RESEARCH ARTICLE OPEN ACCESS

Mitigating Flooding Attacks in Disruption Tolerant Network

Aniekan Julius Bassey [1], C Fancy [2]
M.Tech Student [1], Assistant Professor [2]
Department of information Technology
SRM University
Tamil Nadu - India

ABSTRACT

Disruption Tolerant Networks (DTN) provides communication in challenged networking environment where traditional protocols breaks down due to extreme delay and disruptions. Mobility of nodes and opportunistic contact among nodes for data communications is processed using DTN. In the absence of reliable connectivity, DTN are exposed to flooding attacks, nodes only exchange data and uses network resources (storage capacity, contact opportunity) when moving in transmission range of each other. Motivated attackers inject several packets or forward replicas of the same packet into the network to as many nodes as possible to exhaust limited network resources, dropping packets, corrupting routing table and counterfeiting acknowledgement. The malicious nodes then lead to delay or destruction of data in transit to its destination. Based on existing system, distributed scheme identify if a rate limit is violated by a node and the basic idea of detection is claim-carry-and-check where the packets and replicas packets sent is counted by each node and other nodes claims the count, the claim is carried by the receiving node as they move and double-check if there is any inconsistency in the claim carried as they contact. Pigeonhole principle is used by the claim structure which assures inconsistent claims made by the attacker that may lead to detection. Each node has a limit over the number of packets that is, as a source node, can send to the network in each time interval. This paper proposed the use of RSA (Rivest-Shamir-Adleman) algorithm to enhance security, identifying the attackers and discard the attacker's node. Identifying flood attacks on the packets works independently for each time interval. A rigorous analysis on the probability of detection is provided and the effectiveness and efficiency of our scheme is evaluated with extensive driven simulations.

Keywords:- DTN, Flood Attack, Detection, Security

I INTRODUCTION

DISRUPTION Tolerant Networks (DTNs) is designed to provide communication in the most unstable and stressed environment where the network would normally be subjected to frequent and long lasting disruptions that severely degrades normal communications. DTNs is frequently used for disaster relief missions, peace-keeping missions and it exploit mobile nodes to transfer data carried by human beings, vehicles etc. Data exchange between two nodes is achieved when they are in contact with each other and network resources e.g. buffer space allows the nodes to move in transmission range with each other. Due to limitations of buffer space and bandwidth, attacker injects malicious packets into as many nodes as possible to waste network resources. As the network resources are exhausted this lead to flooding of numerous packets and replica packets. In such scenarios, networks may be mostly disconnected, i.e., maximum period of the time, end to-end paths connecting every node pair does not exist. In a DTN, preventing flooding attack totally is not feasible but their effects are minimized and the problems are quickly resolved when they occur. To cope with repeated, long-lasting disconnections, opportunistic routing techniques have been proposed in which, a node chooses if to forward or store-and-carry a message. Despite a rising amount of this kind of proposals, there is still a little consent on the most appropriate routing algorithm in this context. Motivated attackers inject numerous packets into the network as well as forwarding replicas of the packet to as many nodes as possible. Such attacks include [10] dropping data, flooding the network with extra messages, corrupting routing tables, and falsifying network acknowledgments.

Furthermore, mobile nodes expend a lot of energy on transmission of packets and replica packets flooded in the network; this makes the battery life to be shortened. Hence [1], it is vital to secure DTNs against flood attacks. In other to defend against flooding attacks, a few works have been done with respective to various attacks, routing socially selfish DTN [2], Blackhole attack [4], Wormhole attack [5] and routing misbehavior [6]. DTNs are robust against numerous malicious attackers in the absence of

authentication [8]. Without authentication, some nodes eager to join the network increases because of easier deployment. Addressing problem in flood attacks in DTNs is an issue, [9] outsider attackers flooding packets without valid cryptographic credentials can be easily filtered with authentication systems but authentication doesn't work alone when insider attackers with valid cryptographic credentials flood packets and replicas with valid signatures.

Rate limiting technique is employed to effectively mitigate flood attack. This helps to control the rate of traffic sent or received by a node in the network. It can be seen as a form of filtering packets and a violation of the rate limit enhance the detection of attack hence, flood attack can be controlled in the network. In this work, neighbor discovery of a malicious node is an enhancement in mitigating flooding attack in DTN. It allows the selection of node to forward the packet and enables exchange of information among the neighbors in the network in the case of a malicious node.

This paper is structured as follows. Section II reviews related work. Section III presents overview of flood attacks. Section IV presents our models, basic idea. Section V is our scheme. Section VI presents our simulation and analysis of our solution. Section VII contains the conclusion of the paper.

II RELATED WORK

Various schemes have been proposed on security attacks and how to mitigate the attack in the network. Previous work indicates resemblances with this work and the approach used to detect an attacker shows reliable connectivity with the nodes. Ren et al. [5] shows that wormhole attacks are harmful in disrupting the normal network operation in DTNs that is, one location of the packet is recorded by the malicious node and then tunnels them to another colluding node, which replays them locally into the network. Adversary connects two compromised nodes far away in the network using a low-latency link. The compromised node makes a record of transmission and channels the data packets to another compromised node that will replay them. This gives the nodes within the transmission range of the compromised nodes an impression that they are far away neighbours of some other nodes. Their method to detect wormhole attacks is a detection mechanism that exploits the existence of a prohibited topology in the network which utilizes the determination of the presence of a special network topology. It is prohibited under normal situations without attacks in the network, by reducing the transmission range of a node for a short duration during detection. The propose method can detect wormhole attacks efficiently and effectively in DTNs but cannot address flooding attack.

Li et al. [4] Blackhole attack has the risk that malicious nodes will forge metrics and then make it available in other to attract packets for launching attacks. They proposed an encounter ticket scheme to verify the proof of contacts, upon which nodes base their computed belief and uncertainty towards the capability of each potential forwarding node. However, the encounter ticket used cannot address the problem in flood attacks. Li and Cao [6] proposed a distributed scheme to mitigate routing misbehaviour by controlling forwarding of number of packets to the misbehaving nodes. The approach involves packet dropping and routing misbehaviour and it works even if the routing metrics is falsifies or not. To mitigate routing misbehaviour, mobile ad hoc networks previous works reduce the traffic flowing to the bad nodes by avoiding them in path selection. However, due to lack of tenacious path in DTNs, this cannot be directly applied.

Kuriakose and Daniel [7] employed the rate limit to mitigate flood attack in DTN and proposed a scheme which exploits intrusion system that detect compromised node which utilized the correlation of delivery probability between the nodes. This effectively detects malicious nodes and mitigates the negative impact of data delivery, reduced propagation delay and increase packet delivery ratio.

III OVERVIEW OF FLOOD ATTACKS

Flooding attack involves an attacker exhausting the network resources e.g. bandwidth such that it consumes the node resources like computational and battery power or disrupt the routing operation to cause network performance degradation. It is an attack that attempts to cause a failure in a computer system or data processing unit by delivering extra input than entry can process properly. For convenience, we call the two types of attack packet flood attack and replica flood attack, respectively. They waste precious bandwidth and buffer resources, preventing nonthreatening packets from being sent and thus degrade the network service provided to good nodes. A malicious node can generate and send a large no. of RREQs in a short period of time to a destination node that doesn't exist in the network, this results in flooding the whole network, consumption of all the battery power, bandwidth, thus leading to a denial of service. Due to the occurrence of flooding attack in the network, a non-malicious node is unable to serve other nodes due to the network flooding enacted by the malicious node fake request and useless data packets. This results in the following problems in the network:

- Exhaustion of the nodes battery power
- Wastage of node processing time, thus increasing the overhead
- Wastage of bandwidth
- Degradation of throughput
- Overflow of the routing table entries which causes exhaustion of network resources like memory (storage space)

In DTNs, a single packet can usually be delivered to its destination with a probability smaller than 1 due to the opportunistic connectivity.

A. Packet Flood Detection

This is one of the kinds of security threat every network comes across starting from the simple network design to a more complex network. If an attacker are floods more packets than its rate limit can accept, it fraudulently states count that is 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 [1]. The total number of unique packets that each and every source node generates and sends to the network in the current interval must be counted to identify the attacker that violates their rate limit L. 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. The claimed count must have been used before by the attacker in another claim. Pigeonhole principle is used for assurance of the re-usage of claim and one can say two claims are inconsistent. [1]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. An attacker will be easily identified when an inconsistency is discovered.

B. Replica Flood Detection

An attacker floods the network with a numerous replicas of the same packet into the network thereby exhausting the limited network resources. This is the upmost target of an attacker to a network. The technique which is claim, carry and check is exploited to identify and detect the attacker that forwards replicas and buffered packet more times than its limit l. If the source node of a packet or an intermediate hop (node) transmits the packet to its next hop, it claims a replica count which means the number of times it has spread the replicas of that packet as well as the current transmission. The next hop comes to know the nodes 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.

IV SYSTEM MODEL

This evaluates the various routing protocols used to make assumptions about the size, connectivity and mobility.

A. Loose Time synchronization Model

Similar to other work [1], [7] large data item are splitted into smaller packets (or fragments) to enable easy data transfer. We assume predefined size for all the packets and a lifetime to each of the packet. As a packet's lifetime is used up, the packet is discarded because it becomes meaningless. Each of the packet generated by nodes is unique, this is applied by including the source node ID and a locally unique sequence number, which is assigned by the source for this packet, in the packet header. This assumes that time is loosely coordinated, such that any two nodes should be in the same time slot at any given time. Since the inter contact time is usually at the scale of minutes or hours, the time slot can be at the measure of a few minutes.

B. Trust Model

Public-key cryptography system is assumed to be available. Therefore, the Key Generation Center (KGC) is needed. Private Key is generated for each node based on the node's id by the KGC and publishes a small set of public security parameters to the node. Only the KGC can generate the private key for a node id. Using this system, an attacker is unable to forge the node id and private key pair and they don't know the private key of a good node (not attacker).

C. Rate Limit Model

Rate limit certificate is acquired from a trusted authority for each of the nodes. The certificate includes the node's ID, its approved rate limit L, time of validation of the certificate and the signature of the trusted authority. The public key certificate and the rate limit certificate can be merged or they can be use separately. The number of unique packets generated by each node as a source must be counted and sent to the network in the current interval to detect the violation of rate limit. Our idea is for the node to count the number of unique packets sent out by the source then claim the count that is to update packet count in each packet sent out. The node's rate limit certificate is also attached to the packet; this enables other nodes that are receiving the packet to know the authorized rate limit L for the transmission of the packets.

D. Claim Construction Model

Two separate sets of claims are maintained by each of the nodes (P-claim and T-claims respectively) for metadata exchange, a sampled set which includes the P-claims taken from recently contacts with different nodes. To increase the probability of attack detection, one node also stores a small percentage of claims which is exchanged from its contacted node, and exchanges them to its own future contacts which is known as redirection. It removes the forwarded claims from other nodes immediately after it has exchanged them to different nodes.

E. RSA Algorithm

RSA provides reputability of electronic communications and data storage by both public key encryption and digital signatures. A private key for each node is generated by the KGC based on the node's id and publishes a small set of public security parameters to the node. It minimum key length is 1024 for a secured RSA transmission. Its security is based on the difficulty of factoring large integers. Node A sends an encrypted message to Node B without any prior exchange of secret keys. Node A uses Node B's public key to encrypt the message and B decrypts with its private key known only to him. With RSA, node A can sign a message using their private key and B can verify it using A's public key. If the keys are verified to be authentic and the march, the packet is forwarded to the next node but if the keys doesn't march, the packet is dropped and known to be a malicious packet.

V OUR SCHEME

Detecting an attacker whose rate limit L is violated involves counting the number of unique packets from each of the nodes. Each of the nodes as a source generates and forwards the packets to the network in the current interval. However, since the node forwards its packets to any of the nodes that it gets in contacts at any time and place, no other node can monitor all of its sending activities. Stressing on this challenge, our idea is for the node to count the number of unique packets by itself that it, as a source, has sent out then claim the up-to-date packet count (with additional information such as the node ID and a timestamp) in each packet sent out. The node's rate limit certificate is attached along with the packet; this is so that other nodes that are receiving the packet can learn of its authorized rate limit L. If more packets are flooded by an attacker such that it exceeds its rate limit, it has to dishonestly claim a count smaller than the real value in the flooded packet. As the real value of the count is larger than its rate limit, this clearly indicates that an attack has occurred. The claimed count must have been used previously by the attacker in another claim, which can be guaranteed by the pigeonhole principle, and these two claims are inconsistent. The malicious packet received by the nodes from the attacker carries along the claims included in those packets as they move around in the network. When the two nodes are in contact with each other, check is done to determine if there is any inconsistency between their collected claims. If any inconsistency is detected, the attacker is identified.

Furthermore, providing additional security measures on the routers, malicious attacks can be effectively prevented. In a network system without infrastructure such as ad hoc network, routing can be accomplished by collaboration of autonomous nodes in the form of self-organization; DSR routing is used in this work. In this case, any attempt that requires regulating the behaviour of each autonomous node will result in a major overhead. The second idea is detection. Here, nodes with abnormal behaviours are detected when their credential fails and are marked as malicious, thus avoided by well-behaved nodes during packet routing. However, since there is no centralized monitoring point and network administrative authority, it becomes extremely difficult and expensive to effectively detect faulty nodes. In summary, the goal of both designs is to acquire a fault-free network by preventing its nodes from selfishness or malicious attacks, or purging nodes with such behaviours. The encrypted packets are secured from the attacker access and are verified for integrity. We going to introduce a new form to enhance the security by the way of using RSA (Rivest-Shamir-Adleman) algorithm to enhance security, we improving the existing concept by identifying the attacker and discard the node from which the data packets transmitted and also increasing the life time of network. This security measure is to encrypt the packet that is sent from the source to the destination. At the destination, the packet is decrypted and the data received. For convenience, we first describe our scheme assuming that all nodes have the same rate limit L and relax this assumption. Without loss of generality, we only consider one time interval when describing our scheme.

PROTOCOL

If two nodes are in contact with each other and they have a number of packets to forward to each other. Then our protocol is
sketched in the algorithm.

Algorithm 1. The protocol run by each node in a contact
1: Metadata (P-claim and T-claim) exchange and attack

detection
2: if Have packets to send then
3: For each new packet, generate a P-claim;
4: For all packets, generate their T-claims and sign them with a hash tree;
5: Send every packet with the P-claim and T-claim attached;
6: end if
7: if Receive a packet then
8: if Signature verification fails or the count value in its P-claim or T-claim is invalid then
9: Discard this packet;
10: end if
11: Check the P-claim against those locally collected and generated in the same time interval to detect inconsistency;
12: Check the T-claim against those locally collected for inconsistency;
13: if Inconsistency is detected then
14: Tag the signer of the P-claim (T-claim, respectively) as an attacker and add it into a blacklist;
15: Disseminate an alarm against the attacker to the network;
16: else
17: Store the new P-claim (T-claim, respectively);
18: end if
19: end if

When a packet is sent by a node, the T-claim is attached to the packet. As numerous packets can be sent in a contact, signing each packet T-claim distinctly is costly. The nodes also attaches a P-claim to the packets generated by itself and have not been sent to other nodes before. P-claim and T-claim are attached to a packet when a node receives the packet. After the packet is received, the packet is alongside the claims previously collected to discover if there is any inconsistency. P-claims that are generated the same time interval are cross-checked for any inconsistency. If there is no inconsistency detected, such a node's the P-claim and T-claim is stored locally.

For proper flood attacks detection, P-claims and T-claims recently collected by small number of two nodes that exchange claims are also checked for inconsistency. As an attacker is detected by a node, the attacker is added into blacklist such that any packet originating or sent from the attacker is rejected or not accepted. An alarm is broadcast to all the other nodes that an attacker is identified and blacklisted in the network.

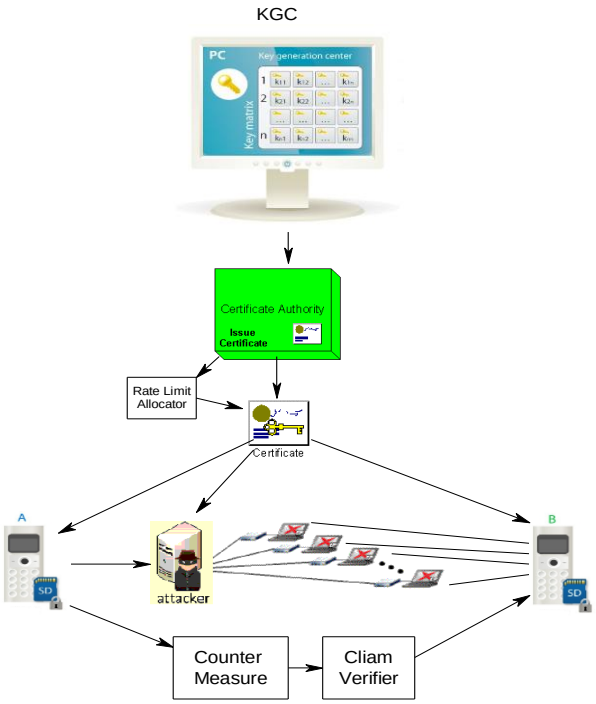

Fig 1 Architecture Diagram

VI SIMULATION AND ANALYSIS

A simulation study was conducted simulation to evaluate the effectiveness of our scheme in mitigating flooding attacks.

A. *Simulation setup*

To evaluate the performance and cost of our scheme, we run a simulation of the system with different packet flood and replica flood attack scenarios. In the simulation setup, 50 nodes are deployed to move in a 500 x 500 square meters area with 2 nodes are identified as the source and destination after 2.5ms of simulation. The moving speed is randomly selected to simulate the speed of walking and transmission range of each node. The duration of the simulation is 0 to 299ms. The source and destination node are selected and identified after a few second of simulation, 10 percent of the nodes are deployed as the attackers. They are randomly deployed and selectively deployed to high connectivity nodes. The buffer size of each node is 5MB, bandwidth is 2Mpbs. Each node generates packets of 10KB with random destination at different rate.

In our simulations, an attacker is an intermediate node whereas an honest node can be a source, a destination or an intermediate node The source node forwards encrypted packets to the next hop using DSR routing to the next node with a valid node id, sequence no and rate limit from the certificate authority. Illustrating the general network throughput, all honest nodes generate traffic destined for

other randomly chosen honest nodes.The parameters primarily focus on are: the number of packets, the percentage of packet delivery ratio and route life time.

B. *Simulation results*

Graph illustration 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.

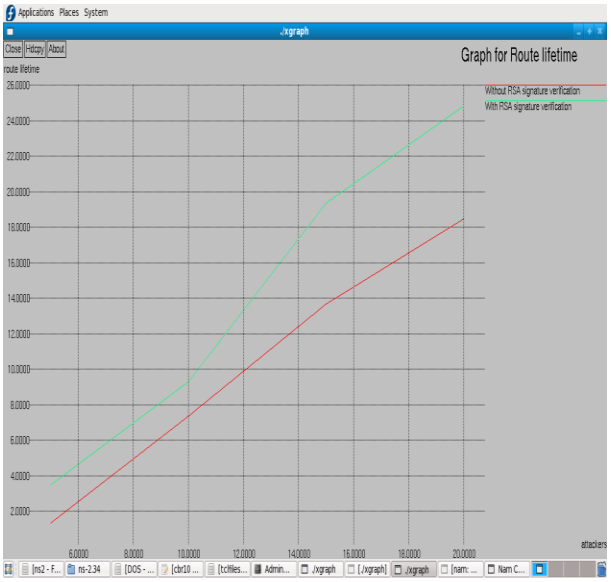

Fig 2 Route Lifetime

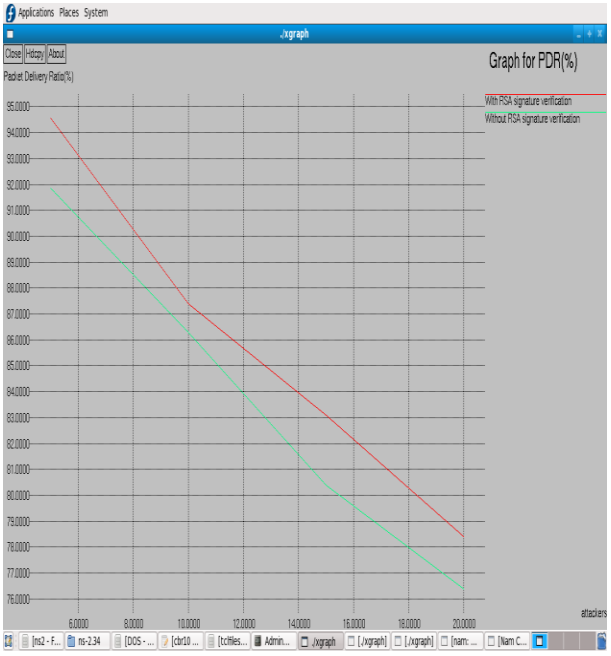

Fig 3 Packet Delivery Ratio

Figure 2 shows the effect of route life time where there is an improvement compared to existing systems without the RSA algorithm. Figure 3 show the packet delivery ratio between RSA algorithm and without RSA algorithm. Packet delivery probability is ratio of number of successful messages each destination receives vs the number of messages sent by each sender. The results demonstrate that attacker's node and the good nodes shows a much more effective packet delivery rates thereby mitigating flooding the network with malicious packets. The packet delivery ratio is higher with the RSA algorithm.

VII. CONCLUSION

Rate limit is a mechanism that is employed to mitigate flood attack in DTN using rate limit certificates from the trusted certificate authority. The proposed scheme exploits claim-carry-and-check to probabilistically detect the violation of rate limit in DTN environments maintains in each time interval. If there is a violation of the rate limit, it effectively detect malicious node and mitigate the negative impact of the data delivery, effectively reduced propagation delay and increased the packet delivery ratio. Key based security, RSA algorithm was used along with rate limiting technique to increase efficiency in resource utilization. In the future, to detect the attacker sending packet with the rate limit, we plan to investigate collusion between malicious nodes with key generation using AES and MAC algorithm to increase efficiency in resource utilization.

REFERENCES

[1] Q. Li, W. Gao, and G. Cao, *To Lie or to Comply: Defending against Flood Attacks in Disruption Tolerant Networks*, Ieee Transactions On Dependable And Secure Computing, Vol. 10, No. 3, 2013.

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

[3] S. Zhang, C. Zhu, J. K. O. Sin, and P. K. T. Mok, "A novel ultrathin elevated channel low-temperature poly-Si TFT," *IEEE Electron Device Lett.*, vol. 20, pp. 569–571, Nov. 1999.

[4] 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.

[5] Y. Xue and K. Nahrstedt, *"Providing fault-tolerant ad-hoc routing service in adversarial environments,"*

Wireless Personal Comm., vol. 29, no. 3-4, pp. 367–388, 2004.

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

[7] 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.

[8] 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.

[9] D. Kuriakose and D. Daniel, "Effective Defending against flood attack using strem check Method in Tolerant network"

[10] J. Burgess, G. D. Bissias, M. D. Corner, and B. N. Levine, *"Surviving attacks on disruption-tolerant networks without authentication,"* in MobiHoc '07: Proceedings of the 8th ACM international symposium on Mobile ad hoc networking and computing. Montreal, Quebec, Canada: ACM Press, 2007, pp. 61–70.H.

[11] 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.

[12] Nisha H. Bhandari, *"Survey on DDoS attacks and its detection defense approach,"* International Journal of Science and Modern Engineering, Vol.1, Issue.3, pp.67-71, Feb 2013.