ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Distributed Analysis of Node Imitation Attacks in Disruption Tolerant Networks

Mr. Puttu Chandra Sekhar
M.Tech Student,
Department of CSE,
Sri Venkateswara Institute of
Science & Technology, Kadapa, A.P.

Ms.T.Lakshmi Prasanna, M.Tech
Assistant Professor,
Department of CSE,
Sri Venkateswara Institute of
Science & Technology, Kadapa, A.P.

ABSTRACT:

Disruption Tolerant Networks (DTNs) make use of opportunistic acquaintances between nodes for data relations. DTNs build feasible to spread data while mobile nodes are only erratically associated, make them appropriate for applications where no other announcement transportation is available such as armed forces scenarios and rural areas. Being without reliable connectivity, two nodes are capable of exchanging data when they move into the announcement scope of each other (which is called a contact among them). DTNs utilize such contact prospect for data forwarding by way of "store-carry-and-forward" when a node receives some packets it stores these packets in its buffer, carries them approximately pending it connections an additional node and next into view them. I will provide employ rate limiting to be a current feature in prevent of overflow attacks in DTNs and exploits the "claim-carry-and-check" to possibly identify the strength of rate limit in DTNs upbringing. These network nodes are transportation the claims when they move and cross-check if their taken claims are certain to take when they contact. I will do to provide scrupulous analysis on the probability of detection, and evaluate the effectiveness and efficiency of our scheme with widespread trace-driven simulations. My map uses able of makings to keep the control, to be in place for storing space expenditure little.

Keywords:

Disruption tolerant network, Routing, Attacks, Security, Detection.

1.INTRODUCTION:

The maximum provided in the bandwidth for defense space and size leads to assort exposed submerge attacks in the anticipated DTNs.

Here all submerge attacks are fired and triggered when we have cruelly or malignly or materialistically inspired attackers who introduce some fog and unwanted packets into the network, or in sometimes the alternative injecting of various packets by the attackers will be duplicated or replicas the same packet to as many nodes as possible to make the network resources usage as much as and make the system slow. Here the two types of attacks are called Replica Flood Attack, Packet Flood Attack, were flooded packets and replicas attacks on packets may throw away the priceless bandwidth and buffer size and avoid the packets from being endorse with ahead to the next node and as a result to worsen the network provision made available to good nodes. The surge in popularity of online social networking (OSN) services such as Face book, Twitter, LinkedIn, Google+ has been accompanied by an increased interest in attacking and manipulating them. Due to their open nature, they are particularly vulnerable to the Sybil attack under which a malicious user can create multiple fake OSN accounts.Each node itself counts 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, exchange some claims when they contact, and cross-check if these claims are inconsistent

2.LITERATURE ANALYSIS:

The literature review on lifeline response to seismic shocks has been broadly being divided into four categories: estimation of the damage to infrastructure components; estimation of infrastructure system performance; estimation of the economic losses associated with the response; and decision support methodologies for prioritizing infrastructure investment. Loss estimation, both direct and indirect (e.g. business interruption), is the primary focus of the financial industry in relation to lifeline response, whilst investment in infrastructure is important to improve its resilience and in doing so attempt to minimize potential economic losses and reduce premiums.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

The literature review is an evolving process but the following sections report on the progress thus far.

3.DISRUPTION TOLERANT NETWORKS:

A set of mobile nodes which are carried by human beings in vehicles will have Disruption Tolerant Networks (DTNs). In these networks the data is transferred when the mobile nodes are intermittently connected to each other with making them appropriate for applications where we have no communication infrastructure available such as military setups, forests and rural areas. Due to lack of Network consistent connectivity, the source and destination nodes can only exchange data when they move into the broadcast range of each other.

To forward the data when a nodes receives some packets it stores these packets in node buffer, carries them around until it contacts with another node, and then forwards them to the wanted node. Since the contacts between source and destination nodes are opportunistic and the duration of a contact time is also very long because of mobility, and here we have only bandwidth which is only available during the opportunistic contacts is a limited network resource.

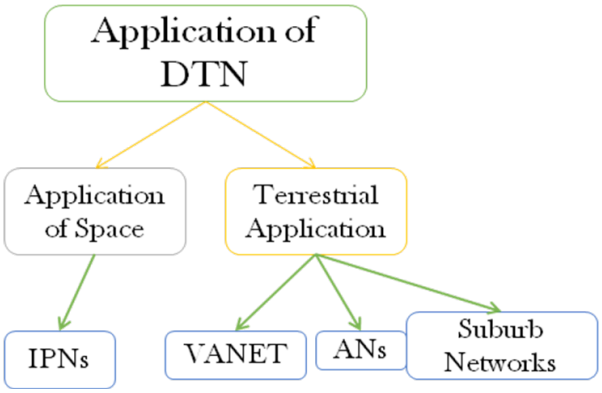


Fig 1: Applications of DTN's

3.1.SCHEME:

The detection of packet flood attacks works independently for each time interval. Without loss of generality, we only consider one time interval when describing our scheme. For convenience, we first describe our scheme assuming that all nodes have the same rate limit L, and relax this assumption .

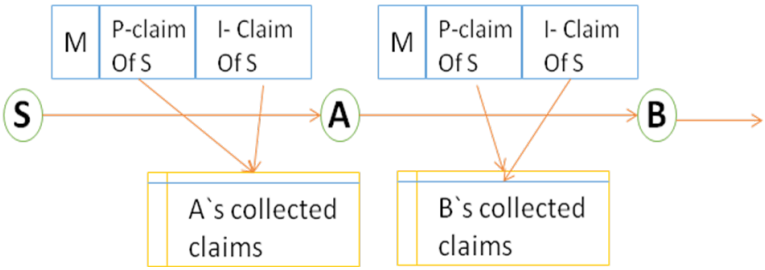


Fig 2: The conceptual structure of a packet and the changes made at each hop of the forwarding path.

3.2 CLAIM CONSTRUCTION:

Two pieces of Meta data are added to each packet (see Fig. 2), 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. 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.

1) 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 contacted node, it generates a P-claim as follows: P-claim: S, Cp, t, H (m), SIGSs (H (H (m)|S|Cp|t))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.

2) T-claim: 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 (i.e., the number of times it ha transmitted m out) and the current time t. The T-claim is:T-claim: A, B, H (m), ct, t, SIGA(H(A|B|H(m)|ct|t))B checks if ct is in the correct range based on if A is the source of m. If ct has a valid value, B stores this T-claim. In single-copy and multi-copy routing, after forwarding m for enough times, a deletes its own copy of m and will not forward m again.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

3) Claim Detection :

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.

3.2.1 Inconsistency Caused by Attack:

In a dishonest P-claim, an attacker uses a smaller packet count than the real value. (We do not consider the case where the attacker uses a larger packet count than the real value, since it makes no sense for the attacker.) However, this packet count must have been used in another P-claim generated earlier. This causes an inconsistency called count reuse, which means the use of the same count in two different P-claims generated by the same node. For example in Fig. 3(a) the count value 3 is reused in the P-claims of packet m3 and m4. Similarly, count reuse is also caused by dishonest T-claims.

3.2.2 Replica Flood Attacks in Quota-based Routing Protocols:

Our scheme to detect replica flood attacks can also be adapted to quota-based routing protocols. Quota-based routing works as follows. Each node has a quota for each packet that it buffers, and the quota specifies the number of replicas into which the current packet is allowed to be split. When a source node creates a packet, its quota for the packet is L′ replicas, where L′ is a system parameter. When the source contacts a relay node, it can split multiple replicas to the relay according to the quality of the relay. After the split, the relay's quota for the packet is the number of replicas split to it, and the source node's quota is reduced by the same amount. This procedure continues recursively, and each node carrying the packet can split out a number of replicas less than its current quota for the packet. It can be seen that each packet can simultaneously have at most L′ replicas in the network. In quota-based routing, replica flood attacks (where an attacker sends out more replicas of a packet than its quota) can be detected by our approach as follows.

First, we observe that quota-based routing (with the total quota determined at the source) can be emulated by single copy routing if different replicas of the same packet appear different to intermediate nodes and each replica is forwarded in a similar way as single-copy routing. A node can split multiple replicas of a packet to another node, but it can only send each replica out once. For instance, if a node has forwarded Replica 1 to one relay, it must remove Replica 1 from its local buffer, and it cannot forward this replica again to another relay.

3.3 ROUTING MISCONDUCT:

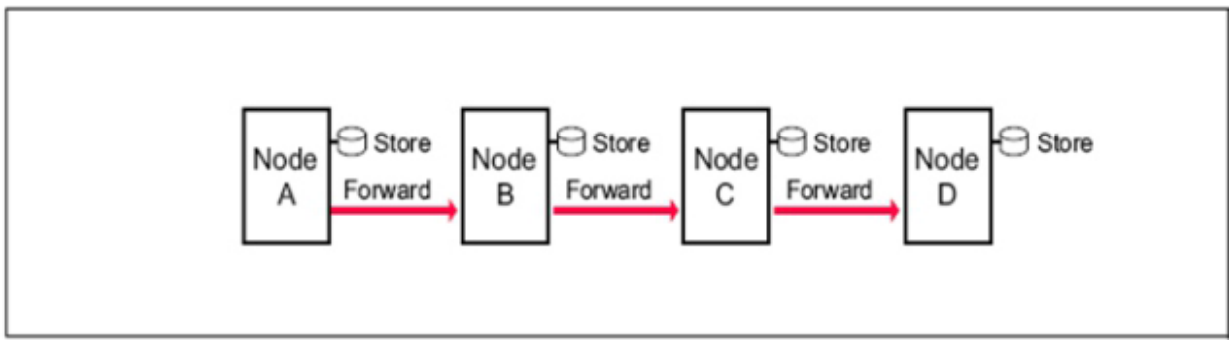
Routing misconduct deals with the concept where malicious nodes tend to drops packets which are received. It is caused by attackers to minimize packet delivery ratio and wastage of resources. So this has to be prevented to maintain the network. The general idea is, when two nodes are contacted they should generate a relation record, which consists of when contact has been made, which packets are available in their buffer before exchange of data and what packets need to be sent, unique ID. Then the record must include a sign for assuring verified.

So the node has to carry its relation record and report it to the next contacted node. So by this scheme the dropped packets are detected. Node N1 contacts with Node N2, the relation record M is generated. Node N1 sends packet N2. Then if suppose N2 drops packet m2 from its node and contacts N3. Node N3 analyses relation record and finds that packet m2 is dropped. This shows that the node N2 is malicious and attackers have caused to drop the packets.

3.4 STORE-CARRY & FORWARD:

DTNs overcome the problems connected with stopping at connectivity; long or not fixed in value loss of time, asymmetric facts rates, and high error rates by using store-and forward note eclectic apparatus. This is a very old way to used by pony-express and of the post systems since old times. Complete work notes (complete gets in the way of attention to program user knowledge computers) or pieces (parts) of such notes are moved (forwarded) from a place for storing for storing place on one network point (switch intersection) to a storage place on another network point, along a path that eventually reaches the place where one is going.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal



Store-and-forwarding methods are also used to email systems, but these systems are not node-to-node relays but rather than the both the source and destination independently contact a central storage device at the centre of the links.The storage places can hold messages indefinitely. They are called persistent storage, as opposed to very short-term storage provided by memory chips and buffers. Internet routers use memory chips and buffers to store incoming packets for a few milliseconds while they are waiting for their next-hop routing-table lookup and an available outgoing router port.

DTN routers need persistent storage for their queues for one or more of the following reasons:

» A communication link to the next hop may not be available for a long time.
» One node in a communicating pair may send or receive data much faster or more reliably than the other node.
» A message, once transmitted, may need to be retransmitted if an error occurs at an upstream (to forward the source to destination) node, or if an upstream node declines acceptance of a forwarded message.

3.5 CLAIM – CARRY & CHECK:

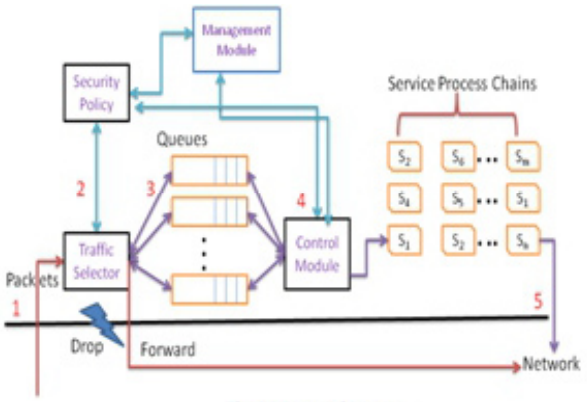
To detect the attackers that violate their rate limit L, I must count the number of unique packets that each node as a source has generated and sent to the network in the current interval since the node may send its packets to any node it contacts at any time and place, no other node can monitor all of its sending activities. To address this test to 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 in each packet sent out. The node rate limit certificate is also attached to the packet such that other nodes receiving the packet can learn its authorized rate limit.

Advantages:

» The main goal is a technique to detect if a node has violated its rate limit.
» The two types of attack packet flood attack and replica flood attack are detected.
» In proposed system DTNs follows “claim-carry and check”.

4.THE FIDRAN ARCHITECTURE:

This section briefly describes the FIDRAN architecture, for a detailed discussion we refer to the framework consists of core components which run permanently and of add-on gears the security services which are dynamically integrated into the system as needed. The core functionality comprises the traffic selector, the security policy, the control/management module and the default queuing discipline. Security services are implemented as loadable modules featuring IPS specific networking services. The capabilities provided by the underlying programmable networking infrastructure allow distributing the FIDRAN system on pro Gramm able routers.



The FIDRAN Architecture

The dynamic creation of an IPS overlay network is thereby enabled. Secure communication between programmable nodes is also provided. All network traffic is redirected to the traffic selector, which according to the rules

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

specified in the security policy assigns the traffic to one of the categories: forward, process or drop. Traffic that is assigned to the category forward is directly forwarded and not analyzed by any installed security service. It is either not necessary to check this traffic or another programmable node on the route to the end-system is in charge of doing so. Traffic in the category process is queued and analyzed by specific security services. The detailed proceeding for queuing and analysis as well as the reaction in case of a detected attack is also specified in the security policy. Finally, traffic belonging to the category drop is blocked altogether by the traffic selector. The management and the control modules are responsible for the configuration of the FIDRAN system.

4.1 EMULATION:

The performance of FIDRAN was assessed on the Cy¬ber Defense Technology Experimental Research tested which is a shared infrastructure designed for medium scale repeatable experiments in computer security. The tested provides a pool of over 300 computers of vary¬ing hardware which can be used to emulate networks. As scenario we chose the Abilene network depicted. For this network real world data traffic flows and link capacities is available on the project's web-site describes in detail the FIDRAN prototype implemented which includes a set of security services and which was used during the experi¬ments. S2.

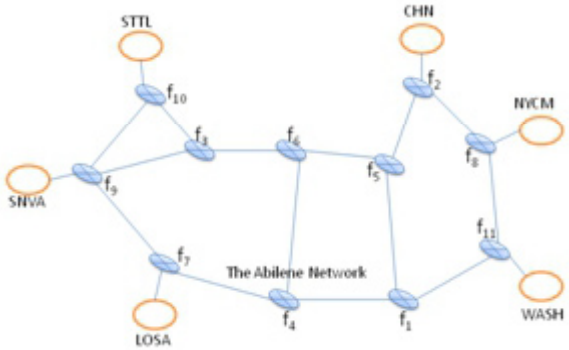


Table I represents the traffic matrix, the column index specifies the source and the row index the destination. Measurements of local-area and wide-area network traffic have shown that packet-switched data traffic is self-similar. Glen Kramer implemented a tool to synthetically generate self-similar network traffic traces by the superposition of a large number of 0/1 renewal processes whose ON and OFF periods are heavy tailed distributed.Finally, to avoid effects of congestion and flow control mechanisms all experiments were restricted to UDP-traffic.

To consider the hardware resources provided by the DETER tested, the network was emulated on a scale of 1 : 100 which means that traffic rates were divided by 100 and accordingly the delays were multiplied by 100.

4.2 The Abilene Network:

In the network each subnet sends data to all other sub¬nets resulting in an overall number of 30 traffic flows. The broadcast delay for each link was specified by dividing the distance from start node to end node by the speed of light. Table I represents the traffic matrix, the column index specifies the source and the row index the destination. To generate the traffic each subnet is supplied with an UDP sender for each destination which generates self-similar traffic as described above. Each experiment lasted 1800s and contained the sending of over 7, 500,000 packets.

To -->	CHIN	LOSA	NYCM	SNVA	STTL	WASH
CHIN	X	35.53	6.77	3.75	8.37	14.77
LOSA	113.58	X	51.50	10.30	26.26	58.90
NYCM	71.82	64.68	X	1.44	31.91	108.35
SVNA	5.68	34.09	3.29	X	55.06	2.13
STTL	66.26	27.79	21.84	9.02	X	15.63
WASH	93.45	75.20	176.86	8.22	36.30	X

Table I: The Abilene Traffic Matrix [Mbps]

Each traffic flow must be analyzed by three security ser¬vices, whereby the service processing times Ts were scaled as mentioned. We study the performance of the solutions obtained for both presented MILPs (single-path routing and multipath routing) with the objective of minimizing the maximum router utilization, and compare them to the solutions of the MILPs presented in extended to general¬ized topologies.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

4.3 TRAFFIC MODELING:

The COST Action 253 is aiming to study high speed terres¬trial (based on ATM technology) networks inter-connected by non-GEO satellite constellations. The per-formance of these networks depends very much on the successful char¬acterization and estimation of offered services and traffic loading, as well as on efficient man-agement techniques for the integrated, terrestrial and space system.The QoS parameters associated with every service cat-egory are given in Table.2: as they are recom-mended by ITU-T. 356 (U means unbounded).

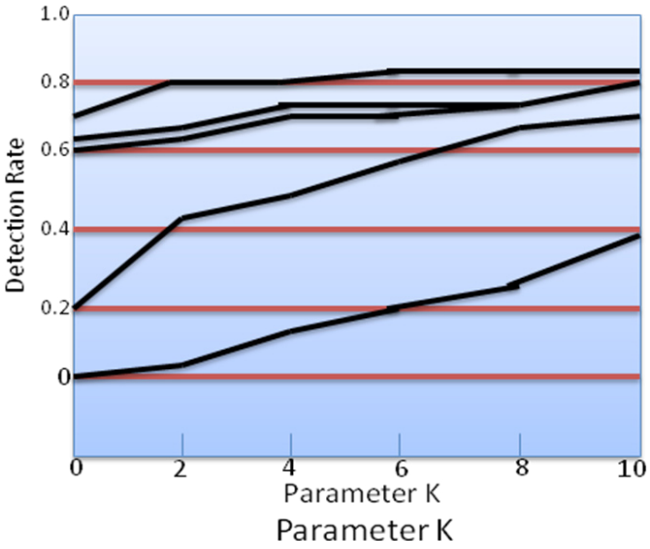
	CTD	CDV	CLR
Default	No	No	No
Class1	400 msec	3 msec	3.10^{-7}
Class2	U	U	10^{-5}
	CER	CMR	SECBR
Dfault	4.10^{-7}	1/day	10^{-4}
Class1	Default	Default	Default
Class2	Default	Default	default

4.4 PERFORMANCE EVALUATION

4.4.1 Experiment Setup:

To evaluate the performance and cost of our scheme, we run simulations on a synthetic trace generated by the Ran-dom Waypoint (RWP) mobility model and on the MIT Reality trace collected from the real world. In our syn-thetic trace, 97 nodes move in a 500×500 square area with the RWP model. The moving speed is randomly selected from to simulate the speed of walking, and the transmis-sion range of each node is 10 to simulate that of Bluetooth. Each simulation lasts 5 × 105 time units.

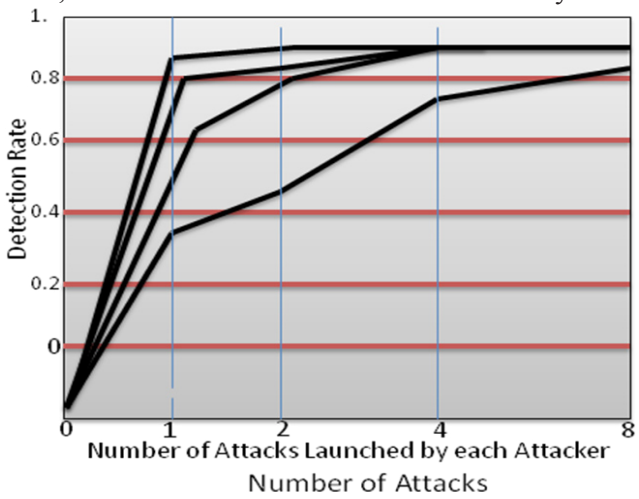
The Reality trace to have social community structures. 97 smart phones are carried by students and staff at MIT over 10 months. These phones run Bluetooth device discovery every five minutes and log about 110 thousand contacts. Each contact includes the two contact parties, the start time and duration of the contact.



Parameter K

4.4.2 Number of Attackers :

The synthetic trace to verify our analysis results since in this trace the contacts between node pairs are which con-forms to our assumption for the analysis. We divide the trace into 10 segments, each with 5×104 time units, and run simulations on each of the 3rd−7th segments 3 times with different random seeds. Each data point is averaged over the individual runs. Spray-and-Wait is used as the routing protocol to consider the worst case of packet flood detection. Here we only verify the detection probability for the basic attack, since the detection probability for the strong attack can be derived from it in a straightforward way. In this group of simulations, each attacker launches the basic attack once. It sends out two sets of packets to two good nodes with 10 packets in each set (i.e., n = 10), and these two sets contain mutually inconsistent packets. First fix parameter y = 1:0 (see Table I) but change param-eter K from 0 to 10, and then we fix parameter K = 10 but change y from 0 to 1:0. It can be seen that the simulation results are between the analytical lower bound and upper bound, which verifies the correctness of our analysis.



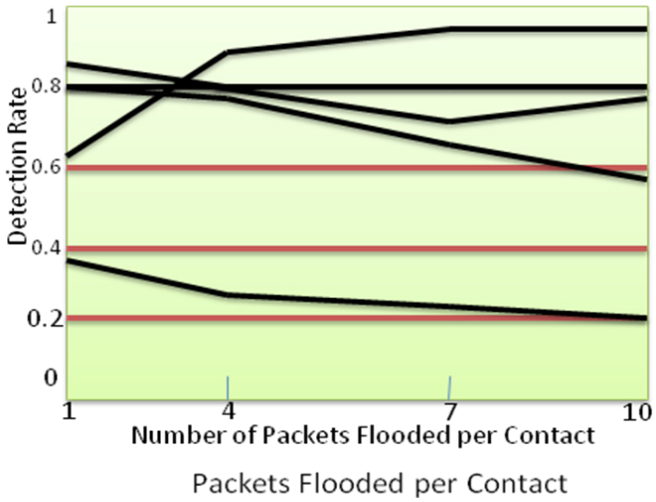
Number of Attacks

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

4.4.3 Packets Flooded Per Contact:

The reality trace is used. The trace into segments of one month, and run simulations on each attack once, and it floods one packet out (i.e., n = 1, y = 1:0). By default, attackers are selectively deployed to high-connectivity nodes. Parameter K in different routing protocols.

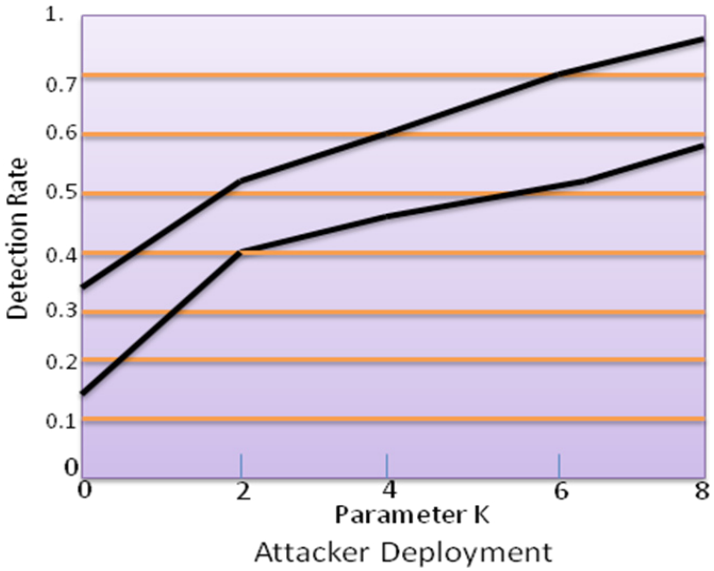
Generally speaking, when K increases, the detection rate also increases because the inconsistent packets are detection rate is lower when attackers are selectively deployed to high-connectivity nodes. This is because when attackers are selectively deployed they have more contacts with good nodes.



4.4.4 Flooded Replicas under Collusion:

As mention colluders can flood a small number of replicas without being detected. To evaluate their effect, we run simulations on the Reality trace when all attackers collude.

The simulation settings are the same. We compare our scheme with the case of no defense even when 20% of nodes are attackers and collude, our scheme can still limit the percentage of wasted transmissions to 14% in single-copy routing (SimBet) and 6% in multi-copy routing (Spray-and-Focus), which is only 1/7- 1/5 of the wasted transmissions when there is no defense.



5.RELATED WORK:

Routing naughtiness takes place in mobile ad hoc networks when the node agrees to forward the packet but does not. In order to avoid this naughtiness two approached are applied. They are watchdog and path ratter. The regulator monitors the national nodes endure they forward the packet or not. The protocol is based on priority wise. The prioritization is based on the duration, storage, message delivery, history of the nodes etc. The node replication attacks in sensor networks are detected in distributed way. The node duplication attacks are attacks that replicate the node and produces in the network. It also causes more disconnections in the network.The node location in order to accidentally selected witness, exploiting the birthday paradox to detect replicated nodes. Data forwarding in delay tolerant networks is very difficult. Data forwarding is not much effective in delay tolerant networks. To capably forward the data we exploit transient contact patterns some nodes in DTNs may remain connected with each other during specific time periods to form transient connected subnets despite the general absence of end-to-end paths among them.

6.CONCLUSION:

According to the thesis that has been published in the above paper it could be clearly illustrated the arguments and discoveries against flood attacks in disruption tolerant networks. This guards and keep safes by protecting against attacks by getting in the way attacker from injecting flooded small parcels.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

The process to detect both flood and duplicate attacks by inconsistency claims made by the attacker could be illustrated. Also the application layer attacks are detected and network points which drop small packets are detected. This scheme is cost effective and provides security for network such as get disruption tolerant network. The packet send a only one packet such sending the way bad behavior can increase the packet delivery ratio and does not waste system resources such as power and bandwidth. Our novel concept allows the protection capacity provided by a p-cycle to be used efficiently.

For the scenario under consideration, we also showed that the joint optimization of single path routing and service placement is a big improvement with respect to optimal service placement over routes calculated with the FIDREN Architecture, since the latter does not take the additional router load due to security processing into account. Reduces the computation time for setting up a multicast traffic request by enumerating a set of candidate p-cycles based on the PC score Good solutions were ob-tainted for both presented strategies. The single-path strategy tends to generate long paths to disburden heavy loaded routers. In contrast, the multi-path strategy splits huge flow into smaller ones and re-routes these over different paths. Both solutions show that they balance the load well.

7.R EFERENCES:

1. K. Fall, "A delay-tolerant network architecture for challenged internets," Proc. 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," SIGCOMM Workshops, 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. INFOCOM, 2006.

5. S. J. T. U. Grid Computing Center, "Shanghai taxi trace data," http://wirelesslab.sjtu.edu.cn/.

6. D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Workshop Sensor Network Protocols and Applications, 2003.

7. Routing for vehicle-based disruption tolerant net¬works. Proceedings of the 25th IEEE International Conference on Computer Communications, Apr. 23-29, IEEE Explore Press, Barcelona, Spain, pp: 1-11. DOI:10.1109/INFOCOM.2006.228.

Author's Details:

Mr S.Vasu received

The M.Tech in Computer Science from JNTUA University of AP. He is currently an Associate Professor in the Department of Computer Science Engineering and Information Technology at the SVCET, Chittoor. His paper published on "Distributed Detection of node replication attacks in DTNs", www.ijmetmr.com , Vol. 1, ISSUE No: 9, September 2014, ISSN No: 2348-4845.

Mr. B Rama Ganesh

received the B.Tech Degree in Computer Science and Information Technology from JNTUH University of TS, and received the M.Tech degree in WT from JNTUH University of TS. He is currently an Associate Professor in the Department of Computer Science Engineering and Information Technology at the VEMU Institute of Technology, Chittoor. His Pursuing research scholar on Department of CSE, Ph.D from GITAM University, Vizag, AP.

M. Ramesh Reddy

received the B.Tech Degree in Information Technology from JNTUA University of AP in 2012, and received the M.Tech degree in Computer Science Engineering from

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

JNTUA University of AP in 2015. He is currently an Assistant Professor in the Department of Computer Science Engineering and Information Technology at the VEMU Institute of Technology, Chittoor. His research interests networking and ethical hacking, wireless and mobile networking. His Papers Published on "Distributed Detection of node replication attacks in DTNs", www.ijmetmr.com, Vol. 1, ISSUE No: 9, September 2014, ISSN No: 2348-4845, "Combined Transfer Routing and Circulation of Protection Services in Elevated Rapidity Networks", www.ijmetmr.com, Volume No: 2 (2015), Issue No: 9 (September), Page 74-80. He is the member of IJMETMR.

Peralla Srinivasulu

received the B.Tech Degree in Information Technology from JNTUA University of AP in 2012, and received the M.Tech degree in Computer Science Engineering from JNTUA University of AP in 2014. He is currently an Assistant Professor in the Department of Information Technology at the St Martin's Engineering College, Hyderabad. His research interests networking and wireless and mobile networking. His paper research on "Defending against To Flood Attacks in Disruption Tolerant Networks"

Bathala Subbarayudu

received the B.Tech Degree in Information Technology from JNTUA University of AP in 2012, and received the M.Tech degree in Computer Science Engineering from JNTUA University of AP in 2014. He is currently an Assistant Professor in the Department of Information Technology at the St Martin's Engineering College, Hyderabad. His research interests networking and wireless and mobile networking. His paper published on "Combined Transfer Routing and Circulation of Protection Services in Elevated Rapidity Networks", www.ijmetmr.com, Volume No: 2 (2015), Issue No: 9 (September), Page 74-80.

Puttu Chandra Sekhar

received the B.Tech Degree in Computer Science Engineering from Global College of Engineering & Technology affiliated to JNTUA University of AP in 2012, and pursuing M.Tech in Computer Science Engineering from Sri Venkateswara Institute of Science & Technology, Kadapa. His research interests networking and wireless and mobile networking. Present His research on "Defending against To Flood Attacks in Disruption Tolerant Networks"

.