ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

Volume 3, Special Issue 3, March 2014

2014 International Conference on Innovations in Engineering and Technology (ICIET'14)
On 21st & 22nd March Organized by

K.L.N. College of Engineering, Madurai, Tamil Nadu, India

Thwarting Flood Attacks in Disruption Tolerant Networks Based On Claim and Key Verification

G.Pushpa Rega[1], S.Hasan Hussain[2]

Department of Computer Science and Engineering, Syed Ammal Engineering College, Ramanathapuram, India

Department of Computer Science and Engineering, Syed Ammal Engineering College, Ramanathapuram, India

Abstract— Disruption Tolerant Networks (DTNs) make the most of the mobility of nodes and the opportunistic contacts among nodes for data communications. Owing to the restriction in network resources such as contact prospect, buffer space and bandwidth, DTNs are open to flood attacks. To guard against flood attacks in DTNs, Rate limiting based on certificate was proposed. In Rate limiting, every node has a bound over the number of packets that it can generate in each time interval and a bound over the number of replicas that it can generate for each packet. The main objective is to detect the node who send the packets more than their limit and to mark limit exceeding nodes as attackers .Here detection adopted claim-carry-check technique, where every node counts the number of packets or replicas that it has sent and send that count to other nodes, a particular node after receiving the counts from the contacted nodes, just carry that claims when they travel across the network, and cross-check if their carried claims are conflicting when they communicate with other nodes. Using Rate limit certificate only the flood attacker who exceeds the rate limit was identified. To overcome this, the proposed approach uses key. Key will be generated for the node who wish to send packets less than the rate limit. In addition to rate limit certificate, key also be checked at every contact. AES and MAC algorithm will be used for key generation. Based on keys, attackers who sends packet within the rate limit can also be easily identified.

Keywords— DTN, security, flood attack, detection, Key.

I.INTRODUCTION

A disruption-tolerant network (DTN) is a network intended so that temporary or intermittent communications problems, limitations and anomalies have the least possible adverse impact.Disruption Tolerant Networks (DTNs) [1] has transportable nodes usually carried by human beings [5], [6], vehicles [8], [25], etc. DTNs aid data transfer when portable nodes are only occasionally connected, making them suitable for applications where no communication transportation is available such as military scenarios and rural areas. Two nodes can only swap data when they are in the particular communication range of each other because of lack of consistent connectivity. In DTNs data forwarding takes place using one technique called "store-carry-and-forward"[12]. This technique works as follows, when a node obtains some packets, it stores these packets in its buffer, carries them until it communicates other node, and then forwards those buffered packets to them. The usable bandwidth available during the contacts is a limited resource because the contacts between nodes are opportunistic and the contact may be short duration for the reason that of mobility. In addition to that mobile nodes may have restricted buffer space. Owing to the restriction in bandwidth and buffer space, DTNs are exposed to flood attacks. In flood attacks, cruelly or egoistically stimulated attackers instil as many packets as possible into the network, or instead of inserting different packets the attackers 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. The expensive bandwidth and buffer resources are usually wasted by these flood attacks and it also prevents gentle packets from being forwarded. So the network service provided to good nodes gets degraded. Moreover, mobile nodes pay out much power on transmitting/receiving flooded packets and replicas which may cut down their battery life. Therefore, it is a critical situation to make safe DTNs beside flood attacks.

Although so many approaches have been planned to preserve against flood attacks on the Internet [7] and in wireless sensor networks [2], they presume

constant connectivity and cannot be directly useful to DTNs that have broken connectivity. In DTNs, little work has been done on flood attacks, despite the many works on routing [10], [8], [26], data dissemination [14], [27], black hole attack [15], wormhole attack [17], and selfish dropping behaviour [12], [24].In DTN Rate limiting [11] was engaged to shield against flood attacks in DTNs. In this approach, each and every node has a bound over the number of packets that it can send to the network in each time interval. Each and every node also has a bound over the number of replicas that it can generate for each packet. The two limits say L and l are used to mitigate packet flood and replica flood attacks, respectively. If a node violates or exceeds its rate limits, it will be detected and its data traffic will be sorted. In this manner, the amount of flooded traffic can be inhibited. We generally use three routing methods for forwarding packets. They are singlecopy routing[19],[10],Multicopy routing[13] and Propagation routing[9],[4],[20].

Here main objective is to detect node that violates the rate limit and mark rate limits exceeding node as attacker. On the Internet and in telecommunication network it is easy to find out the violation of rate limit because we have the egress router and base station for accounting each user's traffic. But it is challenging in DTNs due to lack of communication structure and constant connectivity. Since a node moves around and may send data to any contacted node, it is very difficult to count the number of packets or replicas sent out by this node. Basic idea of finding inconsistency is claim carry-and-check. Each node itself calculates the number of packets or replicas that it has sent out, and claims the count to other nodes; the receiving nodes carry the claims around when they move across the network, swap some claims when they contact, and cross-check if these claims are conflicting. If an attacker forwards more packets or replicas than its limit, it has to use the same count in more than one claim according to the pigeonhole principle and this inconsistency may lead to detection. Using this technique, only Attackers who exceed the rate limit can be identified. Key based approaches will be used to detect all kind of attackers.

Based on this idea, packet flood and replica flood attacks was detected using different cryptographic structure .This approach offers probabilistic detection because of opportunistic contacts in DTNs. The more traffic an attacker floods, the more likely it will be detected. The amount of claims exchanged in a contact is controlled by system parameters that will flexibly adjust the detection probability. Using extensive trace-driven simulations, the success and competence of our scheme are evaluated.

II. RELATED WORK

A few recent works [15],[8], [21], [12], [17], [24] also deal with security matters in DTNs. Li et al. [15] considered the blackhole attack.Inorder to attract packets, some of the malicious node counterfeit routing strategies and use those strategies to drop all received packets. This is called blackhole attack. An approach *Encounter ticket* was proposed by them to prove the survival of relations and prevent the falsification of routing metrics, but this approach cannot be used to tackle flood attacks.

Burgess, Gallagher, Jensen, and Levine [8] proposed one routing protocol called *MaxProp* to route messages via sporadically connected nodes. It fully depends on prioritizing packets in buffer based on ranking packets by considering the cost assigned to its destination. It can efficiently perform routing but attacks cannot be identified by this protocol.

Li and Cao [24] also proposed a dispersed method to diminish packet drop attacks. Every node in the network is required to maintain a contact record based on its previous contacts. Whenever a particular node encounters other node, it will send packets along with its contact record to the encountered node. Usually a malicious node always provides a forged record to prevent it from detection. So based on these records one node can easily identify the selfish nodes

Ren et al.[17] studied wormhole attacks in DTNs. Chen and Choon [21] proposed a credit-based approach and Shevade et al. proposed a gaming-based approach [12] to provide reasons for packet forwarding. Here pair wise Tit For Tat(TFT) mechanism was used to identify the bad behaviour of nodes.Owing to the lack of consistent end-to-end paths, network conditions variability, and long response delay in DTNs, TFT practical for DTNs is challenging. Nelson,Bakht, and Kravets[16] discussed one routing technique called Encounter based routing(EBR) which based on this property "*the future rate of node encounters can be roughly predicted by past data".*EBR routing maximizes delivery ratios while minimizing overhead and delay but it is vulnerable to denial of service attack.

Zhu,Li and Cao [23], [28] addressed some privacy issues. However, these work do not deal with flood attacks. Other works (e.g., Sprite [3]) discourage violence by comparing the amount of network resources that a node can use with the node's donations to the network in terms of forwarding. This approach has been proposed for mobile adhoc networks. It cannot be applied to DTNs because of inconsistent connectivity among nodes. Another recent work [18] proposed a batch authentication protocol for DTNs.To save the computation cost,multiple packet signatures were verified in an cumulative way. This work is opposite to ours, and their protocol can also be used in our scheme to additional cut the working out cost of verification.

Corresponding to our work, Natarajan et al. [22] also proposed a scheme to decide resource misuse in DTNs. In their approach, the activities of nodes were monitored by the gateway of a DTN.If an expected behaviour is deviation from expected behaviour, there is an clear indication of attacks. With this comparision, attacks can be easily identified. This scheme works in a totally distributed manner and requires no special nodes but it requires a special gateway for counting.

III. EXISTING SYSTEM

In Disruption Tolerant Networks (DTNs), due to the constraint in network assets such as contact chance and buffer space, DTNs are exposed to flood attacks. Rate limiting was proposed to defend against flood attacks in DTNs. In Rate limiting, every node has a bound over the number of packets that it can generate in each time interval and a bound over the number of replicas that it can generate for each packet. The main objective is to detect the node who send the packets more than their limit and to mark limit exceeding nodes as attackers. Here detection adopted claim-carry-and check. There are two kind of attacks possible in DTNs.they are packet flood attack in which attackers flood networks by sending many packets and replica flood attack in which attackers flood networks by sending many replicas of particular packet. Every node has packet limit L and replica limit l.Using Rate limiting, node who exceeds any one of the or both the limits are identified as attacker.

A.Packet Flood Detection

The number of unique packets that each and every source node has generated and sent to the network in the current interval T must be counted to detect the attackers who violate their rate limit L. Main idea is to permit the node itself count the number of unique packets that it has sent out, and claim the current packet count along with a little secondary information such as its ID and a timestamp in each packet sent out. Every other node receiving the packet can find out its authorized rate limit L using node's rate limit certificate which is attached to the packet. If an attacker is flooding more packets than its rate limit, it has to fraudulently declare a count lesser than the actual value in the flooded packet, from the time when the actual value is larger than its rate limit and thus an obvious sign of attack. The claimed count must have been used before by the attacker in another claim. Pigeonhole principle used for guarantee the reusage of claim and one can say two claims are inconsistent. Wherever they move, the particular nodes carry the claims of the received packets from the attackers. Checking is performed for inconsistencies between their collected claims at every communication between two nodes. When an inconsistency is found, an attacker will be easily identified.

B.Replica Flood Detection

The main objective of the attackers is to flood the networks by sending large no of replicas into the network for depleting the resources. Claim-carry-and-check mainly used for detecting 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 replica count which means the number of times it has spreaded the replicas of that packet (including the current transmission). The next hop come to know the node's replica limit l for the packet based on if the node is the source or an intermediary node and which routing protocol is used and make sure that the claimed count is contained by the correct series.

C. Claim Construction

Packet count claim(P-claim) and Transmission count claim(T-claim) are mainly used for detecting packet flood and replica flood respectively.P-claim generally created by source and it will not be changed during its transmission. But T-claim will be processed hop by hop. When a node receives a packet, it first peels off the T-claim and add its T-claim to the packet then forwards it to next hop.

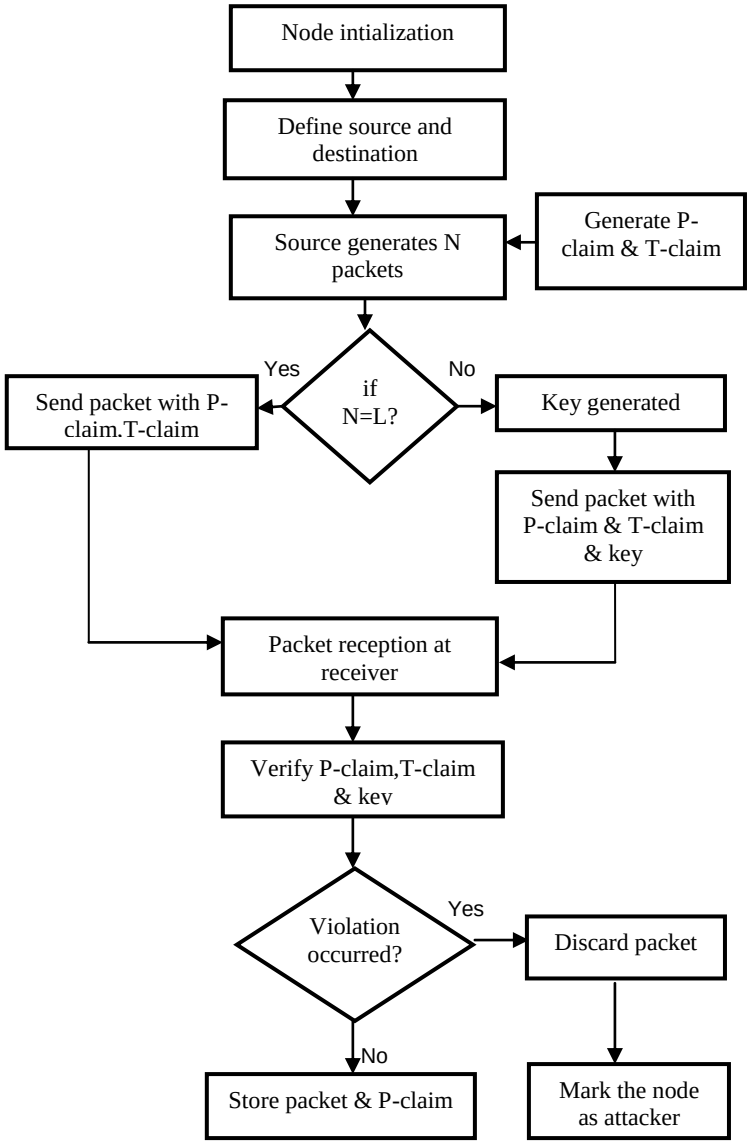

Fig. 1. Shows that how the attackers will be detected using key.

IV. PROPOSED SYSTEM

In the existing system, we can identify only the attackers who exceed the rate limit with the help of rate limit certificate. But if they sends packet within the rate limit, they won't be identified in the Disruption Tolerant Networks .So as to identify that kind of attacks we are going to use key. If the original user sends packet less than rate limit value, then they have to generate key with that packet count. So that key is transferred to each and every node along with the packets. At the receiver side Rate limit certificate and key will be checked. Based on the key, we can easily identify the attackers who sending unwanted packets within the rate limit. The key will be generated based on AES algorithm.

.

A.Advantages of Proposed System

By using keys, Attackers who send packets within the rate limit can be easily identified
In this system, Network efficiency and its performance can be improved by identifying attackers using keys.
Network bandwidth and buffers can be efficiently used.
Most of the packets will be prevented from loss.

To improve the efficiency in network utilization and to detect the attackers, the following components are required

B.Node création & packet Generation

In this process, the sample network formation is created. The dynamic network formation is based on node creation & node connection in MANET. The node creation is based on set of node deployment. After the node deployment, the connections are provided. We 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. The form of delay we consider consists primarily of random queuing delay and transmission delay at each intermediate hops. The file which is to be transfer is to be selected & it is splitted into number of packets for data transmission. The splitting process is based on file length, according to that the files are splitted.

C.Trusted Authority

When a user joins the network, he will request a trusted authority for a rate limit, where authority acts as the network operator. In the request, this user specifies a proper value of L based on calculation of user file size. After getting that value L, authority just checks the request for approval. If the trusted authority approves this request, it issues a rate limit certificate to this user. The user can prove its authenticity to other nodes with rate limit certificate. Increase (decrease) of his demand will be predicted. According to that prediction, he can request for a higher (lower) rate limit. The demand and sanction of rate limit may be done offline. The litheness of rate limit leaves genuine user's usage of the network unconstrained. So that the certificate is verified, & send to user.

C.Claim Détection

Using Claim-carry-and-check technique, the attacker who forwards a buffered packet more times than its limit can be easily identified. Distinctively, when the source node of a packet or an intermediate hop forwards 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). The next hop come to know the node's limit for the packet based on if the node is the source or an intermediary node and which routing protocol is used and make sure that the claimed count is within the correct range. Thus, whenever an attacker wants to transmit the packet more than its limit, it must claim a false count which has been used before. Similarly in packet flood attacks, the attacker can be detected. At each contact rate limit certificate will be checked for inconsistencies.

D.Flood Detection

The number of unique packets that each and every source node has generated and sent to the network in the current interval T must be counted to detect the attackers who violate their rate limit L. Main idea is to permit the node itself count the number of unique packets that it has sent out, and claim the current packet count along with a little secondary information such as its ID and a timestamp in each packet sent out. Every other node receiving the packet can find out its authorized rate limit L using node's rate limit certificate which is attached to the packet. If an attacker is flooding more packets than its rate limit, it has to fraudulently declare a count lesser than the actual value in the flooded packet, from the time when the actual value is larger than its rate limit and thus an obvious sign of attack. The claimed count must have been used before by the attacker in another claim. Pigeonhole principle used for guarantee the reusage of claim and one can say two claims are inconsistent. Wherever they move, the particular nodes carry the claims of the received packets from the attackers. Checking is performed for inconsistencies between their collected claims at every communication between two nodes. When an inconsistency is found, an attacker will be easily identified. In the same way replica attackers also identified. Based on AES, key will be generated for the node who wishes to send packet within their rate limit. Then attackers will be identified based on rate limit certificate and key.How the attackers will be detected shown in Fig.1.

E.Performance Evaluation

In this module, Graph representation is used for evaluating the performance of the algorithm.This shows that when compared to other approaches, the proposed framework has the ability to adjust to change in time & cost parameter values. Since in the real world, it is infrequent that the same unit instances are recorded in a large number of data sources, and the costs are typically different. The performance gap between the proposed framework and other approaches is at the high level compare to other approaches. Better elasticity in the query processing process will be provided.

V.CONCLUSION AND FUTURE WORKS

Rate Limiting technique is used for diminishing flood attacks in DTNs using Rate limit Certificates from the Trusted Authority, and proposed a scheme which exploits claim-carry-and-check to probabilistically detect the violation of rate limit in DTN environments. Our scheme uses proficient constructions, so that the computation, communication and storage cost are kept low. It works in a distributed manner, not relying on any online central authority or infrastructure, which well fits the environment of DTNs. Moreover, it can put up with a small number of attackers to conspire.

In future work, in order to identify attacker who sends packet within the rate limit and to improve resource utilization, Key based security will be used along with Rate Limiting technique to increase efficiency in resource utilization.AES and MAC algorithm going to be used for key generation.

REFERENCES

[1] K. Fall, "A Delay-Tolerant Network Architecture for Challenged Internets," Proc. ACM SIGCOMM, pp. 27-34, 2003.
[2] 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.
[3] S. Zhong, J. Chen, and Y.R. Yang, "Sprite: A Simple, Cheat-Proof, Credit-Based System for Mobile Ad-Hoc Networks," Proc. IEEE INFOCOM, vol. 3, pp. 1987-1997, 2003.
[4] 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.
[5] 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.
[6] M. Motani, V. Srinivasan, and P. Nuggehalli, "PeopleNet: Engineering a Wireless Virtual Social Network," Proc. MobiCom, pp. 243-257, 2005.
[7] J. Mirkovic, S. Dietrich, D. Dittrich, and P. Reiher, Internet Denial of Service: Attack and Defense Mechanisms. Prentice Hall, 2005.
[8] J. Burgess, B. Gallagher, D. Jensen, and B. Levine, "Maxprop: Routing for Vehicle-Based Disruption-Tolerant Networks," Proc. IEEE INFOCOM, 2006.
[9] N. Eagle and A. Pentland, "Reality Mining: Sensing Complex Social Systems," Personal and Ubiquitous Computing, vol. 10, no. 4, pp. 255-268, 2006.
[10] E. Daly and M. Haahr, "Social Network Analysis for Routing in Disconnected Delay-Tolerant MANETs," Proc. MobiHoc, pp. 32-40, 2007.
[11] B. Raghavan, K. Vishwanath, S. Ramabhadran, K. Yocum, and A. Snoeren, "Cloud Control with Distributed Rate Limiting," Proc. ACM SIGCOMM, 2007.
[12] U. Shevade, H. Song, L. Qiu, and Y. Zhang, "Incentive-Aware Routing in DTNS," Proc. IEEE Int'l Conf. Network Protocols (ICNP '08), 2008.
[13] 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. 77-90, Feb. 2008.
[14] W. Gao, Q. Li, B. Zhao, and G. Cao, "Multicasting in Delay Tolerant Networks: A Social Network Perspective," Proc. ACM MobiHoc, 2009.
[15] F. Li, A. Srinivasan, and J. Wu, "Thwarting Blackhole Attacks in Distruption-Tolerant Networks Using Encounter Tickets," Proc. IEEE INFOCOM, 2009.
[16] S.C. Nelson, M. Bakht, and R. Kravets, "Encounter-Based Routing in Dtns," Proc. IEEE INFOCOM, pp. 846-854, 2009.
[17] 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.
[18] 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.
[19] Q. Li, S. Zhu, and G. Cao, "Routing in Socially Selfish Delay Tolerant Networks," Proc. IEEE INFOCOM, 2010.
[20] 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.
[21] B. Chen and C. Choon, "Mobicent: A Credit-Based Incentive System for Disruption Tolerant Network," Proc. IEEE INFOCOM, 2010.
[22] V. Natarajan, Y. Yang, and S. Zhu, "Resource-Misuse Attack Detection in Delay-Tolerant Networks," Proc. Int'l Performance Computing and Comm. Conf. (IPCCC), 2011.
[23] Z. Zhu and G. Cao, "Applaus: A Privacy-Preserving Location Proof Updating System for Location-Based Services," IEEE INFOCOM, 2011.
[24] 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.
[25] S.J.T.U.Grid Computing Center, "Shanghai Taxi Trace Data," http://wirelesslab.sjtu.edu.cn/, 2012.
[26] 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.
[27] W. Gao, G. Cao, M. Srivatsa, and A. Iyengar, "Distributed Maintenance of Cache Freshness in Opportunistic Mobile Networks," IEEE ICDCS, 2012.
[28] Q. Li and G. Cao, "Efficient and Privacy-Preserving Data Aggregation in Mobile Sensing," Proc. IEEE Int'l Conf. Network Protocols (ICNP '08), 2012.