A Taxonomy on Misbehaving Nodes in Delay Tolerant Networks

Waqar Khalid, Zahid Ullah, Naveed Ahmed, Yue Cao, Muhammad Khalid, Haleem Farman, Muhammad Arshad, and Haitham Cruickshank

Abstract

Delay Tolerant Networks (DTNs) are type of Intermittently Connected Networks (ICNs) featured by long delay, intermittent connectivity, asymmetric data rates and high error rates. DTNs have been primarily developed for InterPlanetary Networks (IPNs), however, have shown promising potential in challenged networks i.e. DakNet, ZebraNet, KioskNet and WiderNet. Due to unique nature of intermittent connectivity and long delay, DTNs face challenges in routing, key management, privacy, fragmentation and misbehaving nodes. Here, misbehaving nodes i.e. malicious and selfish nodes launch various attacks including flood, packet drop and fake packets attack, inevitably overuse scarce resources (e.g., buffer and bandwidth) in DTNs. The focus of this survey is on a review of misbehaving node attacks, and detection algorithms. We firstly classify various of attacks depending on the type of misbehaving nodes. Then, detection algorithms for these misbehaving nodes are categorized depending on preventive and detective based features. The panoramic view on misbehaving nodes and detection algorithms are further analyzed, evaluated mathematically through a number of performance metrics. Future directions guiding this topic are also presented.

Index Terms

Delay Tolerant Networks, Flood Attack, Fake Packet Attack, Malicious Node, Misbehaving Node, Packet Drop Attack.

I. Introduction

Delay Tolerant Networks (DTNs) are infrastructure-less networks, where no end-to-end route exists and disconnection of network occurs frequently [1]–[7]. DTNs are primarily developed for Interplanetary Networks (IPNs) [8], however, also applicable in emerging networks such as Vehicular Ad-hoc Networks (VANETs) [9], Underwater Wireless Sensor Networks (UWSNs) [10] and disaster applications [11]. For example, some of these specific applications of DTNs are KioskNet [12], DakNet [13], ZebraNet [14] and WiderNet [15]. Communication in DTNs follow a Store-Carry-Forward (SCF) method to transfer messages among nodes [16]–[18], where the Bundle Protocol (BP) has the ability to reliably transfer a message both hop-by-hop and end-to-end. The convergence layer translates a bundle to underline specific network architecture that enables communication among heterogeneous networks [19], [20].

Due to intermittent connectivity, asymmetric data rate and long delay [21], DTNs face lot of challenges such as reliability [22], [23], time synchronization [22], reorder of bundles, node management, spoof identity [24], resource scarcity [25], [26], routing [27], [28], bundle security [29], [30], key management [31]–[34], fragmentation [35], [36], privacy [37]–[41] and routing misbehavior [42] etc. Even though routing protocols in DTNs have been investigated extensively [43]–[54], inadequate attention is paid to security issues in DTNs.

In DTNs, nodes are vulnerable to various attacks such as black hole [55], insider [56], gray hole [57], wormhole [58]–[60], Denial Of Service (DOS), Distributed Denial of Service (DDOS)/flood [61], faulty node [62], [63] and packet drop [64]. Apart from the above-mentioned attacks, *misbehaving nodes* is one of the key challenging issues of DTNs. Misbehaving malicious and selfish nodes introduce variously attacks (e.g. flood, packet drop and fake packet attack) to overuse scarce network resources. Moreover, this would lead to nodes unavailability, low packet delivery ratio and bogus messages in DTNs. However, the trivial mitigation algorithms in VANETs [65]–[69], Mobile Ad-hoc NETworks (MANETs) [70]–[73], Wireless Sensor Networks (WSNs) [74]–[77], TCP/IP [78]–[82] and UWSNs [83]–[86] are not applicable in DTNs, due to long delay and frequent intermittent connectivity.

In [87], security issues in opportunistic networks are addressed, however with lack of details on flood and packet drop attacks. A comprehensive survey on MANETs is presented in [88], however, the reviewed solutions are not applicable to DTNs. In comparison, this survey discusses a Taxonomy of misbehaving nodes and detection algorithms in DTNs. Following are the main contributions of this article:

Waqar Khalid, Zahid Ullah, and Muhammad Arshad are with Department of Computer Science, Institute of Management Sciences Peshawar, Pakistan, Email: khalid.ping91@gmail.com; zahidullah@imsciences.edu.pk; arshad_khan8824@yahoo.com; fahmad0097@gmail.com

Naveed Ahmad is with Department of Computer Science, University of Peshawar, Pakistan, Email: n.ahmad@uop.edu.pk

Yue Cao and Muhammad Khalid are with Department of Computer and Information Sciences, Northumbria University, Newcastle upon Tyne, UK, Email: yue.cao; m.khalid@northumbria.ac.uk

Haleem Farman is with Department of Computer Science, Islamia College Peshawar, Pakistan, Email: haleem.farman@icp.edu.pk

Haitham Criuckshank is with Institute for Communication System, University of Surrey, UK, Email: h.cruickshank@surrey.ac.uk

- A unique and diverse classification of misbehaving nodes in DTNs, based on different criteria such as the type of attack, number of victim selections, internal and external nodes, intentional and un-intentional packets drop and individual and social selfishness.
- Detailed classification of detection algorithms into eight different types, namely rate limit based, encounter based, watch-dog based, guard-node based, incentive based, merkle-hash-tree based and protocol based detections.
- Rigorous analysis of various detection algorithms based on type of attacks, trusted authority (TA) and its role and mitigation solutions.
- Mathematical evaluation of various detection algorithms, in terms of buffer consumption, cost and network performance.
- Presenting open research issues of misbehaving nodes detection and mitigation.

The rest of the paper is organized as. Section II provides various misbehaving nodes and its associated attacks. Section III explains the detection techniques for misbehaving nodes. In Section IV, existing state-of-the-art protocols handling misbehaving nodes are discussed. Section V is dedicated to analysis of detection techniques and related work using various parameters. Section VI provides mathematical evaluation of detection schemes on certain parameters. Section VII discussed Use Cases. Section VIII Describes Open Research Issues in the Subject area. Finally, the paper is concluded with future work in Section IX.

II. Misbehaving Nodes

Nodes in DTNs send packets based on the general assumption, that intermediate nodes will help to forward it. However, this does not always work with security concern. To better understand the concept of various attacks introduced by misbehaving malicious nodes, we consider four nodes A, B, C and D, as shown in Figure 1:

- In the first scenario, the source node A forwards a packet to destination node D, through the intermediate node B. While node A is not directly connected to node D, thus it forwards a message to node B. At this stage, node A assumes that node B will forward this packet to node D, whereas the latter drops that packet.
- In the second scenario in which node B generates flood attack to waste the limited resources of node C. For simplicity, although we take one node as example but in reality, malicious nodes target more than one nodes to inject flood attacks.
- In the third scenario, node A forwards a message to node B that destined for node D. However, node B drops the packet and injects a new fake packet to induce fake packet attack.

Here, all above scenarios present the misbehavior of nodes would affect overall network [89]–[113]. Figure 2 shows classification of misbehaving nodes and its associated attacks, note that nodes inherently misbehave due to malicious and selfish nodes in the network.

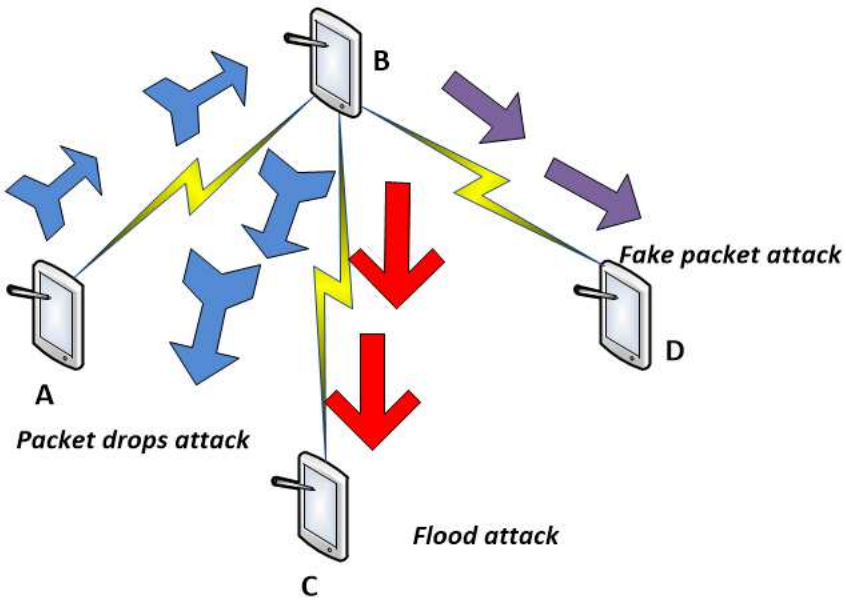

Fig. 1. Packet drop, Packet flood and Fake packet attack

A. Malicious Nodes

Nodes that injecting a large number of packets to overuse the resources of nodes in DTNs is called malicious nodes [114]–[121]. Usually, the behaviour of malicious nodes is to inject more packets into the networks, but sometimes these nodes drop

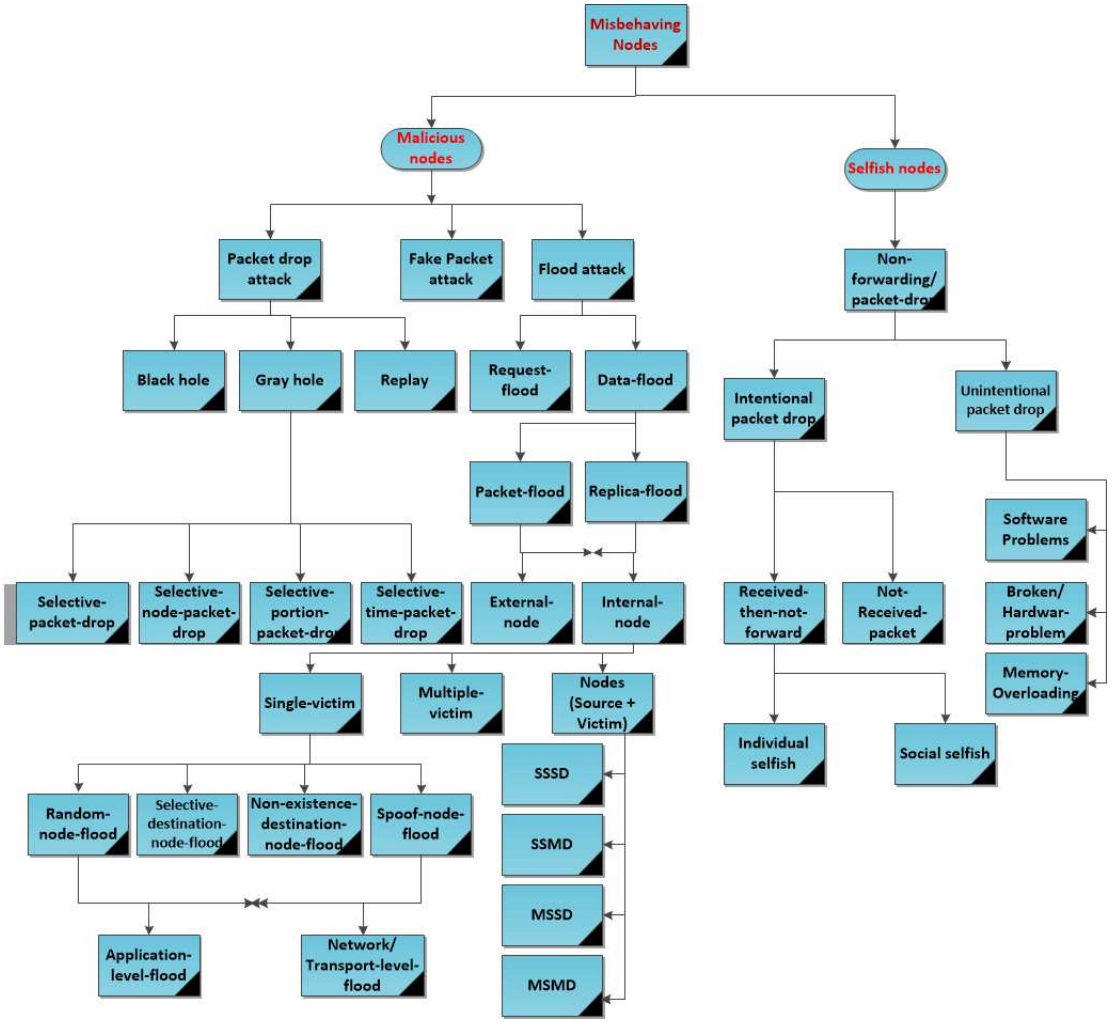

Fig. 2. Misbehaviour Attacks Taxonomy

packets to induce attacks. Malicious nodes launch DOS attack to waste resources and also disrupt the availability of nodes [122]. Here, three different types of attacks that launched by malicious nodes are presented.

1) Packet Drop Attacks: Malicious nodes drop packets to trigger DOS attack [123]–[125], that leads to the decrease in packet delivery ratio, and ultimately causes information loss. These malicious nodes normally drop the whole packet or part of a packet, and we categorize packet drop attacks into further sub-categories:

a) Black Hole Attack: The malicious node drops all packets [126], [127].

b) Gray Hole Attack: The malicious node drops complete or part of the packet [57]. Furthermore, gray hole attack is divided into the following sub-categories [78].

- Selective-Packet-Drop: The malicious node does not drop all packets but drops selective packets.
- Selective-Node-Packet-Drop: The compromised malicious node drops packets from selective nodes.
- Selective-Portion-Packet-Drop: The malicious node does not drop the whole packet, but drops some portions of packets, such header information.
- Selective-Time-Packet-Drop: The malicious node drops the packet during a selective time.

c) Replay Attack: The malicious node which receives packets but forwards them with delay, is defined as replay attack.

2) Fake Packets Attack: In this attack, the malicious node sometimes drops legitimate packets and injects bogus packets.

3) Flood Attack: In flood attack, malicious nodes transfer as many bundles as possible to consume nodal resources (e.g. buffer and bandwidth) [128]–[132]. Whenever malicious nodes inject a large number of packets in the network, this causes resources consumption, losses legitimate messages and creates unavailability problems. We further classify the flood attack into the following two sub-classes:

a) Request-Flood: In this attack, malicious nodes establish communication session with server or another node. In traditional networks, a node sends HTTP request-packets to launch DOS attack to degrade server and work-stations resources. Whereas in DTNs, there is no need of communication session establishment like TCP/IP based network. Therefore, the request-packet flood is not effective in DTNs, due to lack of handshaking protocol in DTNs.

b) Data-flood: The malicious nodes send a large number of data packets instead of solely request-packets. Inherently, data-flood attack overwhelms the resources of DTNs nodes, most of the attackers used this strategy to launch flood attacks. We herein categorize the data-flood attack into two major classes based on the malicious node strategy, which are packet-flood and replica-flood attack [133], [134].

- Packet-flood: A malicious node sends a large number of unique packets to others, aiming to exhaust their buffer, also known as breadth attack [135].
- Replica-flood: A malicious node injects replicas of the same message to waste resources (e.g. bandwidth and buffer), also known as depth attack [135].

We have also classified packet-flood and replica-flood attacks into two further sub-categories based on the cryptography information.

- External-node: The malicious node does not have valid cryptographic credentials, such as key and node Identity (NID), is called external-node.
- Internal-node: Nodes which belong to the network having valid cryptographic key are internal-nodes. Internal malicious nodes are further classified into the following sub-classes on the basis of victim selection.
  - Single-Victim: When the malicious node selects a single node to forward messages and thus results in the overflow of buffer and processing, the victim node becomes unavailable for other nodes due to opportunistic nature of DTNs. This can be further classified into:
    - Random-Node-Flood: The malicious node selects the victim randomly to launch flood attack in the network [134], [136].
    - Selective-Destination-Node-Flood: In this type of flood attack, the malicious node selects a designated node to execute flood attack. Nodes having the highest participation in the relay process are targeted. Here, malicious nodes explore the predictability property of nodes from the routing decision, e.g. decision based on predictability in probabilistic routing protocol using history of encounter and transitivity (PROPHET) [137]. The active nodes in the network are targeted by the malicious nodes [134] [136].
    - Non-Existence-Destination-Node-Flood: In this attack, the fake message is created and forwarded to nodes that do not exist in the network. As such, malicious nodes achieve their goal by wasting other nodal resources. It is worth mentioning that the fake messages would remain in network until their Time To Live (TTL) expires [134] [136].
    - Spoof-Node-Flood: In spoof flooding attack, malicious nodes spoof their identities to launch DOS based flood attack [134], [136].

    The flood attack can be further classified into following two categories, based on the protocol layer:
    - Application-Level-Flood: These attacks target to overuse the resources of server such as CPU and socket [138] [139].
    - Network-Level-Flood/Transport-Level-Flood: Network-level-flood/Transport-level-flood attack [138] [139] is more common in DTNs under which misbehaving nodes continuously flood packets to misuse the network resources (e.g. bandwidth and buffer).
  - Multiple-Victim: When the internal malicious node in DTNs selects multiple nodes to forward unwanted messages, this is called Multiple-victim attack.
  - Source + Victim: On the basis of source plus victim, the following four attacks are further classified:
    - Single-Source-Single-Destination-Flood (SSSD): A single source node targets only one destination node.
    - Single-Source-Multiple-Destination-Flood (SSMD): A single malicious node targets multiple destination nodes to induce flood attacks.
    - Multiple-Source-Single-Destination-Flood (MSSD): Multiple malicious source nodes target single destination node.
    - Multiple-Source-Multiple-Destination-Flood (MSMD): Multiple source malicious nodes target multiple destination nodes to overuse limited resources of legitimate node.

B. Selfish Nodes

Nodes that do not forward packets are defined as selfish nodes. There are many reasons of packet drops [140]–[150], that are categorized into following two classes.

1) Intentional Packet Drop/Wicked-Selfish: Nodes with sufficient memory and forwarding power, but still drop packets intentionally are defined as wicked-selfish nodes. We categorize intentional packet drop into two sub classes [151].

a) Receive-then-not-forward/Hypocritical-Selfish: Sometimes selfish nodes receive packets from forwarder node but silently drop those packets, we call it hypocritical-selfish node.

b) Not-Receive/Deaf-Dumb-Selfish: Deaf-dumb-selfish nodes intentionally do not receive packet from the forwarder node, in order to save its own resources. Such type of selfish node can be further categorized in to two sub classes, which are individual and social selfish nodes [152], [153].

- Individual Selfish Nodes: It refers to node drop packets from all other nodes in a network.

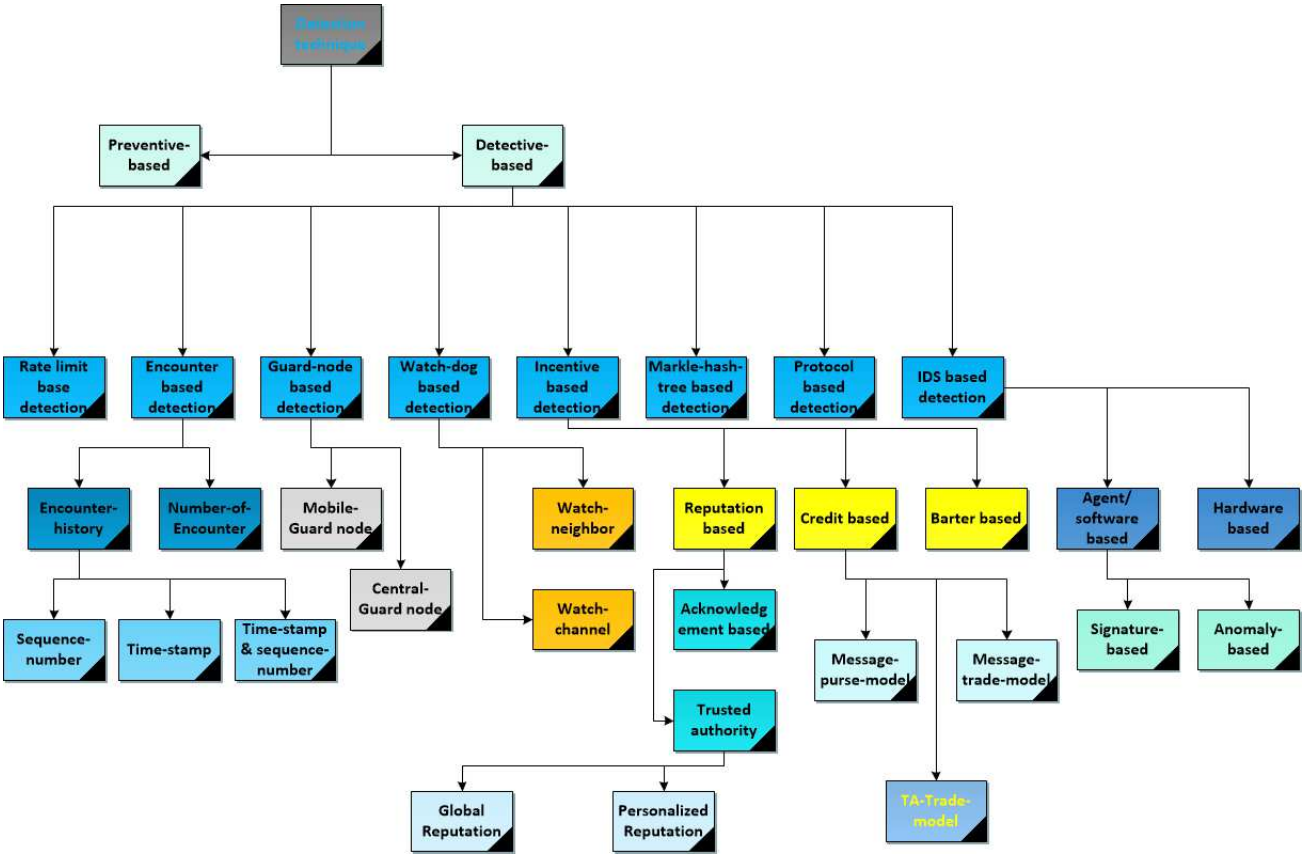

Fig. 3. Misbehaviour Nodes Detection Techniques Taxonomy

- Social Selfish Nodes: It refers to nodes belong to particular group and drop packets from other groups, however, does not drop packets from its own group members.

2) Unintentional Packet Drop/Innocent selfish: This kind of packet drop can occur due to scarce resources. Unintentional packet drop may also occurs due to software fault, broken node (hardware problem), forwarding power and memory overloading [140], [154].

III. Detection Techniques

In this section, we discuss different detection techniques to cope with misbehaving nodes in DTNs. There are two basic approaches, namely detective and preventive based solutions [155]. Figure 3 shows a summarized classification.

A. Rate Limit Based Detection

Nodes send request packets to Trusted Authority (TA) for getting the rate limit certificate (RLC). Here, TA issues RLC, while forwarders send packets along with the RLC, to prove the behaviour of legitimate node. The number of packets can be counted by source nodes, destination node and central authority. In DTNs, source nodes can easily count the number of packets [133], however, it is difficult for destination node and central authorities to count packets due to lack of end-to-end connectivity.

B. Encounter Based Detection

Encounter is defined as the contact of pairwise DTNs nodes. When encounter occurs, each node saves history in terms of time, frequency, node id's and sequence number of forwarding packets etc. Previous works have proposed detection and mitigation algorithms to deal with node's misbehavior pattern. We herein categorize them into two categories, which are based on Encounter-History (Save nodes Contact information, that is id's, sequence number of packets and frequency etc) and Number-of-Encounter (number of encounter with every node). Based on these information researchers detect misbehaving nodes (selfish node) which launches packet drop attacks. Furthermore, the Encounter-History based schemes has three sub-classes, namely Sequence-Number, Time-Stamp and combination of time stamp and sequence number (Hybrid approach). Some of the researchers used only sequence number of packet to detect selfish nodes. In some research articles, researchers used Time stamp of encounter packets to cope misbehaving nodes. Some works proposed combination of above two method which is hybrid approach to mitigate misbehaving nodes.

C. Gateway-Node/Guard-Node Based Detection

The detection and mitigation carried out by the third party is called guard-node based detection. The following are the sub categories.

1) Central-Gateway-Node/Central-Guard-Node Based Detection: In the Central-Gateway-Node detection, the detection and mitigation is done through one centralized node (placed in specific position according to the requirements). Such central node monitors all the traffic activities. Although the entire network traffic passes through the Central-Gateway-Node, this method is ineffective in DTNs as the concept of centralize routing is infeasible.

2) Mobile-Gateway-Node/Mobile-Guard-Node Based Detection: In this type of detection scheme, the Mobile-Guard-Node travels along the packet, to observe the behavior of others. However, this method is not that effective in DTNs, because there is no end to end connectivity.

D. Watch-Dog Based Detection

In Watch-Dog based detection [156], each node keeps and eye on other node for packets received and forwarded. We have categorized this type of detection into two further sub classes.

1) Watch-Neighbor Based Detection: In a Watch-Neighbor based detection, node directly watches their neighbors' behavior to check their selfishness.

2) Watch-Channel Based Detection: Here, node forwards message to intermediate nodes and keeps a copy of message in buffer. It continuously checks the channel for overheads, thereby the case with no overhead means intermediate node is selfish.

E. Incentive Based Detection

In literature, few articles have proposed incentive based algorithms to tackle misbehaving nodes, especially selfish nodes in DTNs [157], [158]. Generically, there are three types of incentive solutions named as reputation based, credit based and barter based.

1) Reputation Based Detection: In Reputation based scheme researchers assign reputation (Threshold value/Reward value). Reputation is increased when they forward packets and decreased when they drops packets to encourage misbehaving nodes to participate in forwarding. Receiver always check reputation value before accepting and sender always check before forwarding a packets. When a node reputation is below threshold value, receiver/sender not accept/not forward packets. The reputation of node is calculated by two methods, either TA calculates nodes reputation or calculated from *acknowledgement*. The TA gives reputation directly to the selfish nodes, to encourage selfish nodes to participate in forwarding process to enhance network throughput and performance. In acknowledgement based reputation solutions, the reputation of a node is calculated from acknowledgement (When they forward packets, node acknowledges which other nodes prove his innocent behavior) of the intending receiver of the messages. Either increase or decrease of nodal reputation is used to handle misbehaving of selfish nodes. The TA based reputation is further divided to two sub-classes that are **Global-Reputation** and **Personalized-Reputation** [159]. In global-reputation solution, TA collects information from all nodes to calculate reputation. On the other hand, in personalized-reputation, the information is collected from specific group members to calculate the reputation.

2) Credit Based Detection: Here, the misbehaving nodes which do not participate in the forwarding process [160], rather forward packet with an encourage of credit/reward. The credit based detection is further categorized into three sub-classes, which are as follows:

a) Message-Purse-Model Detection: When source nodes give credit to forwarding nodes, it is called Message-purse-model [161].

b) Message-Trade-Model Detection: In Message-Trade-Model, a destination node gives credit to forwarding nodes [161].

c) TA-Trade-Model Detection: When a TA or other than source and destination nodes give credit to a node, we call it as TA-Trade-Model. It improves the shortcomings of above two methods.

3) Barter Based Detection: Barter based detection is used to encourage nodes to participate in relay process. Barter based are bargaining strategy (Nodes forward packets with condition). Here, an agreement is signed between nodes to overcome the selfish behaviour, and various barter based algorithms have been proposed to thwart selfishness problems [162]–[165].

F. Merkle-Hash-Tree Based Detection

The Merkle-Hash-Tree is a complete binary tree of hashes. Hashes are calculated from left bottom to top (left leaf node first then right leaf node and then root node). Popular hash algorithms such as SHA1 and SHA2 have been applied. The Merkle-Hash-Tree based detection is also used to detect and mitigate malicious nodes [166]–[169], where a root hash value is added to every packet to detect and mitigate misbehaved nodes.

G. Protocol Based Detection

When some extra capability is plugged into an existing Bundle security protocol to detect and mitigate misbehaving nodes, this article calls this Protocol Based Detection. Some authors proposed Protocol based detection for flood attacks. In protocol based detection authors used Hash value, node id's and signature along with Bundle Security protocol to mitigate malicious nodes. According to our knowledge this method are cheapest to detect malicious nodes. However it only detect outsider node (node do not have a valid cryptographic credential) and unable to detect insider node, which is down side.

H. Intrusion Detection Scheme (IDS) Based Detection

The IDS is a very powerful technique to detect and mitigate attacks in all types of networks [170]. Generically, there are two types of IDSs, with agent based/software and hardware based features. The agent based detection is further classified into two types, with the features of signature based and anomaly based. In signature based, data base of known attack signature is created, which is used to compare for attack detection. In Anomaly based detection, attack is detected with malicious nodes behavior.

Critical Analysis of Detection Techniques: Researchers proposed various method to detect and mitigate misbehaving nodes which launches attacks. According to the critical analysis of this article, Some proposed detection techniques are very efficient to detect malicious nodes. However, few proposed schemes are not efficient to mitigate malicious nodes due to challenging nature of DTNs. Some proposed detection techniques are applicable in constraint environment (Guard-Node, Watch-Dog) or used for specific misbehaving attacks (Flood or Packet drop or Fake packet) detection (Incentive based, Merkle hash tree based, Rate limit based, Encounter based). Few proposed detection techniques detect malicious nodes, Nonetheless it required extra node for detection (Gate-Way-Node). Some detection methods detect malicious nodes by forwarding extra information along with packets (Rate limit base, Encounter based), which consumed resources. Some of detection techniques are centralized (which need one node for detection) like Central-Guard-Node and Mobile-Guard-Node. On the other hand few proposed methods are distributed (detection is distributed among node) like Rate limit based and encounter based algorithms. Fewer proposed methods used TA in mitigation process which improve false positive and false negative ratios.

According to the analysis of this article Rate limit based and Encounter based algorithm are best suitable relative to other methods to detect flood and packet drop attack. Because both schemes are distributed and have TA, which are suitable for DTNs. Rate limit based algorithms detect malicious nodes which launches flood attacks. Encounter based algorithms detect misbehaving nodes which launches flood and packet drop attacks. The down side of Rate limit based algorithm is high detection time. Because it used cross checking strategy to detect malicious nodes. In DTNs nodes are not always connected. Detection are not possible until encounter of other nodes, which share information. Which obviously take time, so resources consumption are high in Rate limit based algorithms. Rate limit based algorithm are useful an environment in which encounter opportunity are high.

The down side of Encounter based algorithms is storing and sharing of encounter history with other nodes. Which consumed buffer and like Rate limit based it always need connected environment, but in DTNs it is not possible always. Also sharing of extra information along with packets in detection is biggest problem in encounter based algorithms. Which consumed limited resources of DTNs. Due to resources consumption packet delivery ratios are decreased and packet loss ratios are increased. Which will be discussed in more detail in mathematical and simulation section of this article. According to analysis of this article, if extra information is completely remove or compress, it will improve delivery ratios and packet loss ratios problems.

Guard-Node based detection method is not very suitable in DTNs. Because in Central-Guard-Node every packet is passed through Central-Guard-Node. And Mobile-Guard-Node one specific node travel along every packets. The deployment of both cases in DTNs are very difficult due to disconnected nature of DTNs. The remedy for this problem is distributed algorithms, in which more than one node is responsible for mitigation.

Incentive based algorithms are not bad option to detect misbehaving nodes which launches only packet drop attacks. There are three categories which are already mentioned in this article. Reputation based algorithms are very efficient to mitigate malicious nodes which launches packet drop attacks. The down side of Reputation based incentive algorithms is calculation (Either TA give reputation, or calculated from acknowledgment). Which is costly and may have high ratio of false positive and false negative. If TA calculate reputation it will keep track of all networks, which is very difficult. On the other hand when reputation is calculated from acknowledgment, it always required connected environment like TCP/IP base networks.

Credit based incentive algorithm are also good approach. However, Credit based algorithm only motivate those selfish nodes which not take in forwarding process (save own's resources). The down side of Credit based algorithm is complex calculation and distribution of credit. There two method for credit distribution Message-Purse-Model (In which source give credit) and Message-Trad-Model (In which destination give credit). In both cases false positive and false negative ratio is high. This article proposed TA-Trad-Model (In which other than source and destination give credit) which overcome the shortcoming of above mentioned both methods.

Barter based incentive is not suitable in DTNs. Because in Barter based algorithm agreement is sign between nodes for forwarding each other packets. Which always need connected environment between all nodes. Barter based is very difficult to deployed in DTNs.

Merkle-Hash-Tree based algorithm are useful to detect malicious nodes which launches fake packet attacks. The down side of Merkle based algorithms is complex calculation of Hash tree in sender side and verification in receiver side. Which is costly in term of buffer, bandwidth, battery and processing usage. Also Merkle-Hash-Tree scheme have high false positive and false negative value. Because in proposed algorithms only black list previous nodes in forwarding, which may not malicious. Which is very big issue in Merkle-Hash-Tree based algorithms. Also the other downside of Merkle-Hash-Tree based algorithms is only detection of fake packets. However, some malicious nodes launches packet drop attacks instead of fake packet attacks, which is not detected by proposed algorithms. in future we will proposed algorithm for fake packet and packet drop attacks which overcome false positive and false negative ratio.

Protocol based algorithm is fair idea to detect malicious nodes which launches flood attacks. But according to our knowledge it only detect outsider malicious nodes. If some extra capability is plug-in an existing Bundle Security Protocol to detect insider attacker. Which will be most efficient and cheap method for misbehaving nodes which launches flood attacks.

According to our knowledge IDS based scheme is not proposed for detection of flood attacks in DTNs. IDS based scheme is fair idea (not complex calculation, distributed, easily deploy and suitable in challenging environment of DTNs) according to our analysis to mitigate malicious nodes which launches flood attacks.

Apart from the above some analysis this article will further analyzed detection techniques with various proposed parameters rigorously in analysis section of this article.

IV. Review of Literature

The misbehaving nodes are catastrophic for DTNs, as they often waste the important and limited network resources. In [136], a queuing mechanism (distributed buffer management scheme) has been proposed. Here, when a node encounters infrequently and forwards more messages, it is indicated as malicious behavior of a node. As such, less buffer space is allocated to all the suspicious nodes, and more buffer space is allocated to frequently encounter nodes.

Although this is very good scheme for detection of malicious nodes which launch flood attack, this scheme works only for probabilistic routing protocol PROPHET [137]. If a node encounters infrequently we can not assume that it is malicious because of the sparse nature of DTNs nodes. In [135], a Gateway-Node to detect and mitigate a flood attack in DTNs is proposed. In this scheme, all the nodes that upload or download bundles, share their buffer status to gateway-node. The Gateway-Node has a data structure, while saves a number of different packets and replica count of nodes. If a node forwards more than allowed number of messages, the Gateway-Node detects it as resource misuse attack. Probabilistic detection techniques for depth attacks have also been proposed to enhance detection time.

In [133], rate limit technique is used to detect and mitigate flood attack. Here, all nodes in network send/forward request for the rate limit certificate to TA. The TA gives rate limit certificate to nodes according to the their requirement. Every node creates a P-claim (packet count claim in current time with a signature) and T-claim (count claim in current time and how many times they forward copy of the packet claim), and sends it along with a packet. Nodes in network cross-check P-claim and T-claim. If there is any inconsistency (nodes find malicious according to pigeon hole principle), the source node is listed as an attacker node. Note that, the cross checking is very difficult in DTNs scenario, as it does not detect the malicious nodes until other node cross checks. The work in [171] enhances that in [133] to add learning automata algorithm, to approximate count packets. In [172], the method is quite similar to [133], to detect and mitigate flood attacks. Authors in [173], also propose a scheme almost having a similar functionality as [133], but it adds crypto key with the existence scheme, by using advance encryption standard (AES) algorithm.

In [174], it uses claim-carry-check method to detect flood attack in DTNs. In [138], the proposed system similar is to [133], which detects both application level and network-level flood attacks in DTNs. The authors have proposed rate limit technique to detect flood attack, which uses cross checking method for inconsistent claim made by the malicious nodes. In [175], the scheme uses rate limiting technique to thwart a flood attack. While, [176] propose a rate limit algorithm using RSA to find exact malicious attackers. The work in [177] mitigates packet flood and replica flood attacks.

Researchers in [178] use three different types of DTNs cookies (hash value of time-stamp, source-id, random-number). The first type of cookie is made from concatenation of time-stamp, source-id and Random-number. The second and third type of DTNs cookie use XOR operation and HMAC for more randomness. The cookie verification finds malicious nodes and then blacklists those nodes that launch flood attacks, whereas this stops only outsider malicious nodes (a malicious node which not have valid cryptographic credentials).

In [179], the proposed reputation solution assumes that there is TA in the network. Malicious nodes flood network with bogus messages, but cannot create genuine messages. Initially, each node in the network creates a message and forwards it to TA. The TA gives reputation based on genuine message. If the reputation of a node is greater than or equal to predefined threshold value, the node will accept message otherwise reject. Some questions are left behind by this mechanism, like what is the criteria for genuine messages? Why malicious nodes does not create genuine messages? How TA recognized genuine messages and bogus messages? The proposed algorithm is suitable only for ideal environment.

In [180], author propose a piggyback scheme to detect multiple attacks associated to black hole, gray hole and flood attack in DTNs. The encounter record scheme with rate limit is used to detect multiple attacks. Malicious nodes have two choices that

to either change the time-stamp or alter the sequence-number of encounter records. This algorithm easily detects misbehaving malicious nodes, but the downside of this algorithm is detection time and cost. However, it detects malicious nodes only if other nodes would share encounter, and that is not suitable in DTNs.

In [181], a stream-node is designed to monitor the network. The Stream-Node contains three tables which are rate-limit table, Dpt-tab (delivery probability table) and B-list (black list) table. The Stream-Node compares the actual delivery probability with an estimated delivery probability. If the difference is greater than pre-defined threshold value, the stream-node detects it as malicious and blacklists that node.

The work in [182] propose probabilistic misbehaving node detection scheme (PMDS) to detect and mitigate malicious node in DTNs. This algorithm consists of event generation and auditing phases. In the event generation phase, events related to delegation, contact and forwarding of every node are recorded. In the auditing phase, the TA collects all event generation information from different nodes, to check if that node is malicious or not. For efficiency and performance, the TA checks nodes with low reputation frequently and that with higher reputation infrequently. Although this is very efficient algorithms to detect malicious node, it is expensive and not suitable for DTNs.

In [183], [184], an observer node monitors all network for selfish nodes. The proposed algorithm assumes that observer node has all public keys of every node. However, observation based detection is very difficult to implement in practical DTNs environment, due to sparse and disconnected nature of DTNs nodes.

In [42], the proposed scheme mitigates packet dropping attacks in DTNs, using contact history based detection. In this algorithm, every node saves its previous contact history, and shares its contact history information with others to detect misbehaving nodes. The proposed algorithm detects inconsistency and misreporting, either in sequence-number and time-stamp. Here, every node keeps contact history information that is down side of algorithm, due to limited resources and opportunistic feature in DTNs.

The credit based schemes proposed in [160] and [185] detect misbehaving nodes through Offline Security Manager (OSM) and Virtue Bank (VB). The OSM is responsible for issuing a certificate to a node and VB is for distribution of credit among nodes. If a node forwards a data to intermediate node, the source node must make a base-layer including nodes IDs, class of service, agreement policy, TTL, time-stamp, certificate, source signature and next forwarder node ID. Intermediate node makes a multiple endorse-layers (Base-layer with digital signature), when the packet is successfully transferred to the destination, destination nodes collect information from all layers and forward it to the VB. The VB calculates and shares a credit among all the participating nodes in relay process. This scheme is prone to processing cost and bandwidth consumption, thus is inefficient in DTNs.

In [126], the proposed algorithm enables all nodes to make packet sending list and receiving list, which is updated directly or indirectly. The work in [154] uses channel sensing mechanism of Watch-dog schemes to detect misbehaving nodes. When a source node forwards a packet to intermediate node, it keeps the original message in its buffer. The source node continuously monitors the channel. If intermediate node sends a packet to destination so source compares the overhead of channel to its buffer. If match then node is not malicious otherwise source detect the intermediate node is malicious. But there is possibility that intermediate node drop a packet and sends its own packet. Also there is probability that other node send a messages so there is overhead in channel. The source assume that node is not malicious but in reality the node is malicious. The false positive and false negative is very high in this particular detection scheme.

The work in [159] mitigate two type of malicious attacks. That is Bad-mounting (when a Rater decreases the reputation of service provider) and Ballot-stuffing (when a Rater increase the reputation of service provider from low to high). The authors derive a formula for global reputation and inconsistency. The proposed algorithm compare inconsistency value and threshold value. If inconsistency value become less than threshold value, node is not malicious, otherwise malicious. Reputation and trust based scheme are not effective in DTNs due to unique nature of DTNs. The ratio of false positive and false negative is high in this particular algorithm.

The proposed work in [186] improved the research of [159] by categorizing a Rater (R) based on the rating to service provider (SP) with low, middle and high priority cluster. This gives a second chance for node to prove that they are not malicious unlike existing iterative trust and reputation management system (ITRM) [159]. The Proposed algorithm have low false positive as compare to ITRM scheme and complexity is linear to cluster unlike existing ITRM that is linear to nodes. In [168] proposed a Merkle-Hash-Tree and trust value to detect and mitigate a selective packet dropping attack in Opportunistic Networks (OppNets) a type of DTNs. It calculates root hash and then append with every packet. Destination node checks, if hash is not verified, thus decrease the trust value of previous node path. In case of multi hop it decrease the trust value of all nodes in the path that may include some legitimate nodes. The false positive and false negative is high in proposed algorithms.

Researchers in [187] proposed an algorithm to detect misbehaving malicious nodes that launch a packet dropping attacks in DTNs. It detects the packet dropping attack by examining the header field which is called indicative field. Indicative field are further divided into three sub field, identification field, flag field and offset field. This is very good scheme but the main problem of this algorithm is cost and the ratio of false positive and negative.

Researchers in articles [188]–[191] discussed different incentive based, reputation based and game based schemes to cope selfish node in DTNs which is responsible for packet drop. The authors also analyzed the impact of selfish nodes on packet delivery ratio in DTNs. The paper [192] proposed collaborative trust management system which is actually Watch-dog based

system to detect malicious node in post disaster scenario. Watch-Dog based system is not very effective in DTNs due to high ratio of false positive. In [193] the proposed Global reputation estimation and analysis technique (GREAT) that is distributed reputation scheme without trusted authority to detect malicious and selfish node in post disaster environment. The proposed scheme detect packet drop, Ballot-stuffing and bad-mounting attacks in DTNs. This work has no involvement of TA and complexity of reputation estimation makes it in-feasible for DTNs.

In [194] the authors proposed a scheme for detection of malicious nodes which drop packets and include a new fake packets in OppNets. The authors proposed a packet creation time to detect attacks. Destination node check the creation time of packet if same or nearly same, algorithm assume node is not malicious otherwise malicious. The proposed scheme is efficient but if malicious node create a packet with legitimate time, then non detectable. Researchers in article [195] proposed the combination of reputation and trust based algorithms to detect malicious path and malicious node in OppNets. The proposed algorithms detect malicious node by using Merkle-Hash-Tree and reputation. In this scheme researchers calculated hash value of every packets. Destination node compare hashes with number of packets. If number of packet is equal to hashes so algorithm assume the node is not malicious. The main problems of this algorithm are cost and lack of TA that leads to more ratio of false positive and false negative. Also the researcher assume that one packet must be reach to destination. But if malicious node drop all packet so algorithm fail.

The authors in [167], [169], [196] propose a Merkle-Hash-Tree to detect a malicious nodes which drop packet and add fake packets. It calculates root hash, and then appends it with every packets. The destination node recalculates hash, if that matches with attached hash then no attack is detected. In case of multi hop case, the proposed scheme detects only the last node which may or may not malicious.

V. Analysis

This section analyzes and summarizes the related work and detection techniques based on our proposed parameters. Misbehaving selfish and malicious nodes launch various attacks such as packet flood, packet drop and fake packet. Related work above three attacks are summarized in Tables I, II and III respectively. The following parameters were used to analyze and evaluate the related work.

- **Approach**: This parameter indicates the type of algorithm used i.e. detective or preventive.
- **Detection method**: There are two methods to deal with misbehaving nodes i.e. probabilistic and deterministic.
- **TA**: Existence and nonexistence of TA and its repercussions.
- **Detection mechanism**: The complexity of detection algorithm.
- **Scheme**: Centralized and Distributed detection.
- **Detection criteria**: Various detection criteria and its impact.
- **Mitigation**: Efficiency of mitigation algorithms to save scarce resources.
- **Action by**: In case of detection, the target node or TA or the designated node can take the mitigation action.
- **Type of attack**: Malicious nodes usually launch flood, fake packet attack and sometimes packet drop attack. On the other hand, selfish nodes launch packet drop attack usually.
- **Problem**: Shortcomings of the techniques described in literature.
- **Additional feature:** Enlist additional features.

The fake packet attacks are summarized in Table I except [187] and [168] that detect selective packet drop attacks. The techniques are mainly based on packet creation time, trust and Merkle-Hash-Tree. Among these three techniques, Merkle-hash-Tree based is relatively efficient to detect malicious nodes. However, Merkle-Hash-Tree incurs additional cost for hash calculation and verification. Due to the scarce resources in DTNs, there is need of an efficient and low cost technique.

All techniques detect only malicious node except [180] that detects both malicious and selfish node summarized in Table II. Moreover, all techniques detect flood attacks except [180], that detects multiple attacks such as flood, black hole and gray hole. Furthermore, all discussed algorithms blacklist the malicious nodes except in [136], which allocates less buffer space to malicious nodes. Most of the researchers have proposed rate limit based algorithms for detecting malicious nodes, that are effective in DTNs. Because rate limit based algorithms are distributed in nature, the TA based algorithms have minimum issues of false positive and false negative. Some of the works proposed Watch-Dog, Guard-Node and encounter based schemes, however they are costly and not suitable for DTNs. According to observations, low cost and distributed algorithms are required to detect malicious nodes in DTNs.

In literature, various algorithms have been proposed on selfish nodes summarized in Table III. Mostly, techniques are based on incentive solution to counter misbehaving nodes. In literature, many other schemes were proposed such as Watch-Dog based, credit-based and reputation based incentive schemes. We concluded that reputation based algorithms are costly and difficult to deploy in DTNs. However, reputation based algorithm is better compared to watch-dog based and Credit-Based. The Credit-Based scheme fails in situation where network have large number of misbehaving nodes.

Table IV analyze detection technique categories based on our proposed parameters which are:

- **Applicability To DTNs**: This is very an important parameter because some proposed algorithms are not suitable for DTNs. This article consider three levels for applicability that is High, Low and Moderate.

TABLE I
FAKE PACKET ATTACKS/MALICIOUS NODES

Article	Detection criteria	Detection method	Mitigation	Problems
[194]	Packet creation time	Each node add time to packets	destination node arrange packet if creation time is not same, node detects malicious and black list nodes	If Malicious node send a packet with legitimate time so what about this? Algorithm detect only fake packet not malicious nodes
[167], [169], [196]	Merkle-hash-tree	Node add root hash to each packet	Destination node calculates root hash if match proceed otherwise malicious. Node black list all nodes in the path.	If only one node in the communication path is malicious,that leads to whole path malicious
[168]	Merkle-hash-tree, trust value	Node add root hash to each packet	Algorithm calculates the root hash if not match so decrease the trust value of nodes in the path by 0.1 if trust value of the nodes become less than 0.2, the node is declared malicious.	The trust value of honest node is decrease if it belongs to malicious path. Detection of malicious node below the threshold value 0.2.
[187]	Merkle-hash-tree	Node add special header in the packets	Indicative filed contains three fields: Identification, flag and offset field. Through identification field node find malicious nodes	More false positive and false negative

- **Shortcoming**: Various shortcomings in the literature schemes.
- **Cost**: Some of algorithms have very high cost due to deployment of extra node to detect malicious nodes. Some of the proposed algorithms also need high processing both on sender and receiver side. Based on these observation this article analyzes that:

$$\text{Cost} = \text{Processing Cost} + \text{Extra Node Cost} \tag{1}$$

  However, we only consider the cost of extra node and assume that processing cost is the same for all detection algorithms. We take two levels for cost: high and Low, where for extra node the cost will be high.
- **Buffer Consumption**: Some of the proposed algorithms store history and other information in the buffer, thus overflows buffer and decreases packet delivery ratio. We consider three levels for this, that are High, Medium and Low to analyze the detection algorithms.
- **Extra Node**: Some of algorithms require extra node to identify malicious node.
- **Detection Accuracy**: Some of algorithms aim to tackle misbehaving nodes in DTNs. False positive and false negative ratio are high, which is catastrophic for DTNs. Based on these observations this article consider three levels: Low, Average and Good.

VI. MATHEMATICAL EVALUATION

This section analyzes the performance of above discussed algorithms in detail. The exact value of all constants and its relation with parameters are out of the scope of this article. Also, exact dependency of parameters and its exact value is the future work of this article. The Opportunistic Network Environment (ONE) [197] is used for simulation that is specifically designed for DTNs. The parameters considered are: number of nodes (50), nodes are mobile, simulation time (20000 sec), random way point mobility model, wait time (120), TTL (300). This article used various routing protocol for simulation which is follow as. Epidemic, Direct Delivery, SprayAndWait, Prophet and First Contact. This article used all mentioned routing protocol for simulation. However, all protocol shows similar results, That is why for illustration results of some protocol are shown in this article. For illustration Epidemic is evaluated for the impact of buffer with packet delivery and loss ratios. SprayAndWait are used for impact of packet size, node speed and transmission range on packet delivery and packet loss ratios. Epidemic, First Contact, Direct Delivery, SprayAndWait and Prophet are used for impact of wait time on packet delivery and packet loss

TABLE II
FLOOD ATTACKS/MALICIOUS NODES

Article	Approach	Scheme	Detection method	TA	TA Role	Detection Criteria	Detection Mechanism	Action by	According Figure 3	Additional Feature
[136]	Detective	Distributed	Probabilistic	-	-	Encounter	Number Of Encounter	By-Self	Encounter Based	Buffer Management Formula
[135]	Detective	Centralized	Deterministic & Probabilistic	-	-	Threshold	Count Number Of Packets	Gate-way Node	Encounter Based	Gate-way
[133]	Detective	Distributed	Probabilistic	+	1) RLC 2) Black listing	Rate-Limit	Claim-Carry-check	TA	Rate Certificate Based	Aggregate Signature With Merkle-tree
[171]	Detective	Distributed	Probabilistic	+	1) RLC 2) Black listing	Rate-Limit	Claim-Carry-Check	TA	Rate Certificate Based	Learning Authomata
[172]	Detective	Distributed	Probabilistic	+	1) RLC 2) Black listing	Rate-Limit	Claim-Carry-Check	TA	Rate Certificate Based	-
[173]	Detective	Distributed	Probabilistic	+	1) RLC 2) Black listing 3) Private Key	Rate-Limit	Claim-Carry-Check	TA	Rate Certificate With Key	Key
[174]	Detective	Distributed	Probabilistic	+	1) RLC 2) Black listing	Rate-Limit	Claim-Carry-Check	TA	Rate Certificate Based	-
[138]	Detective	Distributed	Probabilistic	+	1) RLC 2) Black listing	Rate-limit And Mysql/DNs	Claim-Carry-Check	TA	Hybrid	MYSQL/DNS For Application Level Flood
[175]	Detective	Distributed	Probabilistic	+	1) RLC	Rate-limit	Claim-Carry-Check	TA	Rate Certificate Based	-
[176]	Detective	Distributed	Probabilistic	+	1) RLC 2) Private Key With RSA 3) Black listing	Rate-Limit	Claim-Carry-Check	TA	Rate Certificate With Key	Key
[177]	Detective	Distributed	Probabilistic	+	1) RLC 2) Private Key With AES 3) Black listing	Rate-Limit	Claim-Carry-Check	TA	Rate Certificate With Key	Key
[20]	Detective	Distributed	Deterministic	-	_	Protocol Based Defense	DTNs Cookies	Security Gate-way Node	Protocol Based	Cookies
[179]	Preventive	Distributed	Deterministic	+	Reputation	Compare Reputation To threshold	Check Genuine And Bogus Messages	BY-Self	Incentive	-
[180]	Detective	Distributed	Probabilistic	+	RLC	Rate-Limit & Encounter	Sequence Number And Time Stamp	TA	Hybrid	Piggybacking
[181]	Detective	Centralized	Probabilistic	+	RLC	Rate-Limit	Compare Actual Delivery Probability With Estimated Probability	Guard	Rate Based	Guard-node

TABLE III
PACKET DROP ATTACKS/SELFISH NODES

Article	Approach	Scheme	Detection method	Detection criteria	Detection mechanism	Mitigation	Detected node	Detected Attack	Additional Feature
[182]	Detective	Distributed	Probabilistic	Reputation	Delegation, Forwarding, Contact History Pass to Algorithm	Black list malicious nodes	Selfish	Packet drop	TA give Reputation & perform auditing
[183]	Detective	Centralized	Probabilistic	Reputation	Check FTT and RTT	Broadcast information in the network	Selfish	Packet drop	Observer-node
[184]	Detective	Centralized	Probabilistic	Reputation	Check FTT and RTT	Broadcast information in the network	Selfish	Packet drop	Observer-node
[42]	Detective	Distributed	Probabilistic	Encounter history	Sequence number and time stamp	Black list malicious nodes	Malicious	Packet drop	-
[160], [185]	Detective & Preventive	Distributed	Deterministic	Credit-based	Add one Base Layer And Multiple Endorse Layer	Black list Malicious Nodes	Selfish	Packet drop	Vitual bank & Offline Security Manger
[154]	Detective	Distributed	Probabilistic	Watch-dog	Channel Sensing	Black list malicious nodes	Selfish	Packet drop	-
[159]	Detective	Distributed	Probabilistic	Reputation	Compare Inconstancy With Threshold	Black list Malicious nodes	Social selfish	Bad-mounting & Ballot Stuffing	-
[186]	Detective	Distributed	Probabilistic	Reputation	Compare Reputation Inconsistency	Black list Malicious Nodes	Social selfish	Bad-mounting & Ballot Stuffing	Clustering Which Enhance The Scheme

TABLE IV
ANALYSIS OF DETECTION TECHNIQUES

Category	**Applicability To DTN**	**Shortcoming**	**Extra Node**	**Cost**	**Detection Accuracy**	**Buffer Consumption**
Rate Based	Moderate	Cross-checking, Detection time	Yes	High	Average	Low
Encounter based	Moderate	Buffer-consumption, Detection time	Yes/No	High/Low	Average	High
watch-dog based	Low	Disconnected nature of DTN	No	Low	Low	Medium
Reputation based	Moderate	Collaboration of Selfish nodes	Yes/No	High/Low	Average	High
Credit based	Low	Scheme fail due to High percentage of Misbehavior nodes	Yes	High	Average	Medium
Barter based	Low	If node have not a packet to sent scheme fail	No	Low	Low	Low
Merkle-hash-tree based	Moderate	Detection time and Cost	No	Low	Average	Medium
Guard-node based	Low	Disconnected nature of DTN, Cost	Yes	High	Good	Low

ratio. Table V summarized all parameters and its symbol used in mathematical section. Table VI is Variable stat table, which summarized stat (Independent Variable or Dependent Variable) of variable used in mathematical section.

Performance: Performance is relative parameter which depends on multiple factors, which is represented by Performance-A, Performance-B and Performance-C. There are three arbitrary independent ways to measure Performance according to the analysis of this article, which is represented by Performance-A, Performance-B and Performance-C. There are various parameters which have some certain impacts on the value of Performance. That is why this article classify Performance measurement into three different categories. That is A, B and C. A class depends on applicability (discussed in next paragraph) and buffer consumption broadly. That is Performance is calculated from applicability and buffer consumption. Applicability and Buffer consumption further depends on various parameters, this article discussed all those in detail in next subsequent paragraphs. B class depends on detection accuracy of algorithms, this article calculate Performance from detection accuracy of algorithms (Detection accuracy depends on other parameters, this article discussed all those parameters in subsequent paragraphs). C class depends on cost that is Performance is calculated from cost. Cost of algorithms are divided into two

TABLE V
PARAMETERS SYMBOL LIST

Parameter	*Symbol*	*Description*	*Parameter*	*Symbol*	*Description*
Applicability	AP	AP is very important parameter to evaluate Algorithm in DTNs. Some of the proposed algorithm are not applicable in DTNs because it consumed more buffer space, processing and high cost due to extra node (Guard-Node based). Resources are scarce in DTNs. AP is related to AD and BS.	**Buffer Consumption**	BC	Performance is inversely related to BC. Some proposed algorithm are efficient to mitigate malicious nodes. However it consumed more buffer which cause DR and PL problems in DTNs
Buffer Size	BS	BS is important because due to misbehaving attacks buffer are consumed. Which cause delivery ratio and packet loss ratio problems. DR are directly proportional to BS.	**Algorithm Design**	AD	Performance of algorithm depends on AD. AD is related to Time complexity and Space complexity of algorithms.
Packet Delivery Ratio	DR	It is ratio between Delivered packets to total created packets. Due to misbehaving attacks DR are decreased. The goal of intruder in DTNs to decreased DR.	**Transmission Speed**	TS	NE are increased with TS, which ultimately enhance DR.
Packet Loss Ratio	PL	It is the total drops packets in simulation. Due to misbehaving attacks PL is increased. The objective of malicious nodes in DTNs to increased PL.	**Transmission Range**	TR	TR is directly related to NE, when NE are high so DR will be high and packet loss ratio will be low.
Packet Size	PS	Due to large packet size buffer are consumed which cause DR and PL Problems. Some proposed mitigation algorithm forward extra information (Encounter based) along with packets, which ultimately cause DR and PL problems in DTNs	**Wait Time**	WT	WT is idle time after one packet is forward. WT is inversely related to NE. NE enhance delivery ratios and packet loss ratios.
Number of Encounter	NE	NE is the meeting (Contact) between nodes. NE is directly proportional to DR. NE is increased with TS, TR and WT.	**Detection Accuracy**	DA	The ratio of false positive and false negative indicate DA. Some proposed algorithms have high DA, however few have low DA.
Number of Nodes	NNodes	NNodes is directly related to DA. Rate limit based and encounter based algorithm detect malicious nodes with cross checking. If number of nodes are high so probability of detection will be high.	**Inter Contact Time**	ICT	ICT is the meeting time between nodes. If nodes meet frequently so detection probability will be high. Because some (Rate limit based) proposed algorithm detect malicious nodes with cross checking or encounter strategies. DA is inversely related to ICT.

TABLE VI
VARIABLE STAT TABLE

Equation Number	Independent Variable	Dependent Variable	Equation Number	Independent Variable	Dependent Variable
3	BS	DR, PL	9	WT	DR
4	PS	DR, PL	10	WT	PL
5	NE	DR, PL	14	NNodes, ICT	DA
6	TS	NE, DR, PL	19	DP, CP	PDR
7	TR	NE, DR, PL	20	DP, CP	PLR
8	WT	NE	24	TB, UB	BC

categories that is processing cost and extra node cost (discussed in subsequent paragraphs of this section).

Performance of detection algorithms is directly proportional to Applicability (AP) and inversely to Buffer Consumption (BC). AP is related to algorithm design (Time Complexity and Space Complexity) and Buffer Size (BS). To meet the challenges in DTNs, efficient algorithms are required that have minimum buffer requirements.

$$\text{Performance-A} = (\text{AP} * \text{K1})/\text{BC} \tag{2}$$

Where $K1$ is the constant of proportionality, which depends on multiple parameters e.g., cost, processing power, detection accuracy and processing time. $K1$ is the relative constant which is the ratio between performance times buffer consumption to applicability. Moreover, applicability is directly related to algorithms design (time complexity and space complexity). On the other hand, the delivery and Packet Loss (PL) ratios are related to Buffer Size (BS). If buffer size is increased, Delivery Ratio (DR) also increases [198]. Whereas if buffer size is increased, packet loss ratio is decreased.

$$\text{BS} = (\text{DR} * \text{K2})/\text{PL} \tag{3}$$

Where K2 is constant that depends on multiple factors such as buffer capacity, processing power and connectivity. From the above equation, the delivery ratio is increased with buffer size. While the packet loss ratio is decreased with buffer size up to some certain limit (depending on the value of K2). Fig 4 shows simulation results of packet delivery and loss ratios with buffer size.

Packet delivery ratio and packet loss ratio are related to packet size as well. Delivery ratio is decreased with increased in packet size, and packet loss ratio is increased with increase in packet size [199], as shown in Fig 5.

$$\text{Packet Size (PS)} = C1 * (\text{PL}/\text{DR}) \tag{4}$$

Where C1 is constant of Proportionality, which depends on buffer size and node encounter (connectivity). Moreover, DR is related to number of encounters. The packet delivery ratio increases with number of encounters, while packet loss ratio is decreased. However, the encounter depends on transmission range and transmission speed.

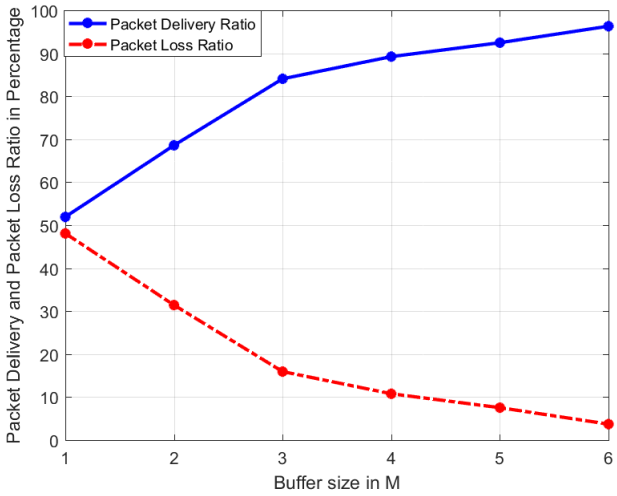

Fig. 4. Impact of buffer size on packet delivery and packet loss ratio

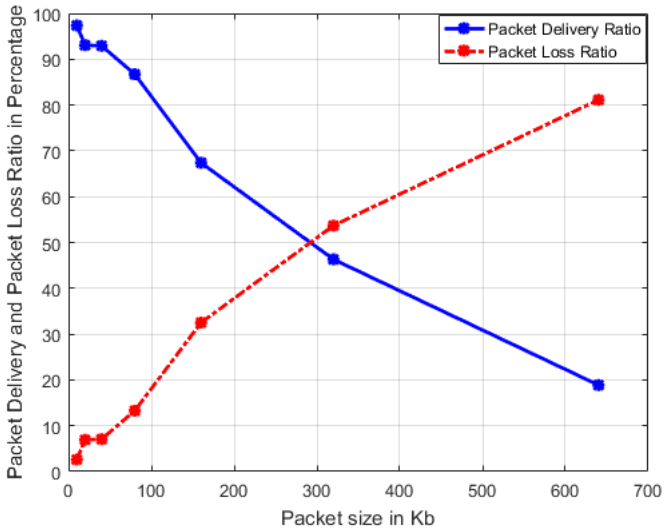

Fig. 5. Impact of packet size on packet delivery and loss ratios

$$\text{Number of Encounters (NE)} = C2 * (\text{DR}/PL) \tag{5}$$

Where C2 is constant which depends on buffer capacity. Eq. 5 implies DR is increased with NE upto certain limit, which depends on buffer capacity. If node buffer is full it means capacity is zero so DR will not increased. NE is increased with moving speed of nodes and transmission range.

$$\text{Moving Speed} = C3 * \text{NE} \tag{6}$$

$$\text{NE} = C4 * \text{Transmission Range} \tag{7}$$

Where C3 and C4 are constants, which depends on multiple factors. When node move fast it will encounter (Contact) with more node. If Transmission Range (TR) of nodes is large it will encounter with more number of nodes, Which is prove in simulation. Furthermore, PL is inversely related to Transmission Speed/Moving Speed (TS) and TR. Figs 6 and 7 show simulation results of packet delivery ratio and packet loss ratio with TS and TR.

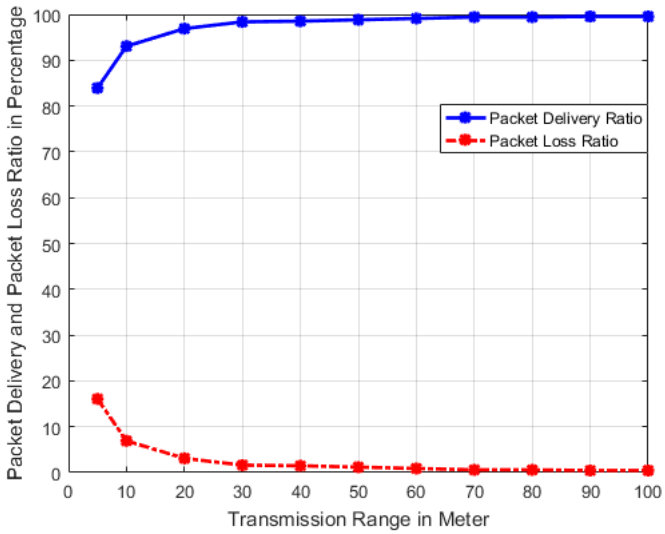

Fig. 6. Impact of transmission range on packet delivery and packet loss ratio

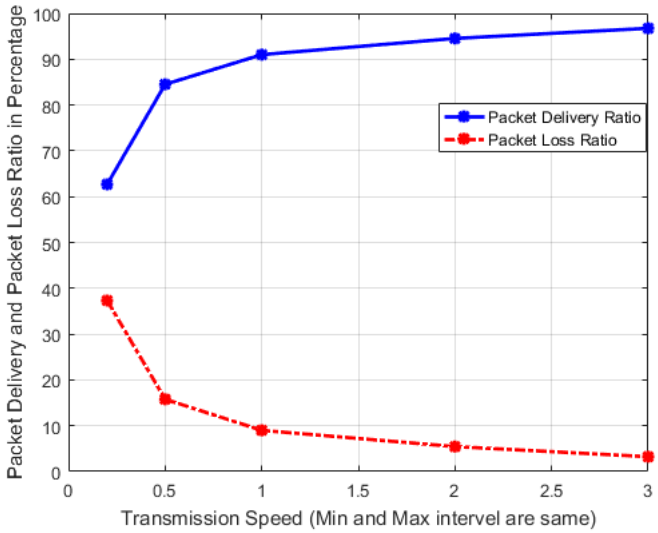

Fig. 7. Impact of moving speed of nodes on packet delivery and packet loss ratio

NE is also related to Wait Time (WT) that affect DR and PL.

$$\text{NE} = C5/\text{WT} \tag{8}$$

$$\mathrm{DR} = C6/\mathrm{WT} \tag{9}$$

$$\mathrm{PL} = C7 * \mathrm{WT} \tag{10}$$

Where C5, C6 and C7 are constants. Figs 8, 9, 10, 11 and 12 shows impact of wait time on packet delivery and packet loss with epidemic, First Contact, Direct Delivery, SprayAndWait and PROPHET respectively. Which is prove of the claims.

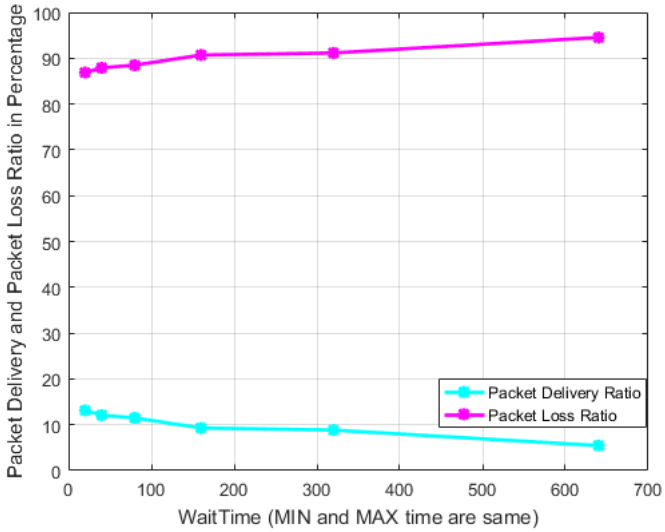

Fig. 8. Impact of wait time on packet delivery and packet loss with Epidemic

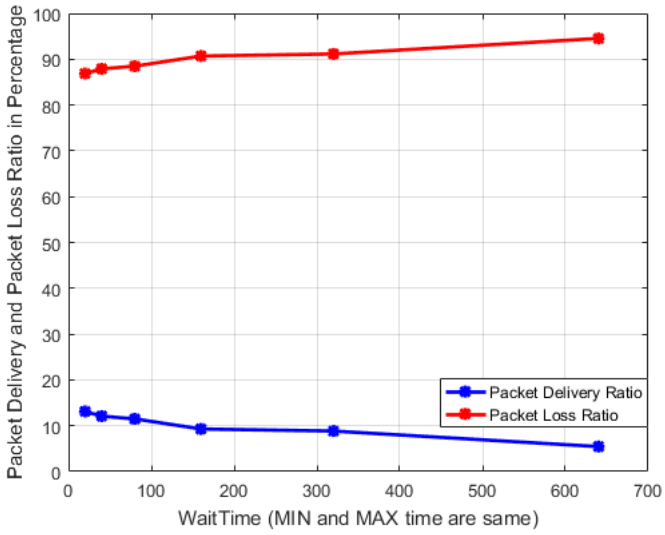

Fig. 9. Impact of wait time on packet delivery and packet loss with First Contact

Fig 13 shows the impact of WT on NE in Epidemic routing. For illustration, this article only shows performance of Epidemic routing, and all other routing protocols discussed earlier show same type results. It is clear from results that WT is increased with the decrease in NE. This ultimately leads to decreased packet delivery ratio and increased Packet loss ratio.

As mentioned earlier in this article AP is directly related to algorithm design (time and space complexity) and node Buffer Size (BS).

$$\mathrm{AP} = (\mathrm{AD} * \mathrm{BS})\mathrm{K3} \tag{11}$$

Where K3 is a constant of proportionality that depends on connectivity.

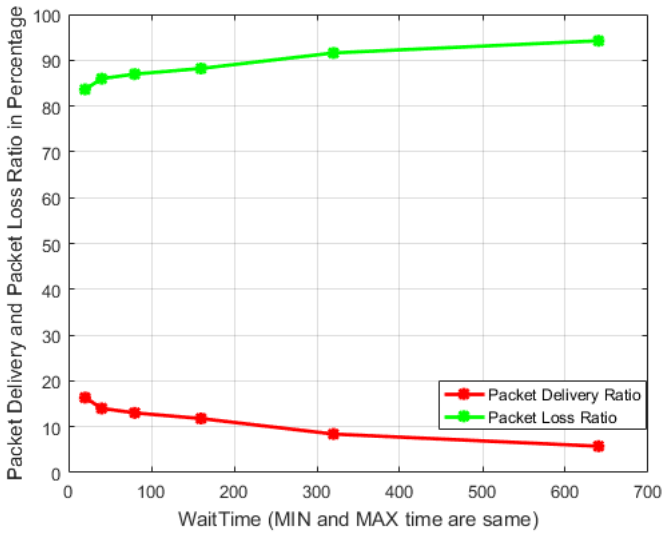

Fig. 10. Impact of wait time on packet delivery and packet loss with Direct Delivery

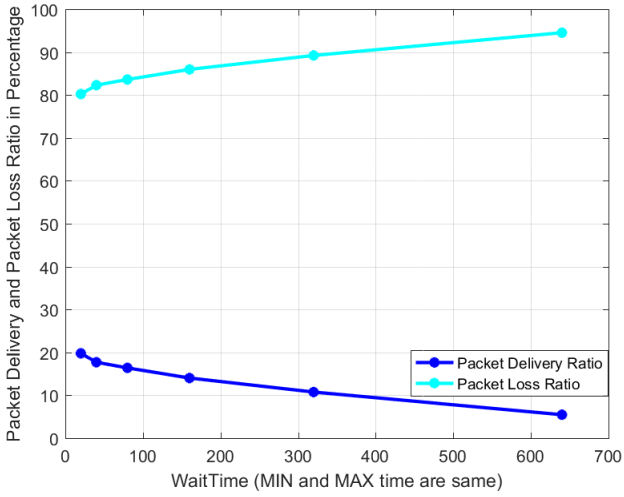

Fig. 11. Impact of wait time on packet delivery and packet loss with SprayAndWait

According to Eq. 11 AP directly depends on AD, BS and K3, where K3 is connectivity constant. If there is no connectivity, K3 becomes zero, so Performance $= 0$. Algorithm with minimum time and space complexity gives better performance. But on the other hand, the performance also depends on node buffer size. In order to calculate performance, put Eq. 11 in Eq. 2, we get

$$\text{Performance-A} = (\text{AD} * \text{BS} * \text{K1} * \text{K3})/\text{BC} \tag{12}$$

Eq. 12 clearly shows that performance directly depends on AD, BS, K1, and K3. Performance will be zero if one of the constant becomes zero. Moreover, BC has a indirect impact on performance. Too large value can degrade the performance, while with small value the performance will increase by keeping other parameters constant. By putting the value of Eq. 3 in Eq. 12, we get

$$\text{Performance-A} = (\text{AD} * \text{K1} * \text{K3} * (\text{DR} * \text{K2})/\text{PL})/\text{BC} \tag{13}$$

Eq. 13 shows that performance is not only directly related to DR, but proportional to the ratio of K2 times DR to PL. This result in high delivery and low packet loss ratios.

The performance also depends on Detection Accuracy (DA). This is related to Inter-Contact Time (ICT) and Number of Nodes (NNodes) in a network. The DA is inversely related to ICT (nodes that meet after long time) and directly proportional to NNodes [133]. Consider an attack scenario based on rate limit and encounter system, misbehaving nodes are not detected until other nodes meet. If nodes meet frequently, this means short ICT and result in high detection probability otherwise low.

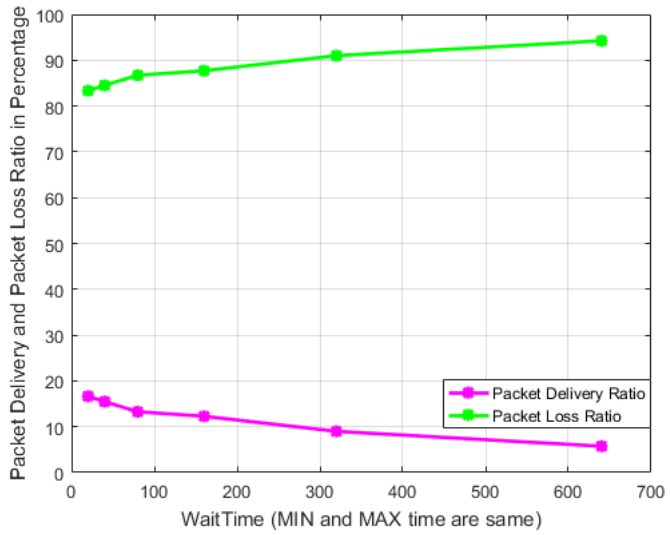

Fig. 12. Impact of wait time on packet delivery and packet loss with PROPHET

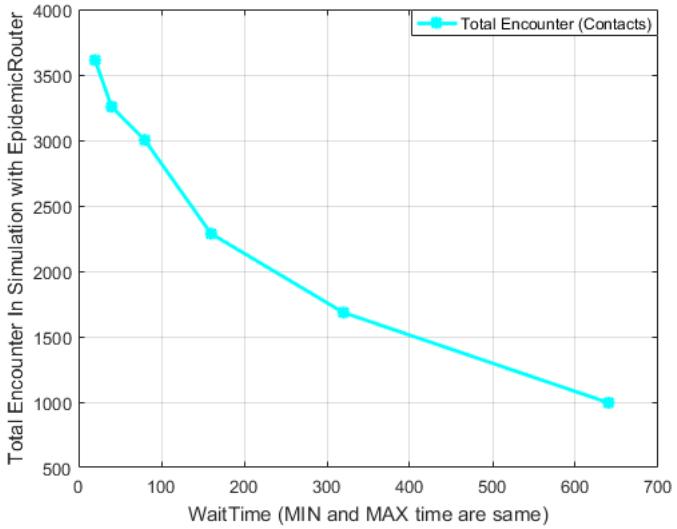

Fig. 13. Impact of wait time on number of Encounter (Contacts)

However, if the ratio of NNodes is high, then detection probability is high by keeping other parameters constant. We define the Detection Accuracy (DA)

$$\mathrm{DA} = \mathrm{K4}(\mathrm{NNodes}/\mathrm{ICT}) \tag{14}$$

Where K4 is a constant of proportionality depending on mobility strategy and scenario. As mentioned earlier that performance is directly related to DA and it depends on other factors as well which are previously discussed.

$$\text{Performance-B} = \mathrm{K5} * \mathrm{DA} \tag{15}$$

Where K5 is a constant which depends on other factors mentioned earlier. Putting the value of Eq. 14 in Eq. 15 we get

$$\text{Performance-B} = \mathrm{K5} * \mathrm{K4}(\mathrm{NNodes}/\mathrm{ICT}) \tag{16}$$

Eq. 16 shows that performance is directly related to NNodes and inversely related to ICT. If the number of malicious nodes are high, so detection probability will be high. Moreover, if ICT is short so detection probability is high, and results in high performance.

As already discussed, the performance of detection algorithms depends on cost as well. According to Eq. 1, Cost is equal to the sum of Processing Cost and Extra Node Cost. Some of the previously discussed proposed algorithms are costly due to processing and extra node for detection [135], [160], [185].

$$\text{Performance-C} = 1/(\text{K6} * \text{Cost}) \tag{17}$$

where K6 is constant. By keeping all other parameters constant put Eq. 1 in Eq. 17 we get

$$\text{Performance-C} = 1/(\text{K6}(\text{Processing Cost} + \text{Extra Node Cost})) \tag{18}$$

Eq. 18 shows inverse relationship. As mentioned earlier in this article Some proposed algorithms used extra node for detection such as Watch-Dog and Guard-Node. In Some proposed algorithms, extra node move along packets. On the other hand processing cost is also important parameter for performance evaluation. Some proposed algorithms use simple methods to detect misbehaving node while others used complex methods. For example, rate limit based scheme only make P-claim and T-claim and forward along with a packet, then cross check the packet which is computational overhead. Merkle-hash tree based scheme calculate hash and append with a packet, receiver side verify hash value. In some proposed schemes, reputation is calculated while few used encounter history. Node shares encounter history with other and all receiving nodes verify it. Battery usage of some algorithms is high. Based on these observations, every scheme have various processing cost. If cost is low, performance will be good. However, in literature researchers do not show processing cost in simulation graph, which is very difficult to predict. That is why measurement of processing cost is out of the scope of this article.

VII. Use Cases

As a use case impact of flood attacks i.e. SSSD, SSMD, MSSD and MSMD (which is already define an attacks Taxonomy in section II of this article), on packet delivery and packet loss ratios is evaluated.

A. Simulation Setup

The simulation is performed using ONE [197] simulator with parameters summarized in Table VII. We consider two scenarios for each approach: Epidemic With Normal nodes (EN), Epidemic With Malicious nodes (EM), First Contact With Normal nodes (FN), First Contact With Malicious nodes (FM), Direct Delivery With Normal nodes (DN), Direct Delivery With Malicious nodes (DM), SprayAndWait With Normal nodes (SN) and SprayAndWait With Malicious node (SM). The ratio of message creation between malicious and normal node is 4:1. The simulation takes one legitimate node and one malicious node in case of SSSD; one malicious and four legitimate nodes in case of SSMD; four malicious and one legitimate nodes in case of MSSD; four malicious and eight legitimate nodes in case of MSMD.

TABLE VII
Simulation Parameters list

Parameter	Assign Value	Parameter	Assign Value
Movement Model	RandomWayPoint	***TTL***	300
Area	500*500	***Group***	2
Buffer Size	5 MB	***Wait Time***	0, 120
Bandwidth	2 Mbs	***Update intervel***	0.1
Nodes	Mobile	***Router***	Epidemic
Moving speed	1, 1.6	***Router***	First Contact
Transmit Range	10 M	***Router***	SprayAndWait
Simulation Time	50000	***Router***	Direct Delivery

Packet Delivery Ratio (PDR): It is the ratio between delivered packets to total created Packets.

$$\text{PDR} = \text{Delivered Packets (DP)}/\text{Total Created Packets (CP)} \tag{19}$$

Packet Loss Ratio (PLR): It is the number of packets drop during communication.

$$\text{PLR} = (\text{CP} - \text{DP})/\text{CP} \tag{20}$$

This article took percent value of PDR and PLR. Add Eq. 19 with Eq. 20 we get.

$$\text{PDR} + \text{PLR} = (\text{DP}/\text{CP}) + (\text{CP} - \text{DP})/\text{CP} \tag{21}$$

$$\text{PDR} + \text{PLR} = (\text{DP} + \text{CP} - \text{DP})/\text{CP} \tag{22}$$

$$\text{PDR} + \text{PLR} = 1 \tag{23}$$

Eq. 23 implies the Sum of PDR and PLR is always be 1. This also imply that sum of percent value of PDR and PLR always be 100.

Buffer Consumption: It is the total buffer consumed in simulation. Buffer Consumption (BC), Total Buffer (TB) and Unused Buffer (UB)

$$\text{BC} = (\text{TB - UB}) \tag{24}$$

B. Use Case 1

This concerns when malicious nodes only forward packets and legitimate node only receive packets. Result shows that due to flood attacks, the packet delivery ratio is decreased and packet loss ratio is increased under evaluated routing protocol. Fig 14 shows packet delivery and packet loss ratios of SSSD, SSMD, MSSD and MSMD attacks, which is already defined in attacks Taxonomy Section II of this article. where results show that almost 29 percent of packet delivery ratio is decreased and packet loss ratio is increased in SSSD flood attacks. Moreover, SSSD attacks have almost same effect on all routing protocols.

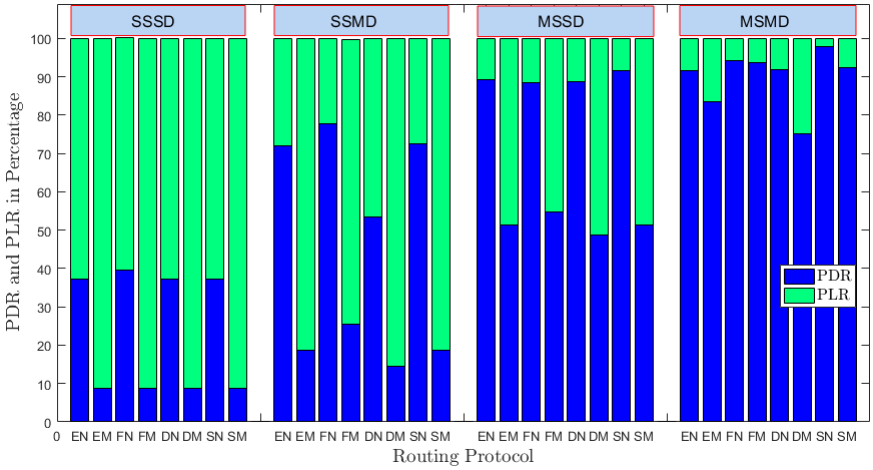

Fig. 14. Impact of Malicious node on PDR and PLR

Simulation results of SSMD flood attacks shows that due to flood attacks, 39 to 54 percent packet delivery ratio is decreased, and packet loss ratio is increased. According to results, Epidemic, First Contact and SprayAndWait shows Similar results, which is more than SSSD attacks. Because single target multiple nodes, which consumed resources of multiple nodes. Direct Delivery protocol is less effected because it deliver packet directly to destination, which consumed less buffer. It is very clear from simulation graph that in case of epidemic and SprayAndWait approximately 53 percent decreased in packet delivery ratio. Simulation graph shows that in case of First contact delivery ratio is decreased almost 52 percent. Simulation graph of direct delivery shows approximately 39 percent decreased in packet delivery ratios and increased in packet loss ratios, when malicious nodes launches attacks.

Simulation results of MSSD flood attacks show that flood attacks has 33 to 40 percent decreased in packet delivery and loss ratios. Which is less than SSMD and more than SSSD. Because in this type of attacks multiple source target one node, which consumed the resources of that single node. The effect of MSSD flood attacks is almost the same in all discussed routing protocols except First Contact which is 33 percent.

It is very clear from simulation graph that packet delivery ratio is decreased and packet loss ratios is increased in case of MSMD flood attacks. Simulation graph shows that there are approximately 1 to 16 percent decreased in packet delivery ratio. Simulation results of First Contact shows negligible effect of flood attacks on packet delivery ratio and packet loss ratios.

Due to flood attacks, the buffer is consumed and ultimately causes packet delivery ratio and packet loss ratio problems. This article simulates all mentioned above attacks to calculate buffer consumption in case of flood attacks. Every node have 5M buffer initially. For illustration purpose, this article calculates buffer consumption on specific time of the simulation that is 4100 seconds. This article test multiple routing protocol, However it shows approximately similar results. That is why for illustration this article simulates buffer consumption for Epidemic Router. Fig 15 show simulation results of used buffer space in case of SSSD, SSMD, MSSD and MSSD. The horizontal side of the graph represents different nodes, and the vertical side represents the used buffer in Bytes. In horizontal side node are given specific id. That is S0, S1, S2, S3, R1, R2, R3, R4, R5, R6, R7 and R8.

Simulation result of SSSD shows that there are clear buffer consumption when malicious nodes launches attacks. Simulation results shows that extra buffer consumption (Buffer Consumption Under Flood Attacks - Buffer Consumption without Flood Attacks) due to attack of one node is almost 3100000 and other node is 2820000 bytes.

Simulation results of SSMD shows that there are buffer consumption in the range of 1.9 to 3.2 MB when malicious node launches flood attacks. Extra buffer consumption of nodes is 300000, 1960000, 2600000, 2300000, and 3020000 bytes due to attack. Due to this buffer consumption packet delivery ratio is decreased and packet loss ratio is increased.

Simulation results of MSSD shows that extra buffer consumption of nodes in range of 1.8 to 3.4 MB approximately. In case of attack extra buffer consumption of nodes in MSSD is 2680000, 324000, 3040000, 2920000 and 1840000 bytes.

Simulation results shows that there are buffer consumption in case of MSMD as well, when malicious nodes launches flood attacks. It is clear from simulation graph that there are extra buffer consumption in MSMD are 120000, 2000000, -

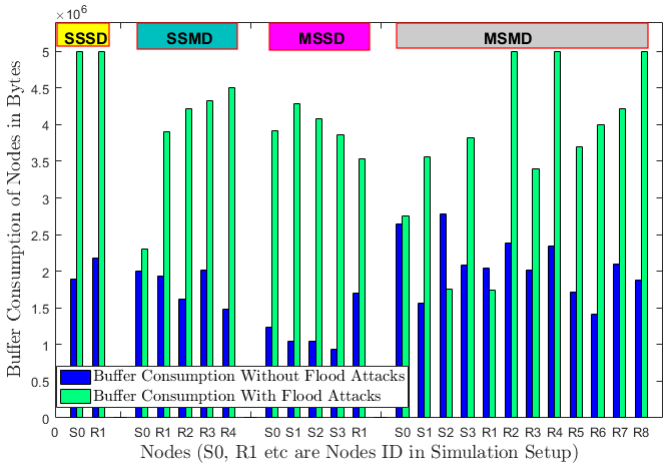

Fig. 15. Impact of Flood attacks on Buffer Consumption

1020000, 1740000, -300000, 2620000, 1380000, 2660000 1980000, 2580000, 2120000 and 3120000 bytes approximately of various nodes. Buffer consumption are less in this case relative to other attacks. Because in this case number of node are more than other attacks. Which imply buffer consumption are less relative to other. It is clear from simulation graph that S2 and R1 consumed less buffer (negative value means under flood attacks extra buffer consumption is smaller than extra buffer consumption without flood attacks.) under flood attacks. This is because of the fact, nodes are mobile in DTNs. Buffer consumption is minimum due to less encounter in simulation (Number of Encounter of R1 is minimum in this case). If number of encounter is minimum so it will consumed minimum buffer. Which is already prove in mathematical section of this article that is why buffer consumption of R1 is negative (If we subtract greater value from smaller it gives negative number). Also S2 are malicious forwarder which forward more packets to other nodes, which down innocent nodes. That is why innocent nodes are not able to forward messages to S2, so extra buffer consumption of S2 is minimum under flood attacks which is shown by negative sign with bytes.

C. Use Case 2

When malicious and legitimate nodes receive and forward packets at the same time, Fig 16 show packet delivery and packet loss ratios of SSSD, SSMD, MSSD and MSMD. Simulation results of all protocol shows almost same results. It is very clear from simulation results that there are approximately 31 percent packet delivery ratio is decreased and packet loss ratio is increased.

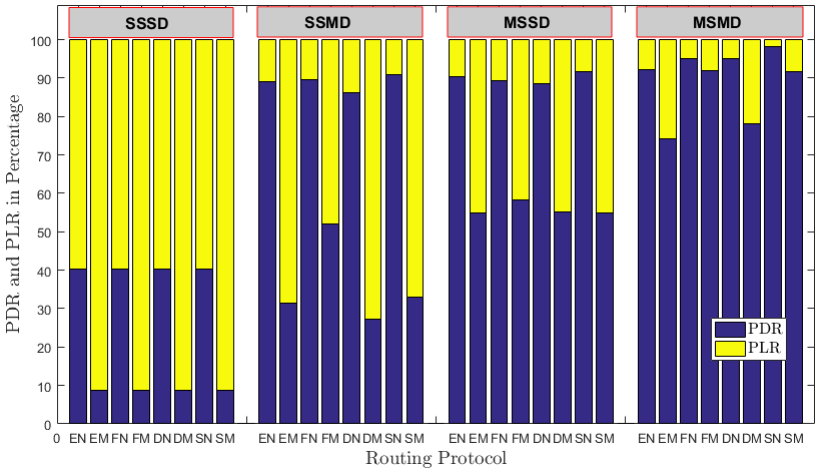

Fig. 16. Impact of Malicious node on PDR and PLR

In SSMD flood attacks, packet delivery ratios is decreased when malicious nodes launches flood attacks. It is very clear from simulation graph that in Direct Delivery almost 58 percent decreased in packet delivery ratio and packet loss ratio. Simulation graph of Epidemic and SprayAndWait shows that there are almost 57 percent decreased in packet delivery ratio and packet

loss ratio, when malicious nodes are deployed. Simulation results of First Contact shows that there are 37 percent decreased in packet delivery ratio when malicious nodes launches flood attacks.

In case of MSSD flood attacks, it is very clear from all the graph of simulation that due to malicious nodes packet delivery ratio is decreased and packet loss ratio is increased. Simulation result shows that in case of Epidemic, Direct Delivery and SprayAndWait packet delivery ratio is decreased 33 to 36 percent approximately. Simulation graph shows that in case of First Contact packet delivery ratio is decreased 31 percent.

Quantitative analysis of MSMD shows that there are approximately 17 percent decreased in packet delivery ratios, when Epidemic and Direct Delivery routing protocol are used. It is clear from the graph of First Contact and SprayAndWait that there are almost 3 to 6 percent decreased in packet delivery ratios when malicious nodes launches flood attacks.

Summary of Simulation Results:

This article take 2 cases with 4 different strategy to launch flood attacks and shows its impact on PDR, PLR and buffer consumption. Simulation is carried out on Epidemic, First Contact, SprayAndWait, Prophet and Direct Delivery. Simulation results shows all the protocol are effected due to flood attacks. From above results this article concluded that packet delivery ratio is decreased and packet loss ratio is increased when malicious nodes launches attacks. Delivery ratio of First Contact are less effected and Epidemic are mostly effected due to malicious nodes attacks. This is because of Epidemic forward more packet which consumed more buffer and First Contact only forward message to one node. Which consumed less buffer. Direct Delivery are also less effected like First Contact because it forward packet directly to destination, which consumed less buffer. Researchers proposed Epidemic and SprayAndWait for improvement in delivery ratio and packet loss ratio. However, in case of malicious nodes presence, Epidemic and SprayAndWait are mostly effected. Because Epidemic forward more packet to all its surrounding nodes, which consumed more buffer. Like Epidemic SprayAndWait Spray packets then wait for certain time which also consumed more buffer of nodes. Which ultimately cause packet delivery ratios are decreased in presence of malicious nodes. For normal situation when there is no malicious nodes Epidemic and SprayAndWait are best for best packet delivery ratios. However, in case of malicious nodes presence Epidemic and SprayAndWait are worst choice. Unlike Epidemic and SprayAndWait First contact forward message to only First contacted node. And Direct Delivery forward directly to destination. Which inherently stop number of messages. That is why buffer are less consumed which enhance packet delivery ratios and packet loss ratios.

Simulation results of use Case 1 and use Case 2 shows that delivery ratio is a little bit high in case of use Case 2. Because in use Case 2 malicious node send and receive packets at same time. Packet delivery ratios of use Case 2 is improve due to malicious node also receive packet which is added in delivery ratios.

VIII. Open Research Issues

The following are the open research issues in the broad area of security in DTNs, and misbehaving nodes particularly.

A. Detection Time

The proposed algorithms in literature that detect malicious node, normally suffered from delays and long duration in the detection. Rate limit based algorithms detect malicious nodes with cross checking strategies. However, due to frequent disconnection, the encounter of nodes will take significant time, and thus consume resources that ultimately causes packet delivery and packet loss ratio problems. As rate limit based algorithms and encounter based algorithms share history information, this takes long time to detect malicious nodes. Therefore, efficient detection time is an open research issue. Moreover, most of the rate limit based detection algorithms have not been with the ability to detect the colluding attacks.

B. Trade-off Between Centralized and Distributed Manners

Guard Node Based Detection is not suitable for DTNs environment, as all traffic will pass through central node. In Mobile Guard Node Based Detection, only one mobile guard node will allow every packets to pass through. As such, there is a need to see the trade-off between centralized and distributed based detection solutions.

C. Personalized Based Reputation Detection

Reputation based detection is also not very suitable like guard node based detection. This is because in former, there are two choices to calculate reputation of nodes i.e. by TA or from Acknowledgment. Both type of detection need end-to-end connectivity, and therefore Personalized Reputation based detection is an open issue.

D. Third Party Trusted Platform

In the credit based detection, either source or destination node gives credit. This process also incurs complex calculation, and causes overused battery and other resources. Moreover, both models may be biased in some use cases. Therefore, trusted third party platform is required to overcome the issue of misuse of trust, and also save energy resources of node for calculation.

E. Insider Attack

The proposed work in literature deployed detection scheme in Bundle Security Protocol. This deployment stops outside attacks but to provides prevention from insider attacker nodes. Therefore, it is important issue to design algorithms that provide safeguard against inside attacker nodes.

F. Extra Information

Some of detection solutions forward extra information along with packets to detect and mitigate attacker nodes, e.g., rate limit based detection forwards packet claim along with packet, and encounter based detection forwards history information. Merkle hash tree based detection forwards hashes along with packets. These extra information consume buffer and bandwidth, and thus causes degrades delivery ratio and packet loss ratio.

IX. Conclusion and Future Work

This article focused on misbehaving nodes in DTNs that launch various attacks and degrade network performance. The misbehaving nodes whether are malicious or selfish, often launch various attacks that mainly drop legitimate packets or inject fake packets to disrupt the network operations. We surveyed a large number of recent publications, and accomplished a comparison, given the characteristics of the reviewed detection algorithms based on our taxonomy. We further concluded performance analysis that misbehaving nodes launch attacks to decrease packet delivery ratio and throughput, increase packet loss ratio, overuse scarce resources, create nodes unavailability and disseminate bogus packets. Based on the study of this article we concluded that Rate limit and Encounter based Algorithms are best relative to other in flood mitigation, Due to its suitability in DTNs. Because Rate limit based and Encounter based algorithms have TA, easily deployed in DTNs and Distributed (In which more than one node is responsible for detection, unlike Centralized based algorithm in which one node is responsible for detection). In Centralized based algorithms false positive and false negative ratio are high relative to Distributed algorithms. Reputation based algorithms are not bad choice in mitigation of packet drop attacks. Credit based algorithms have more false positive and false negative ratio due to Message-Purse-Model and Message-Trade-Model. This article proposed TA-Trad-Model which possibly overcomes the above issues. Watch-Dog and Gate-Way-Node based schemes are not suitable in DTNs. Merkle-hash-Tree based schemes are best choice for mitigation of Fake packet attacks, if some modification are applied in existing algorithms. Protocol based algorithms are cheapest solution for mitigation of Flood attacks with modification for internal malicious nodes detection as well. We further concluded from the simulation results of use cases, that Epidemic and SprayAndWait are not good choice in presence of malicious nodes. First Contact forward less number of packets relative to Epidemic and SprayAndWait. First Contact algorithm do not allowed malicious nodes (Algorithm create barrier for node to forward more packets. Algorithm only allowed forward packet to first contacted node.) to forward large number of packets. Which ultimately consumed less buffer relative to Epidemic and SprayAndWait, which enhanced packet delivery ratio and packet loss ratio. So in presence of malicious node First Contact is best choice for packet delivery ratios. We hope this article would further motivate the research interest in security related topics in DTNs, and accordingly highlight the following directions for future investigations:

1) Hybrid, efficient and distributed algorithms to detect and mitigate flood, packet drop and fake packet attacks.
2) Scalable assumptions of constants terms in analysis to find relationship between parameters in addition to buffer and bandwidth consumption.
3) Preventive based algorithm to thwart malicious nodes, that overuse limited resources.
4) Detection of malicious packet rather than malicious nodes.

References

[1] K. Fall, "A delay-tolerant network architecture for challenged internets," in *Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications*. ACM, 2003, pp. 27–34.
[2] K. Fall, K. L. Scott, S. C. Burleigh, L. Torgerson, A. J. Hooke, H. S. Weiss, R. C. Durst, and V. Cerf, "Delay-tolerant networking architecture," 2007.
[3] T. V. Spyropoulos, *Delay tolerant networks: Protocols and applications*. CRC press, 2011.
[4] F. Esposito and I. Matta, "Preda: Predicate routing for dtn architectures over manet," in *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE*. IEEE, 2009, pp. 1–6.
[5] J. Dhivya and M. Vanithalakshmi, "A survey of backpressure based scheduling algorithms for delay tolerant networks," in *Information Communication and Embedded Systems (ICICES), 2014 International Conference on*. IEEE, 2014, pp. 1–5.
[6] J.-H. Cho and R. Chen, "Provest: Provenance-based trust model for delay tolerant networks," *IEEE Transactions on Dependable and Secure Computing*, 2016.
[7] M. J. Khabbaz, C. M. Assi, and W. F. Fawaz, "Disruption-tolerant networking: A comprehensive survey on recent developments and persisting challenges," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 2, pp. 607–640, 2012.
[8] S. Burleigh, A. Hooke, L. Torgerson, K. Fall, V. Cerf, B. Durst, K. Scott, and H. Weiss, "Delay-tolerant networking: an approach to interplanetary internet," *IEEE Communications Magazine*, vol. 41, no. 6, pp. 128–136, 2003.
[9] Y. Guo, S. Schildt, T. Pogel, and L. Wolf, "Detecting malicious behavior in a vehicular dtn for public transportation," in *Global Information Infrastructure Symposium, 2013*. IEEE, 2013, pp. 1–8.
[10] J. Partan, J. Kurose, and B. N. Levine, "A survey of practical issues in underwater networks," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 11, no. 4, pp. 23–33, 2007.

[11] P. Asuquo, H. Cruickshank, Z. Sun, and G. Chandrasekaran, "Analysis of dos attacks in delay tolerant networks for emergency evacuation," in *Next Generation Mobile Applications, Services and Technologies, 2015 9th International Conference on*. IEEE, 2015, pp. 228–233.

[12] S. Guo, M. H. Falaki, E. A. Oliver, S. Ur Rahman, A. Seth, M. A. Zaharia, and S. Keshav, "Very low-cost internet access using kiosknet," *ACM SIGCOMM Computer Communication Review*, vol. 37, no. 5, pp. 95–100, 2007.

[13] C. Velásquez-Villada and Y. Donoso, "Delay/disruption tolerant networks based message forwarding algorithm for rural internet connectivity applications," in *Computers Communications and Control (ICCCC), 2016 6th International Conference on*. IEEE, 2016, pp. 16–22.

[14] P. Juang, H. Oki, Y. Wang, M. Martonosi, L. S. Peh, and D. Rubenstein, "Energy-efficient computing for wildlife tracking: Design tradeoffs and early experiences with zebranet," in *ACM Sigplan Notices*, vol. 37, no. 10. ACM, 2002, pp. 96–107.

[15] S. E. Loudari, M. Benamar, and N. Benamar, "New classification of nodes cooperation in delay tolerant networks," in *Advances in Ubiquitous Networking*. Springer, 2016, pp. 301–309.

[16] K. L. Scott and S. Burleigh, "Bundle protocol specification," 2007.

[17] W. Narongkhachavana, T. Choksatid, and S. Prabhavat, "An efficient message flooding scheme in delay-tolerant networks," in *Information Technology and Electrical Engineering (ICITEE), 2015 7th International Conference on*. IEEE, 2015, pp. 295–299.

[18] S.-C. Lo, M.-H. Chiang, J.-H. Liou, and J.-S. Gao, "Routing and buffering strategies in delay-tolerant networks: Survey and evaluation," in *Parallel Processing Workshops (ICPPW), 2011 40th International Conference on*. IEEE, 2011, pp. 91–100.

[19] K. Urunov, J.-I. Namgung, and S.-H. Park, "Security challenges of dtn mechanism for iout," *International Journal of Information and Electronics Engineering*, vol. 5, no. 5, p. 330, 2015.

[20] V. Mahendran, S. K. Anirudh, and C. S. R. Murthy, "A realistic framework for delay-tolerant network routing in open terrains with continuous churn," in *International Conference on Distributed Computing and Networking*. Springer, 2011, pp. 407–417.

[21] R. Di Pietro, S. Guarino, N. V. Verde, and J. Domingo-Ferrer, "Security in wireless ad-hoc networks–a survey," *Computer Communications*, vol. 51, pp. 1–20, 2014.

[22] L. Wood, W. M. Eddy, and P. Holliday, "A bundle of problems," in *Aerospace conference, 2009 IEEE*. IEEE, 2009, pp. 1–17.

[23] K. Fall and S. Farrell, "Dtn: an architectural retrospective," *IEEE Journal on Selected areas in communications*, vol. 26, no. 5, 2008.

[24] S. Raut, "A survey based on secure data retrieval in disruption tolerant network," *International Journal of Research in Computer Engineering & Electronics*, vol. 4, no. 6, 2016.

[25] T. Small and Z. J. Haas, "Resource and performance tradeoffs in delay-tolerant wireless networks," in *Proceedings of the 2005 ACM SIGCOMM workshop on Delay-tolerant networking*. ACM, 2005, pp. 260–267.

[26] P. Puri and M. P. Singh, "A survey paper on routing in delay-tolerant networks," in *Information Systems and Computer Networks (ISCON), 2013 International Conference on*. IEEE, 2013, pp. 215–220.

[27] B. Patel, K. Dave, and V. Pandya, "Delay tolerant network," *International Journal of Emerging Technology and Advanced Engineering*, 2013.

[28] S. Jain, K. Fall, and R. Patra, *Routing in a delay tolerant network*. ACM, 2004, vol. 34, no. 4.

[29] S. Farrell, S. Symington, H. Weiss, and P. Lovell, "Delay-tolerant networking security overview," *IRTF, draft-irtf-dtnrg-sec-overview*, vol. 6, 2009.

[30] Z. Lu and J. Fan, "Delay/disruption tolerant network and its application in military communications," in *Computer design and applications (ICCDA), 2010 international conference on*, vol. 5. IEEE, 2010, pp. V5–231.

[31] A. Kate, G. M. Zaverucha, and U. Hengartner, "Anonymity and security in delay tolerant networks," in *Security and Privacy in Communications Networks and the Workshops, 2007. SecureComm 2007. Third International Conference on*. IEEE, 2007, pp. 504–513.

[32] G. Rajan and G. Cho, "Applying a security architecture with key management framework to the delay/disruption tolerant networks," *International Journal of Security and Its Applications*, vol. 9, no. 4, pp. 327–336, 2015.

[33] W. L. Van Besien, "Dynamic, non-interactive key management for the bundle protocol," in *Proceedings of the 5th ACM workshop on Challenged networks*. ACM, 2010, pp. 75–78.

[34] S. A. Menesidou and V. Katos, "Authenticated key exchange (ake) in delay tolerant networks," in *IFIP International Information Security Conference*. Springer, 2012, pp. 49–60.

[35] M. Pitkanen, A. Keranen, and J. Ott, "Message fragmentation in opportunistic dtns," in *World of Wireless, Mobile and Multimedia Networks, 2008. WoWMoM 2008. 2008 International Symposium on a*. IEEE, 2008, pp. 1–7.

[36] N. Asokan, K. Kostiainen, P. Ginzboorg, J. Ott, and C. Luo, "Towards securing disruption-tolerant networking," *Nokia Research Center, Tech. Rep. NRC-TR-2007-007*, 2007.

[37] J. Miao, O. Hasan, S. B. Mokhtar, L. Brunie, and A. Hasan, "4pr: Privacy preserving routing in mobile delay tolerant networks," *Computer Networks*, vol. 111, pp. 17–28, 2016.

[38] J. Zhou, X. Dong, Z. Cao, and A. V. Vasilakos, "Secure and privacy preserving protocol for cloud-based vehicular dtns," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 6, pp. 1299–1314, 2015.

[39] C. P. A. Ogah, H. Cruickshank, Z. Sun, G. Chandrasekaran, Y. Cao, P. M. Asuquo, and M. Al Tawqi, "Privacy-enhanced group communication for vehicular delay tolerant networks," in *Next Generation Mobile Applications, Services and Technologies, 2015 9th International Conference on*. IEEE, 2015, pp. 193–198.

[40] D. Tang and J. Ren, "A novel delay-aware and privacy-preserving data-forwarding scheme for urban sensing network," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 4, pp. 2578–2588, 2016.

[41] N. Ahmad, H. Cruickshank, Z. Sun, and M. Asif, "Pseudonymised communication in delay tolerant networks," in *Privacy, Security and Trust (PST), 2011 Ninth Annual International Conference on*. IEEE, 2011, pp. 1–6.

[42] Q. Li and G. Cao, "Mitigating routing misbehavior in disruption tolerant networks," *IEEE transactions on information forensics and security*, vol. 7, no. 2, pp. 664–675, 2012.

[43] Y. Cao and Z. Sun, "Routing in delay/disruption tolerant networks: A taxonomy, survey and challenges," *IEEE Communications surveys & tutorials*, vol. 15, no. 2, pp. 654–677, 2013.

[44] Y. Cao, Z. Sun, N. Wang, M. Riaz, H. Cruickshank, and X. Liu, "Geographic-based spray-and-relay (gsar): an efficient routing scheme for dtns," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 4, pp. 1548–1564, 2015.

[45] Y. Cao, Z. Sun, H. Cruickshank, and F. Yao, "Approach-and-roam (aar): a geographic routing scheme for delay/disruption tolerant networks," *IEEE transactions on Vehicular Technology*, vol. 63, no. 1, pp. 266–281, 2014.

[46] S. Srinivasa and S. Krishnamurthy, "Crest: An opportunistic forwarding protocol based on conditional residual time," in *Sensor, Mesh and Ad Hoc Communications and Networks, 2009. SECON'09. 6th Annual IEEE Communications Society Conference on*. IEEE, 2009, pp. 1–9.

[47] E. C. De Oliveira and C. V. De Albuquerque, "Nectar: a dtn routing protocol based on neighborhood contact history," in *Proceedings of the 2009 ACM symposium on Applied Computing*. ACM, 2009, pp. 40–46.

[48] T. Li, C. Dong, and G. Chen, "Ccqr: Constant cost quality-based routing protocol in delay tolerant networks," in *Parallel and Distributed Systems (ICPADS), 2009 15th International Conference on*. IEEE, 2009, pp. 190–197.

[49] E. Bulut, Z. Wang, and B. K. Szymanski, "Cost efficient erasure coding based routing in delay tolerant networks," in *Communications (ICC), 2010 IEEE International Conference on*. IEEE, 2010, pp. 1–5.

[50] G. Sandulescu and S. Nadjm-Tehrani, "Opportunistic dtn routing with window-aware adaptive replication," in *Proceedings of the 4th Asian Conference on Internet Engineering*. ACM, 2008, pp. 103–112.

[51] L. Yin, Y. Cao, and W. He, "Similarity degree-based mobility pattern aware routing in dtns," in *Intelligent Ubiquitous Computing and Education, 2009 International Symposium on*. IEEE, 2009, pp. 345–348.

[52] S. Ahmed and S. S. Kanhere, "A bayesian routing framework for delay tolerant networks," in *Wireless Communications and Networking Conference (WCNC), 2010 IEEE*. IEEE, 2010, pp. 1–6.

[53] T. Spyropoulos, K. Psounis, and C. S. Raghavendra, "Spray and wait: an efficient routing scheme for intermittently connected mobile networks," in *Proceedings of the 2005 ACM SIGCOMM workshop on Delay-tolerant networking*. ACM, 2005, pp. 252–259.

[54] ——, "Spray and focus: Efficient mobility-assisted routing for heterogeneous and correlated mobility," in *Pervasive Computing and Communications Workshops, 2007. PerCom Workshops' 07. Fifth Annual IEEE International Conference on*. IEEE, 2007, pp. 79–85.

[55] F. Li, J. Wu, and A. Srinivasan, "Thwarting blackhole attacks in disruption-tolerant networks using encounter tickets," in *INFOCOM 2009, IEEE*. IEEE, 2009, pp. 2428–2436.

[56] Y. Ren, M. C. Chuah, J. Yang, and Y. Chen, "Muton: Detecting malicious nodes in disruption-tolerant networks," in *Wireless Communications and Networking Conference (WCNC), 2010 IEEE*. IEEE, 2010, pp. 1–6.

[57] T. N. D. Pham and C. K. Yeo, "Detecting colluding blackhole and greyhole attacks in delay tolerant networks," *IEEE Transactions on Mobile Computing*, vol. 15, no. 5, pp. 1116–1129, 2016.

[58] Y. Ren, M. C. Chuah, J. Yang, and Y. Chen, "Detecting wormhole attacks in delay-tolerant networks [security and privacy in emerging wireless networks]," *IEEE Wireless communications*, vol. 17, no. 5, 2010.

[59] H. Guo, X. Wang, H. Cheng, and M. Huang, "A routing defense mechanism using evolutionary game theory for delay tolerant networks," *Applied Soft Computing*, vol. 38, pp. 469–476, 2016.

[60] M. T. Scholar, S. GORAKHPUR, and I. C. Choubey, "A survey on malicious nodes in mobile ad hoc network," *Journal of Network Communications and Emerging Technologies (JNCET) www. jncet. org*, vol. 6, no. 3, 2016.

[61] S. Saha, S. Nandi, R. Verma, S. Sengupta, K. Singh, V. Sinha, and S. K. Das, "Design of efficient lightweight strategies to combat dos attack in delay tolerant network routing," *Wireless Networks*, pp. 1–22, 2016.

[62] W. Li, L. Galluccio, M. Kieffer, and F. Bassi, "Distributed faulty node detection in dtns," in *Computer Communication and Networks (ICCCN), 2016 25th International Conference on*. IEEE, 2016, pp. 1–9.

[63] W. Li, L. Galluccio, F. Bassi, and M. Kieffer, "Distributed faulty node detection in delay tolerant networks: Design and analysis," 2016.

[64] S. Zakhary and M. Radenkovic, "Erasure coding with replication to defend against malicious attacks in dtn," in *Wireless and Mobile Computing, Networking and Communications (WiMob), 2011 IEEE 7th International Conference on*. IEEE, 2011, pp. 357–364.

[65] B. Pooja, M. M. Pai, R. M. Pai, N. Ajam, and J. Mouzna, "Mitigation of insider and outsider dos attack against signature based authentication in vanets," in *Computer Aided System Engineering (APCASE), 2014 Asia-Pacific Conference on*. IEEE, 2014, pp. 152–157.

[66] U. Khan, S. Agrawal, and S. Silakari, "A detailed survey on misbehavior node detection techniques in vehicular ad hoc networks," in *Information Systems Design and Intelligent Applications*. Springer, 2015, pp. 11–19.

[67] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on vanet security challenges and possible cryptographic solutions," *Vehicular Communications*, vol. 1, no. 2, pp. 53–66, 2014.

[68] W. Li and H. Song, "Art: An attack-resistant trust management scheme for securing vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 4, pp. 960–969, 2016.

[69] M. Arshad, Z. Ullah, N. Ahmad, M. Khalid, H. Cruickshank, and Y. Cao, "A survey of local/cooperative based malicious information detection techniques in vanets," *EURASIP Journal on Wireless Communications and Networking (EURASIP JWCN)*, 2018.

[70] S. M. Benazir and V. Umarani, "Detection of selfish & malicious behavior using dtn-chord monitoring in mobile networks," in *Information Communication and Embedded Systems (ICICES), 2016 International Conference on*. IEEE, 2016, pp. 1–5.

[71] H.-C. Lee, S.-M. Cheng, K.-P. Wu, and H.-M. Lee, "A responsive probing approach to detect dynamic intrusion in a manet," in *Information, Intelligence, Systems & Applications (IISA), 2016 7th International Conference on*. IEEE, 2016, pp. 1–6.

[72] D. Djenouri, L. Khelladi, and N. Badache, "A survey of security issues in mobile ad hoc networks," *IEEE communications surveys*, vol. 7, no. 4, pp. 2–28, 2005.

[73] A. Babakhouya, Y. Challal, and A. Bouabdallah, "A simulation analysis of routing misbehaviour in mobile ad hoc networks," in *Next Generation Mobile Applications, Services and Technologies, 2008. NGMAST'08. The Second International Conference on*. IEEE, 2008, pp. 592–597.

[74] H. Dai, H. Liu, Z. Jia, and T. Chen, "A multivariate classification algorithm for malicious node detection in large-scale wsns," in *Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on*. IEEE, 2012, pp. 239–245.

[75] S. U. Maheswari, N. Usha, E. M. Anita, and K. R. Devi, "A novel robust routing protocol raeed to avoid dos attacks in wsn," in *Information Communication and Embedded Systems (ICICES), 2016 International Conference on*. IEEE, 2016, pp. 1–5.

[76] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," *Ad hoc networks*, vol. 1, no. 2, pp. 293–315, 2003.

[77] M. Raza, N. Aslam, H. Le-Minh, S. Hussain, Y. Cao, and N. M. Khan, "A critical analysis of research potential, challenges and future directives in industrial wireless sensor networks," *IEEE Communications Surveys & Tutorials*, 2017.

[78] V. Gupta and D. Sangroha, "Protection against packet drop attack," in *Advances in Engineering and Technology Research (ICAETR), 2014 International Conference on*. IEEE, 2014, pp. 1–4.

[79] A. T. Mizrak, Y.-C. Cheng, K. Marzullo, and S. Savage, "Detecting and isolating malicious routers," *IEEE Transactions on Dependable and Secure Computing*, vol. 3, no. 3, pp. 230–244, 2006.

[80] C. Li, J. Yang, Z. Wang, F. Li, and Y. Yang, "A lightweight ddos flooding attack detection algorithm based on synchronous long flows," in *Global Communications Conference (GLOBECOM), 2015 IEEE*. IEEE, 2015, pp. 1–6.

[81] F. Cadet and D. T. Fokum, "Coping with denial-of-service attacks on the ip telephony system," in *SoutheastCon, 2016*. IEEE, 2016, pp. 1–7.

[82] J. Mirkovic, S. Dietrich, D. Dittrich, and P. Reiher, "Internet denial of service: Attack and defense mechanisms (radia perlman computer networking and security)," 2004.

[83] N. Ilyas, M. Akbar, R. Ullah, M. Khalid, A. Arif, A. Hafeez, U. Qasim, Z. A. Khan, and N. Javaid, "Sedg: Scalable and efficient data gathering routing protocol for underwater wsns," *Procedia Computer Science*, vol. 52, pp. 584–591, 2015.

[84] M. Khalid, Z. Ullah, N. Ahmad, M. Arshad, B. Jan, Y. Cao, and A. Adnan, "A survey of routing issues and associated protocols in underwater wireless sensor networks," *Journal of Sensors*, p. 7539751, 2017.

[85] M. Khalid, Z. Ullah, N. Ahmad, H. Khan, H. S. Cruickshank, and O. U. Khan, "A comparative simulation based analysis of location based routing protocols in underwater wireless sensor networks," in *Recent Trends in Telecommunications Research (RTTR), Workshop on*. IEEE, 2017, pp. 1–5.

[86] M. Khalid, Z. Ullah, N. Ahmad, A. Adnan, W. Khalid, and A. Ashfaq, "Comparison of localization free routing protocols in underwater wireless sensor networks," *INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS*, vol. 8, no. 3, pp. 408–414, 2017.

[87] Y. Wu, Y. Zhao, M. Riguidel, G. Wang, and P. Yi, "Security and trust management in opportunistic networks: a survey," *Security and Communication Networks*, vol. 8, no. 9, pp. 1812–1827, 2015.

[88] S. Djahel, F. Nait-Abdesselam, and Z. Zhang, "Mitigating packet dropping problem in mobile ad hoc networks: proposals and challenges," *IEEE communications surveys & tutorials*, vol. 13, no. 4, pp. 658–672, 2011.

[89] N. Magaia, P. R. Pereira, and M. P. Correia, "Selfish and malicious behavior in delay-tolerant networks," in *Future Network and Mobile Summit (FutureNetworkSummit), 2013*. IEEE, 2013, pp. 1–10.

[90] J. Miao, O. Hasan, S. B. Mokhtar, L. Brunie, and K. Yim, "An investigation on the unwillingness of nodes to participate in mobile delay tolerant network routing," *International Journal of Information Management*, vol. 33, no. 2, pp. 252–262, 2013.

[91] J. Solis, N. Asokan, K. Kostiainen, P. Ginzboorg, and J. Ott, "Controlling resource hogs in mobile delay-tolerant networks," *Computer Communications*, vol. 33, no. 1, pp. 2–10, 2010.

[92] N. Li and S. K. Das, "A trust-based framework for data forwarding in opportunistic networks," *Ad Hoc Networks*, vol. 11, no. 4, pp. 1497–1509, 2013.

[93] B. M. Silva, J. J. Rodrigues, I. M. Lopes, T. M. Machado, and L. Zhou, "A novel cooperation strategy for mobile health applications," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 28–36, 2013.

[94] S. Misra, S. Pal, and B. K. Saha, "Cooperation in delay tolerant networks," in *Next-Generation Wireless Technologies*. Springer, 2013, pp. 15–35.

[95] Y. Wu, S. Deng, and H. Huang, "On modeling the impact of selfish behaviors on limited epidemic routing in delay tolerant networks," *Wireless personal communications*, vol. 71, no. 4, pp. 2759–2782, 2013.

[96] H. Chen and W. Lou, "Making nodes cooperative: A secure incentive mechanism for message forwarding in dtns," in *Computer Communications and Networks (ICCCN), 2013 22nd International Conference on*. IEEE, 2013, pp. 1–7.

[97] K. Devi and P. Damodharan, "Detecting misbehavior routing and attacks in disruption tolerant network using itrm," in *Current Trends in Engineering and Technology (ICCTET), 2013 International Conference on*. IEEE, 2013, pp. 334–337.

[98] G. Bigwood and T. Henderson, "Incentive-aware opportunistic network routing," in *Routing in Opportunistic Networks*. Springer, 2013, pp. 383–401.

[99] R. Chen, F. Bao, M. Chang, and J.-H. Cho, "Dynamic trust management for delay tolerant networks and its application to secure routing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 5, pp. 1200–1210, 2014.

[100] N. Magaia, P. R. Pereira, and M. P. Correia, "Nodes' misbehavior in vehicular delay-tolerant networks," in *Future Internet Communications (CFIC), 2013 Conference on*. IEEE, 2013, pp. 1–9.

[101] A. K. Gupta, J. K. Mandal, and I. Bhattacharya, "Mitigating selfish, blackhole and wormhole attacks in dtn in a secure, cooperative way," *International Journal of Information and Computer Security*, vol. 9, no. 1-2, pp. 130–155, 2017.

[102] C. Chakrabarti, "An incentive driven reliable message exchange scheme in post-disaster situation using delay tolerant network," *CSI transactions on ICT*, vol. 5, no. 1, pp. 27–34, 2017.

[103] H. Abubakar, A. Tekanyi, and S. Sani, "Node cooperation strategy on security aided and group encounter prophet routing protocol of an opportunistic network," *International Journal of Computer Applications*, vol. 163, no. 8, 2017.

[104] S. Yasmin, A. Qayyum, and R. N. B. Rais, "Cooperation in opportunistic networks: An overlay approach for destination-dependent utility-based schemes," *Arabian Journal for Science and Engineering*, vol. 42, no. 2, pp. 467–482, 2017.

[105] W. Li, F. Bassi, M. Kieffer, A. Calisti, G. Pasolini, and D. Dardari, "Distributed faulty node detection in dtns in presence of byzantine attack," in *IEEE International Conference on Communications*, 2017, pp. 1–6.

[106] E. DAMIANI, "Addressing selfishness in the design of cooperative systems," Ph.D. dissertation, Politecnico di Milano, Italy, 2017.

[107] R. Skowronski, "Fully distributed gridnet protocol, with no trusted authorities," in *Information Networking (ICOIN), 2017 International Conference on*. IEEE, 2017, pp. 569–574.

[108] W. Li, L. Galluccio, F. Bassi, and M. Kieffer, "Distributed faulty node detection in delay tolerant networks: Design and analysis," 2017.

[109] A. Kumar, S. K. Dhurandher, I. Woungang, M. S. Obaidat, S. Gupta, and J. J. Rodrigues, "An altruism-based trust-dependent message forwarding protocol for opportunistic networks," *International Journal of Communication Systems*, vol. 30, no. 10, 2017.

[110] S. K. Dhurandher, A. Kumar, and M. S. Obaidat, "Cryptography-based misbehavior detection and trust control mechanism for opportunistic network systems," *IEEE Systems Journal*, 2017.

[111] X. Wang, Y. Lin, Y. Zhao, L. Zhang, J. Liang, and Z. Cai, "A novel approach for inhibiting misinformation propagation in human mobile opportunistic networks," *Peer-to-Peer Networking and Applications*, vol. 10, no. 2, pp. 377–394, 2017.

[112] K.-S. Wong, T.-C. Wan, and W.-C. Ang, "A survey on current status of disruption tolerant network support for multicast," in *Computer and Information Sciences (ICCOINS), 2016 3rd International Conference on*. IEEE, 2016, pp. 276–281.

[113] T. Le and M. Gerla, "A security framework for content retrieval in dtns," in *Wireless Communications and Mobile Computing Conference (IWCMC), 2016 International*. IEEE, 2016, pp. 7–12.

[114] X. Wang, Y. Lin, Y. Zhao, L. Zhang, J. Liang, and Z. Cai, "A novel approach for inhibiting misinformation propagation in human mobile opportunistic networks," *Peer-to-Peer Networking and Applications*, vol. 10, no. 2, pp. 377–394, 2017.

[115] A. Morelli, M. Tortonesi, C. Stefanelli, and N. Suri, "Information-centric networking in next-generation communications scenarios," *Journal of Network and Computer Applications*, vol. 80, pp. 232–250, 2017.

[116] D. Bucur and G. Iacca, "Improved search methods for assessing delay-tolerant networks vulnerability to colluding strong heterogeneous attacks," *Expert Systems with Applications*, vol. 80, pp. 311–322, 2017.

[117] M. C. Nimje and P. Junghare, "Detection of node activity, selfish & malicious behavioral patterns using exwatchdog algorithm," *International Journal of Engineering Science*, vol. 5676, 2017.

[118] D. Wu, F. Zhang, H. Wang, and R. Wang, "Security-oriented opportunistic data forwarding in mobile social networks," *Future Generation Computer Systems*, 2017.

[119] C. Chakrabarti, "An incentive driven reliable message exchange scheme in post-disaster situation using delay tolerant network," *CSI transactions on ICT*, vol. 5, no. 1, pp. 27–34, 2017.

[120] W. Li, F. Bassi, M. Kieffer, A. Calisti, G. Pasolini, and D. Dardari, "Distributed faulty node detection in dtns in presence of byzantine attack," in *IEEE International Conference on Communications*, 2017, pp. 1–6.

[121] J. F. Naves and I. M. Moraes, "Mitigating the ack counterfeiting attack in delay and disruption tolerant networks," in *Computers and Communications (ISCC), 2017 IEEE Symposium on*. IEEE, 2017, pp. 1015–1020.

[122] D. Bucur, G. Iacca, M. Gaudesi, G. Squillero, and A. Tonda, "Optimizing groups of colluding strong attackers in mobile urban communication networks with evolutionary algorithms," *Applied Soft Computing*, vol. 40, pp. 416–426, 2016.

[123] R. Chen, F. Bao, M. Chang, and J.-H. Cho, "Dynamic trust management for delay tolerant networks and its application to secure routing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 5, pp. 1200–1210, 2014.

[124] H. Zhu, S. Du, Z. Gao, M. Dong, and Z. Cao, "A probabilistic misbehavior detection scheme toward efficient trust establishment in delay-tolerant networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 1, pp. 22–32, 2014.

[125] S. Yasmin, "Cost-effective routing & cooperative framework for opportunistic networks," Ph.D. dissertation, Capital University, 2016.

[126] P. Nagrath and A. Kumar, "Analysis of malicious activity in delay tolerant networks," in *Innovation and Challenges in Cyber Security (ICICCS-INBUSH), 2016 International Conference on*. IEEE, 2016, pp. 17–20.

[127] S. Jain, "Black hole attack in delay tolerant networks: A survey," *International Journal of Computer Science and Engineering*, vol. 2, no. 4, pp. 172–175, 2014.

[128] I. Saranya and L. Shinny, "Preserving flood attack on delay tolerant network," 2014.

[129] I. Parris and T. Henderson, "Friend or flood? social prevention of flooding attacks in mobile opportunistic networks," in *Distributed Computing Systems Workshops (ICDCSW), 2014 IEEE 34th International Conference on*. IEEE, 2014, pp. 16–21.

[130] F. C. Choo, M. C. Chan, and E.-C. Chang, "Robustness of dtn against routing attacks," in *Communication Systems and Networks (COMSNETS), 2010 Second International Conference on*. IEEE, 2010, pp. 1–10.

[131] P. T. N. Diep and C. K. Yeo, "Detecting flooding attack while accommodating burst traffic in delay tolerant networks," in *Wireless Telecommunications Symposium (WTS), 2017*. IEEE, 2017, pp. 1–7.

[132] T. N. D. Pham, C. K. Yeo, N. Yanai, and T. Fujiwara, "Detecting flooding attack and accommodating burst traffic in delay-tolerant networks," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 1, pp. 795–808, 2018.

[133] Q. Li, W. Gao, S. Zhu, 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, pp. 168–182, 2013.

[134] P. Nagrath, S. Aneja, and G. Purohit, "Flooding attack in delay tolerant network."

[135] V. Natarajan, Y. Yang, and S. Zhu, "Resource-misuse attack detection in delay-tolerant networks," in *Performance Computing and Communications Conference (IPCCC), 2011 IEEE 30th International*. IEEE, 2011, pp. 1–8.

[136] F. C. Lee, W. Goh, and C. K. Yeo, "A queuing mechanism to alleviate flooding attacks in probabilistic delay tolerant networks," in *Telecommunications (AICT), 2010 Sixth Advanced International Conference on*. IEEE, 2010, pp. 329–334.

[137] A. Lindgren, A. Doria, and O. Schelén, "Probabilistic routing in intermittently connected networks," *ACM SIGMOBILE mobile computing and communications review*, vol. 7, no. 3, pp. 19–20, 2003.

[138] C. Balamurugan, M. Viswanathan, T. A. Kumar, and G. Raj, "Detection of flood attacks in dtn using rate limiter technique," *Journal of Computer Science*, vol. 10, no. 7, p. 1216, 2014.

[139] S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (ddos) flooding attacks," *IEEE communications surveys & tutorials*, vol. 15, no. 4, pp. 2046–2069, 2013.

[140] Y. Guo, S. Schildt, T. Po, S. Rottmann, L. Wolf *et al.*, "Mitigating blackhole attacks in a hybrid vdtn," in *A World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2014 IEEE 15th International Symposium on*. IEEE, 2014, pp. 1–6.

[141] J. A. Dias, J. J. Rodrigues, and L. Zhou, "Performance evaluation of cooperative strategies for vehicular delay-tolerant networks," *Transactions on Emerging Telecommunications Technologies*, vol. 25, no. 8, pp. 815–822, 2014.

[142] P. Asuquo, H. Cruickshank, C. P. A. Ogah, A. Lei, and K. Olutomilayo, "A mobility-aware trust management scheme for emergency communication networks using dtn," in *International Conference on Wireless and Satellite Systems*. Springer, 2016, pp. 130–141.

[143] H. Chen, W. Lou, Z. Wang, and Q. Wang, "A secure credit-based incentive mechanism for message forwarding in noncooperative dtns," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 8, pp. 6377–6388, 2016.

[144] S. Misra, B. K. Saha, and S. Pal, "Enforcing cooperation in omns," in *Opportunistic Mobile Networks*. Springer, 2016, pp. 191–221.

[145] N. Dang and X. Bai, "Content delivery mechanism in delay tolerant network," in *Software Engineering and Service Science (ICSESS), 2016 7th IEEE International Conference on*. IEEE, 2016, pp. 493–496.

[146] M. Alajeely, R. Doss, and A. Ahmad, "Security and trust in opportunistic networks–a survey," *IETE Technical Review*, vol. 33, no. 3, pp. 256–268, 2016.

[147] Y. Cai, Y. Fan, and D. Wen, "An incentive-compatible routing protocol for two-hop delay-tolerant networks," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 1, pp. 266–277, 2016.

[148] S. Yasmin, A. Qayyum, and R. N. B. Rais, "Cooperation in opportunistic networks: An overlay approach for destination-dependent utility-based schemes," *Arabian Journal for Science and Engineering*, vol. 42, no. 2, pp. 467–482, 2017.

[149] Z. Su, Q. Xu, K. Zhang, and X. S. Shen, "Modeling of epidemic information dissemination for msns," in *Modeling and Optimization for Mobile Social Networks*. Springer, 2016, pp. 19–40.

[150] C. Sobin, V. Raychoudhury, G. Marfia, and A. Singla, "A survey of routing and data dissemination in delay tolerant networks," *Journal of Network and Computer Applications*, vol. 67, pp. 128–146, 2016.

[151] A. Sharma, D. Singh, P. Sharma, and S. Dhawan, "Selfish nodes detection in delay tolerant networks," in *Futuristic Trends on Computational Analysis and Knowledge Management (ABLAZE), 2015 International Conference on*. IEEE, 2015, pp. 407–410.

[152] L. Wei, Z. Cao, and H. Zhu, "Mobigame: A user-centric reputation based incentive protocol for delay/disruption tolerant networks," in *Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE*. IEEE, 2011, pp. 1–5.

[153] P. Hui, E. Yoneki, S. Y. Chan, and J. Crowcroft, "Distributed community detection in delay tolerant networks," in *Proceedings of 2nd ACM/IEEE international workshop on Mobility in the evolving internet architecture*. ACM, 2007, p. 7.

[154] K. Devi and P. Damodharan, "Detecting misbehavior routing and attacks in disruption tolerant network using itrm," in *Current Trends in Engineering and Technology (ICCTET), 2013 International Conference on*. IEEE, 2013, pp. 334–337.

[155] A. Baadache and A. Belmehdi, "Fighting against packet dropping misbehavior in multi-hop wireless ad hoc networks," *Journal of Network and Computer Applications*, vol. 35, no. 3, pp. 1130–1139, 2012.

[156] J. A. Dias, J. J. Rodrigues, F. Xia, and C. X. Mavromoustakis, "A cooperative watchdog system to detect misbehavior nodes in vehicular delay-tolerant networks," *IEEE Transactions on Industrial Electronics*, vol. 62, no. 12, pp. 7929–7937, 2015.

[157] M. Y. S. Uddin, B. Godfrey, and T. Abdelzaher, "Relics: In-network realization of incentives to combat selfishness in dtns," in *Network protocols (ICNP), 2010 18th IEEE international conference on*. IEEE, 2010, pp. 203–212.

[158] J. A. Dias, J. J. Rodrigues, and L. Zhou, "Cooperation advances on vehicular communications: A survey," *Vehicular communications*, vol. 1, no. 1, pp. 22–32, 2014.

[159] E. Ayday and F. Fekri, "An iterative algorithm for trust management and adversary detection for delay-tolerant networks," *IEEE Transactions on Mobile Computing*, vol. 11, no. 9, pp. 1514–1531, 2012.

[160] H. Zhu, X. Lin, R. Lu, Y. Fan, and X. Shen, "Smart: A secure multilayer credit-based incentive scheme for delay-tolerant networks," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 8, pp. 4628–4639, 2009.

[161] S. E. Loudari, M. Benamar, and N. Benamar, "New classification of nodes cooperation in delay tolerant networks."

[162] L. Liu, "A survey on barter-based incentive mechanism in opportunistic networks," in *Instrumentation and Measurement, Sensor Network and Automation (IMSNA), 2013 2nd International Symposium on*. IEEE, 2013, pp. 365–367.

[163] L. Buttyán, L. Dóra, M. Félegyházi, and I. Vajda, "Barter trade improves message delivery in opportunistic networks," *Ad Hoc Networks*, vol. 8, no. 1, pp. 1–14, 2010.

[164] U. Shevade, H. H. Song, L. Qiu, and Y. Zhang, "Incentive-aware routing in dtns," in *Network Protocols, 2008. ICNP 2008. IEEE International Conference on*. IEEE, 2008, pp. 238–247.

[165] F. Wu, T. Chen, S. Zhong, C. Qiao, and G. Chen, "A bargaining-based approach for incentive-compatible message forwarding in opportunistic networks," in *Communications (ICC), 2012 IEEE International Conference on*. IEEE, 2012, pp. 789–793.

[166] J. Buchmann, E. Dahmen, and M. Schneider, "Merkle tree traversal revisited," in *International Workshop on Post-Quantum Cryptography*. Springer, 2008, pp. 63–78.

[167] M. Alajeely, R. Doss, V. Mak-Hau *et al.*, "Catabolism attack and anabolism defense: A novel attack and traceback mechanism in opportunistic networks," *Computer Communications*, vol. 71, pp. 111–118, 2015.

[168] M. Alajeely, R. Doss *et al.*, "Establishing trust relationships in oppnets using merkle trees," in *Communication Systems and Networks (COMSNETS), 2016 8th International Conference on*. IEEE, 2016, pp. 1–6.

[169] ——, "Malicious node traceback in opportunistic networks using merkle trees," in *Data Science and Data Intensive Systems (DSDIS), 2015 IEEE International Conference on*. IEEE, 2015, pp. 147–152.

[170] R. Mitchell and R. Chen, "A survey of intrusion detection in wireless network applications," *Computer Communications*, vol. 42, pp. 1–23, 2014.

[171] D. D. Hepsiba and S. Prabhu, "Enhanced techniques to strengthening dtn against flood attacks," in *Information Communication and Embedded Systems (ICICES), 2014 International Conference on*. IEEE, 2014, pp. 1–4.

[172] S. B. Lavanya, S. G. Devi, M. A. Mary, and M. M. E. Dyana, "Deducing malicious attacks in disruption tolerant networks," *Indian Journal of Emerging Electronics in Computer Communications-IJEECC*, vol. 1, no. 1, pp. 110–115, 2014.

[173] R. EZHILARASAN and R. RAMESHKUMAR, "Protection and detection of flood attacks in disruption tolerant networks."

[174] G. Rani and K. S. Kumar, "Defending against flood attacks in disruption tolerant networks," 2014.
[175] V. Rathna, "Preserving data against flood attacks in disruption tolerant networks," 2015.
[176] A. J. Bassey and C. Fancy, "Mitigating flooding attacks in disruption tolerant network."
[177] K. Ramaraj, J. Vellingiri, C. Saravanabhavan, and A. Illayarajaa, "Denial of service flood attacks in disruption tolerant networks."
[178] G. Ansa, H. Criuckshank, Z. Sun, and M. Al-Siyabi, "A dos-resilient design for delay tolerant networks," in *Wireless Communications and Mobile Computing Conference (IWCMC), 2011 7th International*. IEEE, 2011, pp. 424–429.
[179] P. Nagrath, S. Aneja, and G. Purohit, "Defending flooding attack in delay tolerant networks," in *Information Networking (ICOIN), 2015 International Conference on*. IEEE, 2015, pp. 40–45.
[180] P. T. N. Diep and C. K. Yeo, "Detecting flooding attack in delay tolerant networks by piggybacking encounter records," in *Information Science and Security (ICISS), 2015 2nd International Conference on*. IEEE, 2015, pp. 1–4.
[181] D. Kuriakose and D. Daniel, "Effective defending against flood attack using stream-check method in tolerant network," in *Green Computing Communication and Electrical Engineering (ICGCCEE), 2014 International Conference on*. IEEE, 2014, pp. 1–4.
[182] Z. Gao, H. Zhu, S. Du, C. Xiao, and R. Lu, "Pmds: A probabilistic misbehavior detection scheme in dtn," in *Communications (ICC), 2012 IEEE International Conference on*. IEEE, 2012, pp. 4970–4974.
[183] C. Chakrabarti, A. Banerjee, and S. Roy, "An observer-based distributed scheme for selfish-node detection in a post-disaster communication environment using delay tolerant network," in *Applications and Innovations in Mobile Computing (AIMoC), 2014*. IEEE, 2014, pp. 151–156.
[184] C. Chakrabarti, S. Chakrabarti, and A. Banerjee, "A dynamic two hops reputation assignment scheme for selfish node detection and avoidance in delay tolerant network," in *Research in Computational Intelligence and Communication Networks (ICRCICN), 2015 IEEE International Conference on*. IEEE, 2015, pp. 345–350.
[185] H. Zhu, X. Lin, R. Lu, and X. Shen, "A secure incentive scheme for delay tolerant networks," in *Communications and Networking in China, 2008. ChinaCom 2008. Third International Conference on*. IEEE, 2008, pp. 23–28.
[186] A. A. Chandavale and T. P. Chaure, "An approach to detect malicious node for delay tolerant networks," in *TENCON 2015-2015 IEEE Region 10 Conference*. IEEE, 2015, pp. 1–6.
[187] M. Alajeely, R. Doss *et al.*, "Defense against packet dropping attacks in opportunistic networks," in *Advances in Computing, Communications and Informatics (ICACCI, 2014 International Conference on*. IEEE, 2014, pp. 1608–1613.
[188] L. Kulkarni, D. Mukhopadhyay, and J. Bakal, "Analyzing security schemes in delay tolerant networks," in *Proceedings of the International Conference on Data Engineering and Communication Technology*. Springer, 2017, pp. 613–620.
[189] R. Sharma and D. Gupta, "Effects of selfish node on routing protocols in delay tolerant network."
[190] M. Malathi and S. Jayashri, "Design and performance of dynamic trust management for secure routing protocol," in *Advances in Computer Applications (ICACA), IEEE International Conference on*. IEEE, 2016, pp. 121–124.
[191] R.-I. Ciobanu, C. Dobre, M. Dascalu, S. Trausan-Matu, and V. Cristea, "Collaborative selfish node detection with an incentive mechanism for opportunistic networks," in *Integrated Network Management (IM 2013), 2013 IFIP/IEEE International Symposium on*. IEEE, 2013, pp. 1161–1166.
[192] P. Asuquo, H. Cruickshank, C. P. A. Ogah, A. Lei, and Z. Sun, "A collaborative trust management scheme for emergency communication using delay tolerant networks," in *Advanced Satellite Multimedia Systems Conference and the 14th Signal Processing for Space Communications Workshop (ASMS/SPSC), 2016 8th*. IEEE, 2016, pp. 1–6.
[193] S. Basu and S. Roy, "A global reputation estimation and analysis technique for detection of malicious nodes in a post-disaster communication environment," in *Applications and Innovations in Mobile Computing (AIMoC), 2014*. IEEE, 2014, pp. 179–185.
[194] M. Alajeely, R. Doss, V. Mak-Hau *et al.*, "Packet faking attack: a novel attack and detection mechanism in oppnets," in *Computational Intelligence and Security (CIS), 2014 Tenth International Conference on*. IEEE, 2014, pp. 638–642.
[195] M. Alajeely, R. Doss *et al.*, "Reputation based malicious node detection in oppnets," in *Computer Science and Software Engineering (JCSSE), 2016 13th International Joint Conference on*. IEEE, 2016, pp. 1–6.
[196] M. Alajeely, R. Doss, V. Mak-Hau *et al.*, "Defense against packet collusion attacks in opportunistic networks," *Computers & Security*, vol. 65, pp. 269–282, 2017.
[197] A. Keränen, J. Ott, and T. Kärkkäinen, "The one simulator for dtn protocol evaluation," in *Proceedings of the 2nd international conference on simulation tools and techniques*. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2009, p. 55.
[198] C. Sobin, "An efficient buffer management policy for dtn," *Procedia Computer Science*, vol. 93, pp. 309–314, 2016.
[199] N. Bezirgiannidis and V. Tsaoussidis, "Packet size and dtn transport service: Evaluation on a dtn testbed," in *Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2010 International Congress on*. IEEE, 2010, pp. 1198–1205.