in which all the previous records of packet delivery at each point are protected so that other nodes can detect insider attacks by analyzing these packet delivery records. The un-forgeable packet is generated by using a private key and the public key generated at each node during the network setup phase. When two nodes meet, they record the number of packets exchanged between them, and generate the secure records for each other with their private keys. After that when a node discloses its previous packet records to its neighboring nodes, they check and analyze the records to decide the sanity of this node. They also detect the presence of the black hole attack instigated by the encountering node. The compromised node declares a higher random packet delivery probability to other nodes, which is larger than a threshold. Such actions will increase the chance of a compromised node being selected as the next hop node for relaying packets to the nodes that are being attacked. Once selected as the next hop node, the compromised node will drop certain percentage of the data it receives from other nodes and damage the normal data delivery process in the network. They used network simulator 2 (Ns-2) for the purpose of evaluation along with random way point model (RWP) and Zebranet mobility model for nodes movement.

Advantages

The false positive rate and the detection ratio achieved show the efficacy of the detection scheme.

Disadvantages

Malicious behavior of the node is considered only from the point of view of the attacker and not among the current network nodes. Maintaining history of packet exchanges is questionable in real-time deployments.

Prophet was used as a routing protocol. The various metrics used for evaluation are average detection time, false positive rate and detection ratio.

Authors in [14] proposed SATS that used credits to stimulate the nodes' cooperation in relaying other nodes' messages and to enforce fairness. SATS used a trust system to assign a trust value for each node. A node's trust value is high when the node actively forwards others' messages. The data is forwarded through highly trusted nodes so that the Black-Hole attacks can be avoided and network can be saved from the degradation of message delivery. To prevent such intentional attacks, the source node pays credits to the intermediate nodes for relaying their packets. The trust value of the node is based on its cooperation to deliver the messages without dropping them. If a node frequently drops messages, its trust value degrades and thus its chance to be involved in future message-forwarding decreases. SATS secures the payment and trust calculation using an offline central unit called the trusted party (Tp). Each node registers with Tp to obtain a unique identity ID, public/private key pair, and a certificate before joining the network. Tp maintains the nodes' credit account and trust values. While connecting with Tp, the nodes update their trust values by submitting the payment receipts and renewing their certificates. On receiving the receipts, Tp updates the credit accounts and trust values of the nodes which are connected to it. The source node is charged and the carriers are rewarded if and only if the destination node receives the

messages. The main motive behind the attack is to steal credits, pay less, communicate freely, and falsely improve their trust values. SATS can be incorporated with any data-forwarding protocol. The main parameters taken into consideration while selecting the next hop node in SATs are the nodes' trust values and the probability with which the nodes can deliver the message. Only the intermediate nodes along the first successful delivery path are rewarded. For each delivered message, the last intermediate node composes a proof of message delivery. The node contacts Tp to submit the batch of receipts it has accumulated during the process. If all verifications pass, Tp charges the source node, rewards the intermediate nodes, and updates the intermediate nodes' trust values. The nodes' signatures enable Tp to ensure that the listed nodes in a receipt have been indeed participated in forwarding the message. This is important to secure the payment and trust value of node Ti. Ti is low for the Black-Hole attackers and the less cooperative nodes but it is high for the normal nodes that actively forward others' messages. The underlying idea of the trust system is that the destination node is receiving a message only if the carriers that have forwarded the message are cooperating. Therefore, for each delivered message, Tp increases the trust values of the carriers that forwarded the message. SATS aims to recognize the good nodes and forward the messages through them. In this way, SATS can avoid the Black-Hole attackers in message forwarding and penalize them by not making credits. SATS used Matlab for their evaluation purposes.

Advantages

SATS handles both selfishness and black-hole attacks in DTNs.

Disadvantages

If centralized trust systems are attacked, the node's trust values can also be attacked and changed. The nature of these systems always creates the possibility of getting easily attacked.

Prophet was used as a routing protocol and the metrics used for evaluation is delivery rate.

VI. CONCLUSION AND FUTURE WORK

This paper describes the blackhole attacks in DTNs which act as a major security threat. The author also presented the proposed solutions to the attacks and discussed the advantages and disadvantages of each. Some of the challenges of routing in DTNs are considered in the proposed protocols but still a lot more work needs to be done. The author proposes to carry out work on security solutions to black-hole attacks which are independent of the routing protocols used in DTNs.

REFERENCES

[1] F. Warthman. "Delay-tolerant networks (dtns): A tutorial", 2003.

[2] Amin Vahdat and David Becker. "Epidemic routing for partially connected ad hoc networks", Technical Report CS-2000-06, Department of Computer Science, Duke University, April 2000.

[3] Shikha Jain, Sandhya Aneja. "Spread and Erase: Efficient Routing Algorithm Based on Anti-Message Info Relay Hubs for Delay Tolerant Networks", In Computer Networks & Communications (NetCom), Vol. 131 (2013), pp. 643-651.

[4] Guoliang Liu; Krishnamani, J.; Sunderraman, R.; Yingshu Li, "Prediction-based routing with packet scheduling under temporal constraint in delay tolerant networks," Performance Computing and Communications Conference (IPCCC), 2013 IEEE 32nd International , vol., no., pp.1,7, 6-8 Dec. 2013

[5] J.Burgess, B.Gallagher, D.Jensen and B.N.Levine, "Maxprop: Routing for vehicle-based disruption-tolerant networking," in Proceedings of IEEE Infocom, April 2006.

[6] A. Lindgren, A. Doria, and O. Schelen, "Probabilistic routing in intermittently connected networks," in Mobile Computing and Communications Review, 2003.

[7] A. Balasubramanianm, B. Levine, and A. Venkataramani. "DTN routing as a resource allocation problem", In Proc. of ACM SIGCOMM, 2007.

[8] S. C. Nelson, M. Bakht and R. Kravets, "Encounter-based Routing in DTNs", in Proceedings of IEEE Infocom, Rio De Janeiro, Brazil, pp.846-854, Apr. 2009.

[9] http://www.netlab.tkk.fi/tutkimus/dtn/theone

[10] Yanzhi Ren, Mooi Choo CHuah, Jie Yang, Yingying Chen, "MUTON: Detecting Malicious Nodes in Disruption-Tolerant Networks".

[11] M. Chuah, P. Yang, and J. Han, "A ferry-based intrusion detection scheme for sparsely connected adhoc networks," in Proceedings of first workshop on security for emerging ubiquotous computing, 2007.

[12] http://www.isi.edu/nsnam/ns

[13] Yanzhi Ren, Mooi Choo Chuah, Jie Yang, Yingying Chen, "Detecting Blackhole attacks in Disruption-Tolerant Networks through packet exchange recording".

[14] M. E. Mahmoud, M. Barua, X. Shen, "SATS: Secure Data-Forwarding Scheme for Delay-Tolerant Wireless Networks."

AUTHORS PROFILE

Shikha Jain is an Assistant Professor in the Department of Computer Science, BR Ambedkar College of the Delhi University, India. Shikha Jain received her B.Sc. degree (First Class Hons.) in Physics from Delhi University, India in 2008 and the M.Sc. degree from the Institute of Informatics and Communication, University of Delhi, India in 2010. Her research Interests include Cognitive Radio Networks, Delay Tolerant Networks, and Security in Wireless Networks and Ad hoc Networks.