ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014

Data Protecting Against Flood Attacks

P.Sudha[1], B.Sivananthan[2]

PG Scholar-M.E, CSE, Gnanamani College of Engineering, Namakkal, T.N, India[1]

Assistant Professor, CSE, Gnanamani College of Engineering, Namakkal, T.N, India[2]

Abstract: Using the mobility of nodes and the opportunistic contacts among nodes the Disruption Tolerant Networks (DTNs) performs the data communications. DTNs are vulnerable to flood attacks in which attackers send as many packets or packet replicas as possible to the network, in order to overuse the limited network resources. The existing system adopts claim-carry-and check: each node itself counts the number of packets or replicas that it has sent and claims the count to other nodes; the receiving nodes carry the claims when they move and cross-check if their carried claims are inconsistent when they contact. It provides rigorous analysis on the probability of detection. But the time interval and rate limit are main issues in this scheme. So we propose the no rate limiting to defend against flood attacks in DTNs by sending data's simultaneously with no time interval and no packets rate limit. The proposed scheme provides the effectiveness and efficiency with extensive result.

Keywords: Disruption Tolerant Network, Routing, Flood Detection, Security.

I. INTRODUCTION

Disruption Tolerant Networks (DTNs) enable data transfer when mobile nodes are only intermittently connected. Lack of consistent connectivity, two nodes can only exchange data when they move into the transmission range of each other (which is called a contact between them).DTNs employ contact opportunity for data forwarding with "store- carry-and-forward", when a node receives some packets, it stores these packets in its buffer, carries them around until it contacts another node, and then forwards them. The contacts between nodes are opportunistic and the duration of a contact may be short because of mobility. Due to the limitation in bandwidth and buffer space, DTNs are vulnerable to flood attacks. In flood attacks maliciously or selfishly motivated attackers inject as many packets as possible into the network, or instead of injecting different packets the attacker's forward replicas of the same packet to as many nodes as possible. The two types of attack packet flood attacks and replica flood attack, respectively. Flooded packets and replicas can waste the precious bandwidth and buffer resources, prevent benign packets from being forwarded and thus degrade the network service provided to good nodes. Moreover, mobile nodes spend much energy on transmitting/receiving flooded packets and replicas which may shorten their battery life. It is urgent to secure DTNs against flood attacks.

Although many schemes have been proposed to defend against flood attacks on the Internet and in wireless sensor networks, they assume persistent connectivity and cannot be directly applied to DTNs that have intermittent connectivity. In DTNs, little work has been done on flood attacks, despite the many works on routing, data dissemination, black hole attack, wormhole attack, and selfish dropping behavior. The packets flooded by outsider attackers (i.e., the attackers without valid cryptographic credentials) can be easily filtered with authentication techniques. However, authentication alone does not work when insider attackers (i.e., the attackers with valid cryptographic credentials) flood packets and replicas with valid signatures. Thus, it is still an open problem is to address flood attacks in DTNs.

The ability to transport, or route, data from a source to a destination is a fundamental ability all communication networks must have. Disruption-tolerant networks (DTNs) are characterized by their lack of connectivity, resulting in a lack of instantaneous end-to-end paths. In these challenging environments, popular ad hoc routing protocols fail to establish routes. This is due to these protocols trying to first establish a complete route and then, after the route has been established, forward the actual data. However, when instantaneous end-to-end paths are difficult or impossible to establish, routing protocols must take to a "store and forward" approach, where data is incrementally moved and stored throughout the network in hopes that it will eventually reach its destination. A common technique used to maximize the probability of a message being successfully transferred is to replicate many copies of the message in the hope that one will succeed in reaching its destination. This is feasible only on networks with large amounts of local storage and internodes bandwidth relative to the expected traffic. In many common problem spaces, this inefficiency is outweighed by the increased efficiency and shortened delivery times made possible by taking maximum advantage of available unscheduled forwarding opportunities.

In others, where available storage and internodes throughput opportunities are more tightly constrained, a more discriminate algorithm is required. Many nodes may launch flood attacks for malicious or selfish purposes. They may also exploit flood attacks to increase their communication throughput. In DTNs, a single packet usually can only be delivered to the destination with a probability smaller than 1 due to the opportunistic connectivity. If a selfish node floods many replicas of its own packet, it can increase the likelihood of its packet being delivered. The three routing strategies in DTNs are single-copy routing, multi-copy routing and propagation routing. In propagation routing, a node replicates a packet to another encountered node if the latter has more frequent contacts with the destination of the packet. A packet flood

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014

attacker floods packets destined to random good nodes in each contact until the contact ends or buffer is full.

II. RELATED WORK

A. Routing

An introduction to routing in networks with intermittent connectivity, and we cover several representative routing mechanisms. We begin by describing the main approach for message delivery in case of intermittent connectivity. After a brief overview of the Delay Tolerant Networking architecture, we describe the main classes of routing protocols for networking with intermittent connectivity and several representative solutions. Deterministic routing uses accurate estimates of time intervals when node links, called contacts, are available to schedule transmissions. Stochastic routing techniques are either zero-knowledge, where nothing is known about node contacts and state, or use delivery estimation to approximate a metric for end-to-end message delivery that contributes to more intelligent forwarding decisions. Active stochastic routing techniques rely on controlling the trajectory for some mobile nodes to pickup, carry and deliver messages to improve communication capability in sparse networks.

DTNs are a new area of wireless ad-hoc networking that shows great potential in many important applications. Routing and end-to-end message delivery in DTNs is possibly the most difficult problem in an environment where network resources are very limited and connectivity is scarce. The connectivity limitation affects the ability of distributing network-wide node and link information that could be used to optimize network operations. When contacts cannot be deterministically predicted, routing algorithms must rely on probabilistic methods that estimate future contacts with limited accuracy and on multi-copy forwarding that further strains the reduced network resources.

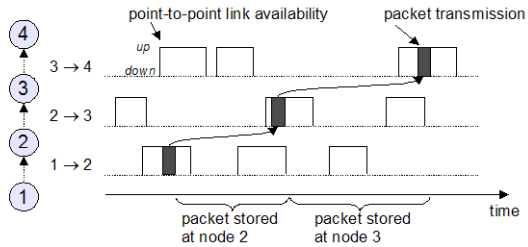

Figure 1. Packet delivery from source 1 to destination 4 is possible without a contemporaneous end-to-end path, provided nodes buffer packets until a link to the next hop becomes available.

Figure 1 illustrates such a scenario. A route from source node 1 to destination 4 passes through nodes 2 and 3. Since there is no time instant when all three links are functioning, the standard IP forwarding approach would cause the packet to be dropped after reception at node 2. With a different approach, the packet could be buffered at node 2 until the 2 ® 3 link becomes available. Similarly, the packet would wait at node 3 before it could be forwarded to the destination 4. Thus, even though no instantaneous source-destination path is ever available for the time considered, a simple store-and-forward protocol could deliver packets successfully. If the node is meanwhile moving, this approach is called store-and-carry.

Several other challenged networks with similar intermittent connectivity have attracted researchers' attention, such as MANETs, wireless sensor networks, acoustic underwater networks and networks for internet access in undeveloped areas. Wireless ad-hoc networks for disaster recovery also suffer from sporadic connectivity, caused mainly by node mobility and by a communication channel with variable quality. A common name for such networks with intermittent connectivity is Delay or Disruption Tolerant Networks (DTN).

B. Disruption Tolerant Network

Disruption Tolerant Network consists of a sequence of time-dependent communication opportunities, called contacts, during which messages are transferred from source towards the destination. Contacts are described by capacity; direction, the two endpoints, and temporal properties such as begin/end time, and latency. Routing in this network with time-varying edges involves finding the optimal contact path in both space and time, meaning that the forwarding decision must schedule transmissions considering temporal link availability in addition to the sequence of hops to the destination. This problem is exacerbated when contact duration and availability are nondeterministic. Contact types are classified and persistent contacts are those always available. On-Demand contacts require some action in order to instantiate. A scheduled contact is an agreement to establish a contact at a particular time, for a particular duration. Opportunistic contacts present themselves unexpectedly. Predicted contacts are based on a history of previously observed contacts or some other information. As DTN routing must operate on a time-varying multigraph, message forwarding requires scheduling in addition to next-hop selection. To optimize the network performance, such as delivery rate or latency, DTN routing must select the right contact defined by a next-hop and a transmission time. If a contact is not known when a message is received from the upper layer, the bundle layer will buffer it until a proper contact occurs or until the message is dropped. In conditions of a DTN with sporadic contact opportunities, the main objective of routing is to maximize the probability of delivery at the destination while minimizing the end-to-end delay.

III. PROPOSED SCHEME

A. Claim-Carry-and-Check

Claim-Carry-and-Check is a detection method. Using this method we can avoid the packet flood attacks as well as replica flood attacks. The proposed system overcomes the problem of time delay and packets rate limit in the existing system. Multiple users can send file simultaneously with no time interval and no packets rate limit. Each sender can select the path to send the packets to receiver. If the file packet is successfully sent to receiver IP address, the sender receives the acknowledgement from the receiver then the backup of the file in the intermediate node will be deleting automatically. This can avoid the traffic problem in Disruption Tolerant Networks (DTNs) and also provides the effective results.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014

B. Packet Flood Detection

The Claim-Carry-and-Check is used to detect the packet flood attacks in the Disruption Tolerant Networks. During the contact opportunity the file packets are sending from source to destination with the intermediate nodes. After the packet reached to destination the backup files are deleting automatically in the subsequent path in the intermediate nodes. So we can avoid the packet flood attacks. It provides the effective result of packet flood detection. One attacker may send a packet with a dishonest packet count to its colluder, which will forward the packet to the network. Certainly, the colluder will not exchange the dishonest claim with its contacted nodes. However, so long as the colluder forwards this packet to a good node, this good node has a chance to detect the dishonest claim as well as the attacker. Thus, the detection probability is not affected by this type of collusion.

C. Replica Flood Detection

The Claim-Carry-and-Check detection method is also used to detect the replica flood attacks. In the Disruption Tolerant Network the sender can send many copies to the receiver with the intermediate nodes .In our scheme the propagation routing is used to perform the data commununications in the Disruption Tolerant Networks. The scheme deletes the copies, when one node sent the copies to other node. Sender only have an own copy of the file packets. So we can avoid the replica flood attacks.

D. Security

Our scheme provides the complete protection to the data. During the routing, if any attackers will attack the good nodes the scheme is to detect the attackers and also provides security to the nodes until the file packet is send to receiver. If any problem is occur the scheme will provides the protection and receiver can receive the trusted data.

E. Detection Rate

The effect of parameter k in different routing protocols. Generally when k increases, the detection rate also increases because the inconsistent packets are exchanged to more nodes and have more chances to be detected. When k=0, no attacker is detected in Spray-and-Wait, since no metadata is exchanged for detection. However, attackers can still be detected in the other three algorithms, because the inconsistent packets are forwarded to multiple nodes and the node that receives two inconsistent packets can detect the attacker. Among these protocols, Propagation achieves the highest detection rate since it replicates inconsistent packets the most number of times. The results when each attacker launches the basic attack independently for a varying number of times. As the attackers launch more attacks, the detection rate quickly increases for obvious reasons.

F. Detection Delay

The CDF (Cumulative Distributed Function) of detection delay when Propagation is used as the routing protocol on the Reality trace. For comparison, the CDF of routing delay (i.e., from the time a packet is generated to the time it is delivered) is also plotted. Here, no lifetime is set for packets. It can be seen that 90 percent of the attacks can be detected by our scheme within 10 days. On the contrary, within 10 days only 60 percent of data packets can be delivered by the routing protocol. Hence, the detection delay is much lower than the routing delay.

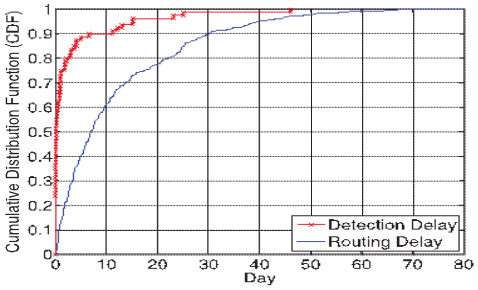

Figure2.The detection delay compared with the routing delay of propagation.

IV. CONCLUSIONS

The proposed system focuses on the no rate limiting to defend against flood attacks in Disruption Tolerant Networks (DTNs).Multiple users can send the data's simultaneously with no time interval and no packets rate limit. So the receiver receives the file packets easily without time delay. The packet flood attacks and replica flood attacks are detected using the claim- carry -and - check detection method. The detection scheme provides the protection to the data and also avoids the attackers to send inconsistent file packets to the Disruption Tolerant Networks. The propagation routing exploits the effective results of detection rate and detection delay. So receiver can receive the trusted data without any delay. The scheme uses efficient constructions to keep the computation, communication and storage cost low. So this scheme is effective to detect flood attacks and evaluate the effectiveness and efficiency with extensive results.

ACKNOWLEDGMENT

The authors express their thanks to the Management and Principal, Head Of the Department (CSE) in Gnanamani College of Engineering.

REFERENCES

[1] K. Fall, "A Delay-Tolerant Network Architecture for Challenged Internets," Proc. ACM SIGCOMM, pp. 27-34, 2003.
[2] P. Hui, A. Chaintreau, J. Scott, R. Gass, J. Crowcroft, and C. Diot, "Pocket Switched Networks and Human Mobility in Conference Environments," Proc. ACM SIGCOMM, 2005.
[3] M. Motani, V. Srinivasan, and P. Nuggehalli, "PeopleNet: Engineering a Wireless Virtual Social Network," Proc. MobiCom, pp. 243-257, 2005
[4] J. Burgess, B. Gallagher, D. Jensen, and B. Levine, "Maxprop: Routing for Vehicle-Based Disruption-Tolerant Networks," Proc. IEEE INFOCOM, 2006.
[5] S.J.T.U.Grid Computing Center, "Shanghai Taxi Trace Data," http://wirelesslab.sjtu.edu.cn/, 2012.
[6] J. Mirkovic, S. Dietrich, D. Dittrich, and P. Reiher, Internet Denial of Service: Attack and Defense Mechanisms. Prentice Hall, 2005.
[7] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Proc. IEEE First Int'l Workshop Sensor Network Protocols and Applications, 2003.
[8] E. Daly and M. Haahr, "Social Network Analysis for Routing in Disconnected Delay-Tolerant MANETs," Proc. MobiHoc, pp. 32-40, 2007.
[9] W. Gao, Q. Li, B. Zhao, and G. Cao, "Multicasting in Delay Tolerant Networks: A Social Network Perspective," Proc. ACM MobiHoc, 2009.

[10] F. Li, A. Srinivasan, and J. Wu, "Thwarting Blackhole Attacks in Disruption-Tolerant Networks Using Encounter Tickets," Proc. IEEE INFOCOM, 2009.
[11] Q. Li and G. Cao, "Mitigating Routing Misbehavior in Disruption Tolerant Networks," IEEE Trans. Information Forensics and Security, vol. 7, no. 2, pp. 664-675, Apr. 2012.
[12] Y. Ren, M.C. Chuah, J. Yang, and Y. Chen, "Detecting Wormhole Attacks in Delay Tolerant Networks," IEEE Wireless Comm. Magazine, vol. 17, no. 5, pp. 36-42, Oct. 2010.
[13] H. Zhu, X. Lin, R. Lu, X.S. Shen, D. Xing, and Z. Cao, "An Opportunistic Batch Bundle Authentication Scheme for Energy Constrained DTNS," Proc. IEEE INFOCOM, 2010.

BIOGRAPHIES

P.Sudha received the BE(CSE)degree from Gnanamani College of Tchnology, Anna University of technology, Coimbatore in 2011. Now she is doing PG degree at Gnanamani College of Engineering, Namakkal.

B.Sivananthan received UG, PG degree from Anna University affiliated colleges. He is currently working as Assistant Professor in the CSE Department at Gnanamani College of Engineering, Namakkal. He has more than 6 years of teaching experience at college.