Addressing Flood Attacks In DTN: Prevent Malicious Invasion

Mahalaxmi. R
II[nd] Year – M.E. CSE
Srinivasan Engineering College
Perambalur
Tamil Nadu, India

Sambath. K
HOD/ CSE
Dhanalakshmi Srinivasan Institute of Technology
Perambalur
Tamil Nadu, India

Manjula. P
HOD / IT
SrinivasanEngineering College
Perambalur
Tamil Nadu, India

Abstract **- Distribution tolerant network utilize the mobility of nodes for contact opportunity, the mobile nodes are move around some situation. Due to limitation in network resource and bandwidth, the number of attacks possible in the network. The node send the number of replica to the network, it defect against the flood attack ,each node rate limit against the flood attack. The claim carry check scheme is proposed against flood attack, The homophoric encryption scheme is used for encryption of data, the P claim and T claim scheme is used For verification of data. The proper buffer management reduce the flood attack in dynamic environment(i.e. above 1000 mobile node)it can tolerate the large flood attack. The claim carry check is proposed against flood attack, homophoric encryption scheme is used for security of data. The P claim and T claim scheme is used for verification of data. The proper buffer management reduces the flood attack in dynamic environment. It can tolerate the large flood attack.**

Keywords - DTN, security, flood attack, detection

1. INTRODUCTION

Delay Tolerant Network (DTN) is suffered from the lack of infrastructure security. In mobile Ad hoc network may suffered by disruption .The security guarantees are difficult to establish in a network without persistent connectivity because the network hinders complicated cryptographic protocols, hinders key exchange, and each device must identify other intermittently visible devices. Solutions have been typically modified from mobile ad hoc network and distributed security.

Many attacks are possible in mobile Ad hoc network. Mobile nodes are the different mobility. Due to contact opportunity of mobile nodes many packets of data get collude. DTN network vulnerable to flood attack and packet replica attack. To avoid the attacks each node count the number of packet sends by node at particular time interval. Claim-Carry-Check scheme is used for count the number of send by node. Each node count the number of packets send out to another node. Claim-Carry-and-Check scheme is used for inconsistency of node contact. The proper buffer management is used for avoid the attacks in Delay Tolerant Network (DTN).The encryption technique is used for encryption of data.

Different type of encryption technique is used for encrypting the data. The new type of encryption technique is homorphic encryption technique and verification of data for security purpose. The different type of claim scheme is used for verification of data; the claim scheme is used for checking and reduces the cost verification. This scheme is uses the pigeonhole principle checking the node contact opportunity for forward the packet. Different type of routing scheme is used for forward the packet.

Propagation routing scheme is used for forward the packet to all the nodes. This type of application is used for any type of network infrastructure. Claim-Carry-and-Check, Each node itself counts the number of packets or replicas that it has sent out, and the claims count to another nodes. The claim scheme is used for checking the cross checks of the node. It is used for avoid the flood attacks in Disruption Tolerant Network.

To avoid the flood attacks in DTN (delay tolerant network) and utilize the resource without any wastage new method of buffer management. It is used for avoid the flood and packet attacks. The mobile nodes are simultaneously changed their location and communicating with other mobile devices. While communicating with other devices tracking of mobile nodes is very important. Because of fewer infrastructures the mobile nodes are can not properly communicating with other device.

Each node counts the contact nodes and the packet size of each data packet. Validity of data packets, packet size of data and its rate limit use the resource without any

waste. Flooding is the main problem in Disruption Tolerant Network. Due to flooding many packet of data get colluded. To avoid the flooding and also avoid the collision of data packet the new type of method is proposed. Due to flooding Dos (Denial of Service) attack and it bring the big traffic in the network. Because of high traffic server and host cannot be connected. Different type of protocol is used for avoid the attacks in Disruption Tolerant Network.

Different type of method is used to detect the flood attacks in Disruption Tolerant Network. Many type of malicious attacks are present in Disruption Tolerant Network. To detect the kind of attacks in DTN and to act against the kind of attacks Disruption Tolerant Network. The new scheme is used for Disruption Tolerant Network to avoid the attacks and utilize the resource without any wastage.

Claim-Carry-and-Check scheme is used for checking the contact opportunity of node, check the availability of node contact and then only node send the packet of data. Claim-Carry-and-Check can also be used to detect the attacker that forwards a buffered packet more times than its limit l.

- Replica flood attack
- Packet flood attack

The cryptographic technique is used for protect the data from the attacker. The attacker launches the many attacks to the network. The authentication and verification scheme is used for detecting the attacks and preventing the attacks in the network. Mobile nodes are having the different mobility and these mobile nodes want to communicate with other device.

2. RELATED WORK

Delay and disruption tolerant networks have been proposed to address data communication challenges in network scenarios where an instantaneous end-to-end path between a source and destination may not exist, and the links between nodes may be opportunistic, predictably connectable, or periodically-disconnected. To describe the store-and-forward and custody transfer concepts that is used in DTNs.

It present simulation results that the usefulness of the custody transfer feature, and a message ferry in improving the end-to-end message delivery ratio in a multi hop scenario where link availability can be as low as 20%. In particular results indicate that one can achieve a delivery ratio as high as 90-99%with appropriate buffer allocations. It is also provide some preliminary insights on the design factors that influence the end to end delivery ratio, e.g., the link availability patterns and buffer allocation strategies.

The usefulness of the custody transfer feature and a message ferry in improving the end-to end message delivery ratio in a multi hop scenario where link availability can be as low as 20%. In particular results indicate that one can achieve a delivery ratio as high as 90-99%with appropriate buffer allocations. It is also provide some preliminary insights on the design factors that influence the end to end delivery ratio, e.g., the link availability patterns and buffer allocation strategies. It do not explore the issue of joint custodianship in this paper. This is left for future work. In addition, the traffic demands from one group to another do not vary with time and that the link availability follows exponential on off distribution.

The traffic demands and the link available. It is may be changing dynamically so one may not be able to predict the maximum required buffer size for the base station. So, more intelligent distributed buffer management schemes still impractical.

If the sending DTN node cannot find a route to the destination of the message, it will trigger its underlying ad hoc network layer to look for a route or neighboring nodes that are closer to the destination than itself. In addition, it will send request message at the DTN layer. The DTN nodes that hear the custody request message will send a custodian accept message to the sender of that request if it has available buffers.

The ad hoc network routing layer, all DTN nodes that receive a route reply message with the DTN option flag will set a bit in the appropriate position (according to its hop distance from the sending node of the route request) to indicate buffer availability before relaying the route reply message. That way, the sender knows whether or not that it can use that route. In a DTN environment, an end-to-end route may not exist. Thus, dual-layer (at ad hoc network routing and DTN layers) approach allows us to identify downstream nodes messages.

3. OUR SYSTEM AND ASSUMPTIONS

Claim-Carry- and-Check

To detect the attackers that violate the rate limit L, It must count the number of unique packets that each node as a source has generated and sent to the network in the current interval. 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. our idea is to let the node itself count the number of unique packets that it, as a source, has sent out, and claim the up-to-date packet count (together with a little auxiliary information such as its ID and a timestamp)in each packet sent out. In Claim-Carry-and-Check scheme, each node counts the number of packets. More Secured Claim scheme is proposed for contact opportunity of each node two pieces of metadata are added to each packet, Packet Count Claim (P-claim) and Transmission Count Claim (T-claim).P-claim and T-claim are used to detect packet flood and replica flood attacks, respectively. To increase the privacy of proposed system homophobic encryption techniques is proposed for more security. It provides the more authentications and checking the each node available and get a contact of the only it can send the packet of messages.

It provide the more security and finding the spoofing of attacker and prevent the attacks finally the information send to destination. The T-claims of all the packets transmitted in a contact should be signed by the transmitting node. Since the contact may end at any unpredictable time, each received T-claim must be

individually authenticated. A naive approach is to protect each T-claim with a separate public-key signature, but it has high computation cost in signature generation and verification.

4. SYSTEM PRELIMINARIES

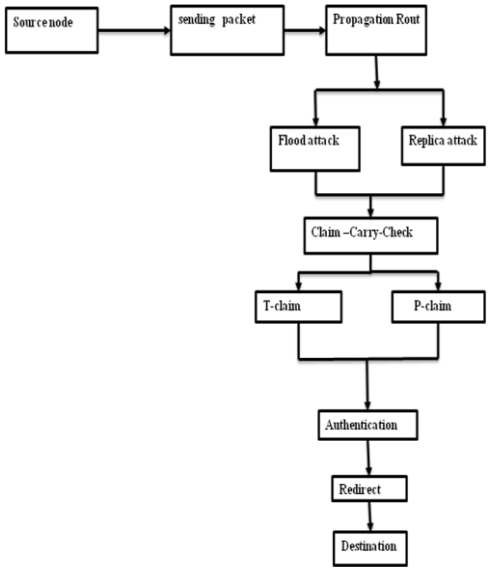

Figure 1. System Architecture

The above Figure shows the proposed system design. It consists of number blocks. Each and every block have the different function. The DTN (Delay Tolerant Network) consists of number of nodes. It make intermediate connectivity's, the source node send the packet of information to destination node .Different type of routing is used for send the information from the source node to destination node. Because of in insensitivity many flooding is possible .The packet attacks and flood attacks in the network.

The attacker also pass the many packet of messages to the network. Flood attack and packet flood attacks in the network .The packet replica is also possible in the network. The claim and carry scheme is introduced for provide the contact opportunity of each node availability and also checking the number packet send out node. After verifying the contact opportunity each node the packet of message redirected to destination.

In T-claim issued by node R. The signature is discarded since it has been verified. It does not need to store its own ID and is not useful for inconsistency check. Then the compacted T claim is R, ct e H32; where e H32 is a 32-bit hash remainder defined similarly as H8 . Suppose W has collected n T-claims generated by R. Then the compact structure of these T-claims is CR ¼ R; locators; ½ He321; ct1 . . . ; ½ e H32n. The locators are randomly and independently generated by W for R. It shared by all the T-claims issued by R. The P-claim node W gets: the source node ID S, packet count cp, timestamp t, and packet hash H. To check inconsistency, W first uses S and t to map the P-claim to the structure Ci S. Then it reconstructs the hash remainder of H using the locators in Ci S.

The redirection is a stealthy attack to flood attack detection. For replica flood attacks, the condition of detection is that at least two nodes carrying inconsistent T-claims can contact. suppose the attacker knows that two nodes A and B never contact. Then, it can send some packets to A, and invalidly replicate these packets to B. In this scenario, this attacker cannot be detected since A and B never contact. Similarly, the stealthy attack is also harmful for some routing protocols like Spray-and-Wait in which each packet is forwarded from the source to a relay and then directly delivered from the relay to the destination.

Attacks detection

Delay Tolerant Networks (DTNs) routing protocols and a thorough quantitative evaluation of many protocols is used for detecting the flood attacks.DTN (Delay tolerant network) DTN protocols, according to their use of three main techniques: queue management, forwarding and replication. Queue management orders and manages the messages in the node's buffer, forwarding selects the messages to be delivered when there is a contact and finally replication bounds the number of replicas in the network. This protocol is used for improve the delivery ratio and overhead and delay.

Routing Techniques

Single copy routing

Mobile networks are wireless networks where most of the time there does not exist complete path from source to destination. A Path is highly unstable and may break soon after it has been discovered. Epidemic algorithms is applied to routing, as a flooding method in the context of intermittently connected mobile network. This algorithm is used for improve the performance. Randomized routing algorithm is used for route the messages from source to destination with probability Single copy routing after forward the packet the node delete the own copy of data.

Multi copy routing

Multi copy routing in delay tolerant network three type of routing scheme is used such as message delay and message delivery ratio and also the buffer occupancy. Direct Transmission is perhaps the most basic DTN routing scheme. Epidemic routing achieves very low delay among routing schemes for mobility-assisted routing. The epidemic routing scheme has large overhead, and also limits the message overhead in terms of buffer management and buffer occupancy.

The multi copy routing in terms of message delivery ratio and delay messages delivered ratio. Multi copy routing scheme is used in the unicast and multicast communication. The source node of a packet sprays a certain number of copies of the packet to other nodes and each copy is individually routed using the single-copy strategy. The maximum number of copies that each packet can have is fixed.

Propagation Routing

The node find it appropriate to forward a packet to another encountered node, it replicates that packet to the encountered node and keeps its own copy. There is no preset limit over the number of copies.

A packet can have to transmit. When very high traffic in delay tolerant network routing table updates the nearby node and send the packet. Static routing in legacy of network for transfer the information. In Propagation, a node replicates a packet to another encountered node if the latter has more frequent contacts with the destination of the packet.

Routing Scheme in DTN

Protocols are proposed for a data delivery in DTNs. The Two nodes are encounter one another, It will exchange all the messages are currently carry with each other. Every node will be able to send information to every other node. So the packets are basically flooded through the network. This represents the fastest possible way in which information can be disseminated in a network with unlimited storage and unlimited bandwidth constraint. Delay Tolerant Networks are a reality. With a large amount of different devices such as the Smart-phones, netbooks, thin-clients being routing protocols for over lays, they are not designed to take into account the underlying technologies when making routing decisions, unlike our predicate routing system.

Store-Carry-and-Forward

In store and forward scheme 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. A store-carry-and-forward approach in which messages are buffered for extended intervals of time until an appropriate forwarding opportunity is recognized. Spray-and-wait and epidemic routing, or deterministic approach such as history-based, model-based, coding-based and variations of these approaches is used for transfer the information. The buffered technique is used for transfer the information.

the queuing management technique is used for transfer the information. The forwarding level: If a node is congested, then bundles must not be forwarded to it temporarily. Some bundles may also be transferred from a congested node to other nearby nodes until congestion is resolved. The nodal buffer level: Here, the most appropriate bundles to be dropped are identified, including the ones being received, so as to reduce buffer space usage.

FIFO -First in first out

The message that was first entered into the queue is the first message to be dropped.

MOFO-Evict most forwarded first

This policy requires keeping track of the number of times each message has been forwarded. The message that has been forwarded the most is the first to be dropped, thus giving messages that have not been forwarded fewer times a chance.

Claim-Carry–and-Check

In claim carry check scheme each node update the neighbor node and update the node contact in delay tolerant network. To detect the attackers that violate their rate limit L, It must count the number of unique packets that each node as a source has generated and sent to the network in the current interval. 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. Each node update the packet count to other node.

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 limit, it has to dishonestly claim a count smaller than the real value in the flooded packet, since the real value is larger than its rate limit and thus a clear indicator of attack.

Cryptographic Technique

Homomorphic encryption is a form of encryption which allows specific types of computations to be carried out on cipher text and obtain an encrypted result which decrypted matches the result of operations performed on the plaintext. For instance, one person could add two encrypted numbers and then another person could decrypt the result, without either of them being able to find the value of the individual numbers.

5. EXPERIMENTAL EVALUATION

DTN Forming

Delay and Disruption Tolerant Networks (DTNs) are networks that aim to bring low-cost best-effort connectivity to challenged environments with no or limited infrastructures. Nodes in DTNs are often highly mobile and experience intermittent connectivity. DTNs can be deployed in developing countries and are poised to play a key part in future space networks. Key differences between DTN and other networks, e.g. Sensor Networks are:

No End To End Path

Node mobility creates partitions in the network. it cannot assume that there is a complete end to end path between a source and destination. If a path does exist it is assumed to be unstable. Instead, an end to end path exists over time, as nodes move and forward messages to each other.

High Message Delays

The opportunistic nature of DTNs means messages that are delivered often experience high delays. Delays can are typically on the order of minutes or hours, but could potentially be days depending on the exact scenario.

Routing

When a node finds it appropriate (according to the routing algorithm) to forward a packet to another encountered node, it replicates that packet to the encountered node and keeps its own copy. There is no preset limit over the number of copies a packet can have. In our simulations, Semi Bit Spray-and-Focus (three copies allowed for each packet) and Propagation are used as representatives of the three routings Strategies, respectively. In Propagation, a node replicates a packet to another encountered node if the latter has more frequent contacts with the destination of the packet.

The store-and-forward and custody transfer concepts that are used in DTNs. Then, it present simulation results that illustrate the usefulness of the custody transfer feature, and a message ferry in improving the end-to-end message delivery ratio in a multi hop scenario where link availability can be as low as 20%. In particular, our results indicate that one can achieve a delivery ratio as high as 90-

99% with appropriate buffer allocations. It is also provide some preliminary insights on the design factors that influence the end to end delivery ratio, e.g., the link availability patterns and buffer allocation strategies. DTNs employ such 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. Since the contacts between nodes are opportunistic and the duration of a contact may be short because of mobility, the usable bandwidth which is only available during the opportunistic contacts is a limited resource.

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 attackers' forward replicas of the same packet to as many nodes as possible.

The two types of attack packet flood attack and replica flood attack, respectively. Flooded packets and replicas can waste the precious bandwidth and buffer resources, prevent packets from being forwarded and thus degrade the network service provided to good node.

Claim Checking

T Claim and P Claim is used for avoid the in consistency. When node A transmits a packet m to node B, it appends a T-claim to m. The T-claim includes A's current transmission count ct for m and the current time t. P claim

When a source node S sends a new packet M (which has been generated by S and not sent out before) to a contact node, it generates a P-claim as follows: P new packet S has created and sent to the network in the current time interval. S increases CP by one after sending m out.

The P-claim is attached to packet M as a header field, and will always be forwarded along with the packet to later hops. When the contacted node receives this packet, it verifies the signature in the P-claim, and checks the value of cp. If CP is larger than L, it discards this packet; otherwise, it stores this packet and the P-claim.

6. CONCLUSION

It employed rate limiting to mitigate flood attacks in DTNs, and proposed a scheme which exploits Claim-Carry-and-Check to probabilistically detect the violation of rate limit in DTN environments. It uses the efficient constructions to keep the computation, communication and storage cost low. It is also, analyzed the lower bound and upper bound of detection probability. Extensive trace-driven simulations showed that scheme is effective to detect flood attacks and it achieves such effectiveness in an efficient way. The scheme works in a distributed manner, not relying on any online central authority or infrastructure, which well fits the environment of DTNs. It can tolerate a small number of attackers to colluded.

REFERENCES

1. J.Burgess,B.Gallagher,D.Jensen,and B.Levine, "Maxprop: Routing for Vehicle-Based Disruption-Tolerant Networks", Proc.IEEE INFOCOM,2006.
2. E.Delay and M.Haahr, "Social Network Analysis for Routing in Disconnected Delay-Tolerant MANETs", Proc. MobiHoc, pp.32-40, 2007.
3. K.Fall, "A Delay-Tolerant Network Architecture for Challenged Internets",Proc.ACM SIGCOMM,pp.27-34,2003.
4. W.Gao, Q.Li, B.Zhao, and G.Cao, "Mulicasting in DelayTolerant Networks: A Social Network Perspective", Proc. ACM MobiHoc, 2009.
5. P.Hui, A.Chaintreau, J.Scott, R.Gass, J.Crowcraft, and C.Diot, "Pocket Switched Networks and Human Mobility in Conference Environments", Proc.ACM SIGCOMM, 2005.
6. F.Li, A.Srinivasan, and J.Wu, "Thwarting Blackhole Attacks in Disruption-Tolerant Networks Using Encounts Tickets",Proc.IEEE INFOCOM,2009.
7. M.Motani,V.Srinivasan, and P.Nuggehalli, "PeopleNet:Engineering Wireless Virtual Social Network", Proc.MobiCom,pp.243-257,2005.
8. S.C.Nelson, M.Bakht, and R.Kravets, "Encounter-Based Routing in Dtns",Proc.IEEE INFOCOM,pp.846-854,2009.
9. B.Raghavan, K.Vishwanath, S.Ramabhadran, K.Yocum, and A.Snoeren "Cloud Control with Distributed Rate Limiting", Proc.ACM SIGCOMM,2007.
10. 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.
11. Z.Zhu and G.Cao, "Applaus: A Privacy-Presrving Location Proof Updating System for Location-Based Services",IEEE INFOCOM,2011.