SHIELDING IN CONTRAST TO FLOOD ATTACKS IN DISRUPTION TOLERANT NETWORKS

GOUSE MODEEN SHAIK, GOUSIYA SULTHANA SHAIK, P. SUBHAN BASHA

 # Student of M.Tech, SSITS, Rayachoti, Kadapa, Andhra Pradesh, India

 # Student of M.Tech, SSITS, Rayachoti, Kadapa, Andhra Pradesh, India

 # Assistant Professor,Department of CSE, SSITS, Rayachoti, Kadapa, Andhra Pradesh, India

Abstract So as to study the consequences of flood attacks on DTN routing, we can run simulations on the MIT Reality trace [15]. We consider three general routing strategies in DTNs. 1) Single-copy routing (e.g., [16], [4]): a node deletes its own copy of the packet, soon after promoting a packet obtainable. As a result, every packet has only one copy in the network. 2) Multi-copy routing (e.g., [17]): the source node of a packet showers a convinced quantity of copies of the packet to other nodes and every copy is independently transmitted using the single-copy scheme. The extreme amount of copies that individual packet can have is static. 3) Propagation routing (e.g., [15], [18], [19]): As a node determines it suitable path to forward a packet to another come-across node that is according to the routing table, it duplicates that particular packet to the come-across node and keeps the copy of its own. There is no predetermined restriction on the quantity of replicas a packet could have. Through simulations, SimBet [4], Spray-and-Focus [17] (allowed number of copies for each packet is three) and Propagation are the representatives of the routing approaches, respectively. During propagation, a particular node duplicates a packet to the other come-across node in case the latter has more regular association with the endpoint of the packet.

I. INTRODUCTION

In the simulations presented here, a packet flood attacker floods packets intended to arbitrary good nodes in every interaction up until the contact ends or the communicated node's buffer is filled. A replica flood attacker duplicates the packets it has produced to each come across node that does not own a fake. Every single good node produces thirty packets on the 121st day of the Reality trace, and each attacker does the similar in replica flood attacks. Every packet perishes in 60 days. The buffer size provided for each node here is 5 MB, bandwidth is 2 Mbps and packet size is 10 KB. Fig. 1 shows the effect of flood attacks on packet delivery ratio. Packet flood attack can dramatically reduce the packet delivery ratio of all three types of routing. When the fraction of attackers is high, replica flood attack can significantly decrease the packet delivery ratio of single-copy and multi-copy routing, but it does not have much effect on propagation routing.

II. LITERATURE SURVEY

1.Sencun Zhu, and Guohong Cao suggest that many nodes might commence flood attacks in support of malevolent or egocentric purposes. Malevolent nodes, which are nodes intentionally positioned by opponent or subverted by opponent by means of mobile phone worms, commence attacks to obstruct network and misuse the resources of previous nodes. Flooded packets along with replicas can misuse valuable bandwidth as well as buffer resources, put off benign packets from being forwarded and consequently mortify network service offered to superior nodes.

2. J. Yang and Y. Chen proposed that node density as well as unpredictable node ad hoc networks are deployed since they do mobility, lengthwise connections are tough not necessitate permanent network to preserve. Due to delay tolerant networks infrastructure for instance base stations or dynamics, deterministic data forwarding is routers. Due to self-organizing environment, certain in situations where the network is an adhoc network is formed in flooded, as well as data forwarding instantaneous where the entire participating procedure does not contain time restriction.

3. C. Karlof and D. Wagner [2] suggests symmetric key cryptography were projected.that concerns of Security in ad-hoc networks are comparable to those within sensor

III. EXISTING AND PROPOSED SYSTEM

In the current system Store and forward approach nodes store packets if they cannot find the next corresponding hop node to deliver them to destinations. The first node stores the packets in its memory and then transmits the selectively to the corresponding nodes with various metrics including the last encounter time, the numbers of previous encounters uses lot buffer and time then the estimated packet delivery probability values to other nodes. In this process it is very hard to verify the network information sparseness and the intermittent connectivity between the nodes.

In DTN systems it cannot provide a contact opportunity for data forwarding with store forward and store carry activities. Here when a node receives some packets of data, then the nodes stores packets in its buffer and carries them around until it contacts the corresponding node, and then forwards them. The contacts between nodes are opportunistic and the period of a contact may be very short because of mobility or movement in the nodes, the usable bandwidth which is only available during the opportunistic contacts is a limited resource. Also, mobile nodes may have limited buffer space. As the current system is having limitation in bandwidth and buffer space controlling in DTNs which 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. For convenience, we call the two types of attack packet flood attack and replica flood attack, respectively.

Disadvantages

1. Selfishly motivated attackers may inject many packets as possible into the network to drain the network resources.
2. Bandwidth resources and buffer space are very vulnerable to flood attacks.
3. store-carry-and-forward are big problem in DTN's
4. Attacks generated in DTN's are The two types of attack packet flood attack and replica flood attack.
5. It is not easy for an adversary to compromise nodes within the network and launch insider attacks using the compromised nodes.
6. They cannot address insider attacks launched by compromised nodes.
7. Insider attacks can cause significant problems in networks

PROPOSED SYSTEM

In this proposed scheme we design rate limiting and giving security to defend against flood attacks in DTNs. In our approach, every node has a limit of packet transmission over the number of packets that they send over the source node and also can send to the network in various time intervals. Every node has a limitation over

the number of replicas that it can generate for each packet. In the proposed scheme the two limits are used to moderate and mitigate replica and packet flood attacks respectively. Our research provides detailed theory and algorithm for detection of claim and carries check with filtered traffic controlling various attacks. The main scope and activity of the project is to detect if a node has violated its rate limits.

Advantages

- The main aim of the project is to design a enhanced technique to detect if a node has violated its rate limit
- The proposed system provides detection and controlling of packet flood attack and replica flood attacks.
- The proposed System provides claim carry and check.
- Our basic idea of detection is claim-carry-and-check.
- Each node itself counts the number of packets or replicas that it has sent out, and claims the count to other nodes.

IV. MODULES OF THE PROJECT

Node Creation & Packet Splitting

That every packet generated by nodes is unique. This can be implemented by including the source node ID and a locally unique sequence number, which is assigned by the source for this packet; we assume that each packet has a lifetime. The packet becomes meaningless after its lifetime ends and will be discarded.

Activities of the Module

1. In this process, the sample network formation is created.
2. The dynamic network formation is based on node creation & node connection. The node creation is based on set of node deployment.
3. To study the problem of transmitting a large file over paths of potentially many hops, and seek optimal ways of splitting the file into a large number of packets over multiple paths, each with different operating parameters over its hops, to minimize the end-to-end delay.
4. The form of delay we consider consists primarily of random queueing delay and transmission delay at each intermediate hops.
5. The file which is to be transfer is to be selected & it is splitted into number of packets for data transmission.

Trusted Authority

When a user joins the network, she requests for a rate limit from a trusted authority which acts as the network operator. In the request, this user specifies an appropriate value of L based on prediction of her traffic demand. If the trusted authority approves this request, it issues a rate limit certificate to this user, which can be used by the user to prove to other nodes the legitimacy of her rate limit.Each

node has a rate limit certificate obtained from a trusted authority. The certificate includes the node's ID, its approved rate limit L, the validation time of this certificate and the trusted authority's signature. The rate limit certificate can be merged into the public key certificate or stand alone.

Activities of the Module

- When a user joins the network, the user requests for a rate limit from a trusted authority which acts as the network operator.
- In the request, this user specifies an appropriate value of L based on prediction of user file size.

- If the trusted authority approves this request, it issues a rate limit certificate to this user, which can be used by the user to prove to other nodes the legitimacy of her rate limit.
- To prevent users from requesting unreasonably large rate limits.
- The request and approval of rate limit may be done offline. The flexibility of rate limit leaves legitimate users' usage of the network unhindered. So that the certificate is verified, & send to user.

3.Packet flood detection

- To detect the attackers that violate their rate limit L, we must count the number of unique packets that each node as a source has generated and sent to the network in the current interval.
- However, since the node may send its packets to any node it contacts at any time and place, no other node can monitor all of its sending activities.
- The node's rate limit certificate is also attached to the packet, such that other nodes receiving the packet can learn its authorized rate limit L.
- If an attacker is flooding more packets than its rate limits and thus a clear indicator of attack.

4.Claim Détection

P-claim is added by the source and transmitted to later hops along with the packet. T-claim is generated and processed hop-by-hop. Specifically, the source generates a T-claim and appends it to the packet. When the first hop receives this packet, it peels off the T-claim; when it forwards the packet out, it appends a new
T-claim to the packet. This process continues in later hops. Each hop keeps the P-claim of the source and the T-claim of its previous hop to detect attacks

Activities of the Module

- Claim-carry-and-check can also be used to detect the attacker that forwards a buffered packet more times than its limit l.
- Specifically, when the source node of a packet or an intermediate hop transmits the packet to its next hop, it claims a transmission count which means the number of times it has transmitted this packet (including the current transmission).
- Thus, if an attacker wants to transmit the packet more than l times, it must claim a false count which has been used before. Similarly as in packet flood attacks, the attacker can be detected.

5.Assessment

- In this module, the performance of the algorithm is evaluated by using Graph representation.
- This shows that the proposed framework is able to adapt to changes in time & cost parameter values while the other approaches cannot.
- The performance gap between the proposed framework and other approaches is at the high level compare to other approaches.
- It provides better flexibility in the query processing process.

V. DISCUSSION AND CONCLUSION

We conclude that the proposed system provides rate limiting with attacks controlling in DTNs, and a provides an novel scheme that utilizes carry and claim check probabilistically and discover the damage of rate limit in DTN environments has been proposed. The proposed scheme is a well organized structure for keep the working and communication storage at very low cost.

Moreover the lower bound and upper bound discovery probability is also examined. As the mobility is very widespread and the trace-driven simulations presented on the widespread provides a new scheme to detect flood attacks and it reach such efficiency in a well organized and secured way. The proposed scheme is provided in a disseminated manner and not banking on any online dominant consultant or resources, and hence the proposed scheme fits the surroundings of DTNs. As the current trace-based learning on campus wireless system illustrates that different nodes have heterogeneity in contact prototype and authenticates usage of social network analysis and giving secured support of data forwarding in delay tolerant networks. As the network is ad-hoc the Concerns of Security in ad-hoc networks are comparable to those within sensor networks and were enumerated in literature; Due to various restriction in bandwidth as well as buffer space the proposed delay tolerant networks are susceptible to control the flood attacks. In our future recommendations we design extensive trace-driven simulations for controlling advanced vampire attacks on mobility and also combine the flood attacks detection in an efficient way. Our enhancements are proposed to a distributed manner, not relying on any online central or de central authority without any infrastructure, which well fits the environment of DTNs. Besides, it can tolerate a small number of attackers to collude. Our Extensive enhancements include trace-driven simulations with effective flood attacks and it achieves such effectiveness in an efficient way. Besides,it can tolerate a small number of attackers to collude

REFERENCES

To Lie or to Comply: Defending against Flood Attacks in Disruption Tolerant Networks Qinghua Li, Student Member, IEEE, Wei Gao, Member, IEEE, Sencun Zhu, and Guohong Cao, Fellow, IEEE.

[2]. J. Mirkovic, S. Dietrich, D. Dittrich, and P. Reiher, Internet Denial of Service: Attack and Defense Mechanisms. Prentice Hall, 2005.

[3]. 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.

[4]. E. Daly and M. Haahr, "Social Network Analysis for Routing in Disconnected Delay-Tolerant MANETs," Proc. MobiHoc, pp. 32-40, 2007.

[5]. J. Burgess, B. Gallagher, D. Jensen, and B. Levine, "Maxprop: Routing for Vehicle-Based Disruption-Tolerant Networks," Proc. IEEE INFOCOM, 2006.

[6]. Q. Li, W. Gao, S. Zhu, and G. Cao, "A Routing Protocol for Socially Selfish Delay Tolerant Networks," Ad Hoc Networks, vol. 10, no. 8, November 2012.

[7]. W. Gao, Q. Li, B. Zhao, and G. Cao, "Multicasting in Delay Tolerant Networks: A Social Network Perspective," Proc. ACM MobiHoc, 2009.

[8]. W. Gao, G. Cao, M. Srivatsa, and A. Iyengar, "Distributed Maintenance of Cache Freshness in Opportunistic Mobile Networks," IEEE ICDCS, 2012.

[9]. F. Li, A. Srinivasan, and J. Wu, "Thwarting blackhole Attacks in Distruption-Tolerant Networks Using Encounter Tickets," Proc. IEEE INFOCOM, 2009.

[10]. 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.

[11]. U. Shevade, H. Song, L. Qiu, and Y. Zhang, "Incentive-Aware Routing in DTNS," Proc. IEEE Int'l Conf. Network Protocols (ICNP '08), 2008.

[12]. 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.

[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.

[14]. B. Raghavan, K. Vishwanath, S. Ramabhadran, K. Yocum, and A. Snoeren, "Cloud Control with Distributed Rate Limiting," Proc. ACM SIGCOMM, 2007.

[15]. N. Eagle and A. Pentland, "Reality Mining: Sensing Complex Social Systems," Personal and Ubiquitous Computing, vol. 10, no. 4, pp. 255-268, 2006.

[16]. Q. Li, S. Zhu, and G. Cao, "Routing in Socially Selfish Delay Tolerant Networks," Proc. IEEE INFOCOM, 2010.

[17]. T. Spyropoulos, K. Psounis, and C.S. Raghavendra, "Efficient Routing in Intermittently Connected Mobile Networks: The Multiple-Copy Case," IEEE/ACM Trans. Networking, vol. 16, no. 1, pp. 7790, Feb. 2008.

[18]. A. Lindgren, A. Doria, and O. Schelen, "Probabilistic Routing in Intermittently Connected Networks," ACM SIGMOBILE Mobile Computing and Comm. Rev., vol. 7, no. 3, pp. 19-20, 2003.

[19]. W. Gao and G. Cao, "On Exploiting Transient Contact Patterns for Data Forwarding in Delay Tolerant Networks," Proc. IEEE 18th Int'l Conf. Networks Protocols (ICNP), 2010.

[20]. J. Burgess, G.D. Bissias, M. Corner, and B.N. Levine, "Surviving Attacks on Disruption-Tolerant Networks without Authentication," Proc. ACM MobiHoc, 2007.