IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 13 June 2023, accepted 17 July 2023, date of publication 20 July 2023, date of current version 26 July 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3297439

SURVEY

Simulative Survey of Flooding Attacks in Intermittently Connected Vehicular Delay Tolerant Networks

WAQAR KHALID[1], NAVEED AHMED[2], (Member, IEEE), SULEMAN KHAN[3], (Member, IEEE), ZAHID ULLAH[4], AND YASIR JAVED[2], (Member, IEEE)

[1]School of Cyber Science and Engineering, Wuhan University, Wuhan 430000, China
[2]Department of Computer Science, Prince Sultan University, Riyadh 12435, Saudi Arabia
[3]School of Psychology and Computer Science, University of Central Lancashire, RR1 2HE Preston, U.K.
[4]Department of Computer Science, Institute of Management Sciences, Peshawar 25000, Pakistan

Corresponding author: Waqar Khalid (khalid.ping91@gmail.com)

The authors would like to acknowledge the support of Prince Sultan University for paying the Article Processing Charges (APC) of this publication. They would also like to thank Prince Sultan University for their support.

ABSTRACT Vehicular Adhoc Networks (VANETs) are an emerging and promising technology that enables vehicles to communicate with roadside units (RSUs) and other vehicles. VANETs contribute to improved traffic efficiency, accident safety, and entertainment services for passengers and drivers. However, VANETs face limitations in areas with intermittent connectivity. To address this scenario, researchers have proposed a specialized use-case known as intermittently-connected-vehicular delay-tolerant-networks (ICV-DTNs), which are a subset of delay-tolerant-networks (DTNs). Security is less explored area compare to routing. Malicious nodes pose significant threats by launching selective packet drops, fake/bogus packets, and flood attacks, depleting limited resources such as bandwidth and node buffer space. Consequently, these attacks result in low message delivery ratios and high message loss ratios. Among these attacks, flood attacks are particularly challenging in ICV-DTNs/Flying Adhoc Networks/Internet of Drones. Various algorithms have been proposed to mitigate flood attacks, but previous approaches have exhibited shortcomings. Firstly, previously proposed algorithms lack efficiency in terms of detection time and accuracy. Secondly, the extent of resource waste or savings after implementing these schemes has not been adequately demonstrated, with no simulation results quantifying the amount of buffer consumption. Additionally, prior algorithms lack a comprehensive definition of flood attacks, which represents a critical research question in this field. To address these gaps, this article not only proposed a unique taxonomy of the flooding attacks but also evaluate various algorithms on diverse parameters. The article also contribute open research areas for the community to investigate the nitty gritty of flooding attacks in ICV-DTNs.

INDEX TERMS Intermittently-connected-vehicular-delay-tolerant-network (ICV-DTNs), intermittently-connected-networks (ICNs), flood-attack, misbehaving-nodes, packets-delivery-ratios, packets-loss-ratios, delay-tolerant-networks (DTNs), resources-consumption.

I. INTRODUCTION

The world is turning into a global village because of communication networks. In recent decades, infrastructure and networks without infrastructure have enabled a wide range of communication devices to be linked over long geographical areas. However, there are certain regions that are not under the umbrella of networks. This lapse is because of the end-to-end connectivity [1], [2]. In most developing countries/areas, end-to-end communication networks are not available, and will not be in the foreseeable future. DTNs [3], [4] are potentially low-cost solution to the aforementioned problem.

DTNs are special sub-class of infrastructure-less networks which suffer from frequent disconnection and variable

The associate editor coordinating the review of this manuscript and approving it for publication was Giovanni Pau.

delay [5], [6]. Initially, DTNs were proposed for communication from one planet (Mars) to another planet (Earth), known as DeepSpaceCommunication (DSC)/InterplanetaryNetworks (IPNs) [7], however, also applicable for many ground-based applications, such as VehicularAdhocNetworks [8], [9], known as ICV-DTNs (The focus of this article on this use-case), UnderwaterWirelessSensorNetworks (UWSNs) [10], [11], Flying Adhoc Networks (FANETs)/Internet of Drones (IODs), and extreme conditions after natural disasters [12], [13]. Popular examples of DTNs are, DakNet [2], ZebraNet [14], WiderNet [15] and KioskNet [16].

There are various challenges in ICV-DTNs, such as variable delay, nodes disconnection, asymmetric-data-rates, and communication between heterogeneous networks [17], [18], [19]. To address the issues of ICV-DTNs, researchers proposed ''Bundles Protocol (BP)''. ''BP'' apply Store-Carry-Forward (SCF) method for forwarding bundles (usually it is unreliable, however, it also has an option of reliability, which is called custodian forwarding) [20]. Due to frequent disconnection, researchers proposed persistent memory for ICV-DTNs nodes, which store bundles in persistent storage until new contact(s) (encounter(s) new node) is available. Furthermore, it also has a convergence layer, which converts/translates a message to specific network architecture, which enables the exchange of data/information between two heterogeneous networks [21].

The aforementioned challenging issues (already mentioned in this article) breed new issues such as Reliability/Time-Synchronization [22], Spoof-Identity, Privacy [23], faulty nodes [24], Key-Distribution [25], Buffer-Management [26], Packet-Fragmentation [27] and Resources-Scarcity [28].

A. CHALLENGES/ISSUES OF INTERMITTENTLY CONNECTED NETWORKS

This section briefly discusses a few issues of intermittently connected networks (few of them are outlined already in this article).

1) PARTIAL NODES CONNECTIVITY

Connectivity is vital for any type of network, communication is impossible without connectivity [29]. In ICV-DTNs, nodes are partially connected, and this provoke problems such as high packet loss ratios (due to dis-connectivity), low packet delivery ratios (due to intermittent connectivity), security issues (malicious nodes are not detected because some of the previously proposed schemes detect various attacks when all nodes share encounter-history packets and rate-limit-certificate), key distribution (due to intermittent connectivity), and long variable delay, etc. Therefore, Partial connectivity is a very important issue in ICV-DTNs (open research problem).

2) NODES TRACKING

In vehicular networks, tracking of particular node is an important parameter for various operations. This includes routing of packets, tracking the position of various nodes, accurate/timely delivery of packets at the destination, and the detection of various malicious attacks [30], [31]. Few security attacks need tracking of vehicles to reduce false positive and false negative ratios. However, position tracking (position falsification attacks) is a challenging task due to the intermittent connectivity of nodes in ICV-DTNs. Therefore, according to the analyses of this article, node tracking is an important research problem of vehicular networks, that is an open research issue for researchers.

3) RELIABILITY/TRANSMISSION IMPAIRMENT (TI)

TI is a condition that causes data packets to be lost. If the transmission media were perfect, the destination nodes will receive the same bundles/packets that the sender/forwarder nodes send. However, this is not the case (both guided and wireless media are not perfect), the receiver does not receive the same packets as sent by the sender because of data loss, bit errors, or bit flip (change binary 0 to 1 or vice versa). This is because of attenuation, distortion, and noise. Traditional networks (TCP/IP) have a mechanism to detect and correct transmission bit errors. However, there is no such type of methodology available in bundle protocol [22], this ultimately creates reliability issue, which is an open research glitch for researchers in this field.

4) TIME SYNCHRONIZATION

Time Synchronization is an important metric for communication, particularly security. Few security attacks are easily mitigated/detected through time synchronization, such as ''Replay Attacks'', ''Worm-Hole Attacks''. A slight-drift in time synchronization creates big issues in networks (attacks are not detected). Researchers implemented time synchronization in traditional networks such as TCP/IP-based networks. However, the implementation of time synchronization in intermittently connected networks are very challenging because of the disconnected and sparse nature of nodes in networks [32]. Therefore, Time Synchronization is an important research problem for researchers to handle.

5) REASSEMBLING OF BUNDLES/PACKETS

Usually, the forwarder nodes forward multiple packets to the destination (the packets reach the destination at different times, due to the frequency of signal, speed of signal, distance between source and destination, and transmission path between sender and receiver). Traditional networks follow specific procedures, usually with packet sequence numbers to re-assemble the packets so the destination nodes can re-assemble the packets. However, there is no such type of mechanism in bundle protocol. Reassembling of bundles are very challenging task/issue in ICV-DTNs due to the long delay and partial nodes connectivity [33].

6) NODES MANAGEMENT IN NETWORKS

Nodes management is a critical issue in networks. Traditional networks follow some rules/procedures/protocols for the management of nodes in networks. However, according

to the studies of this article, there are no such rules/protocols in ICV-DTNs, that bread some new issues. Therefore, Nodes Management is an open research problem for researchers.

7) PACKET FRAGMENTATION

The division of packets/bundles into sub-packets/sub-bundles are known as packet fragmentation. There are two types of packets fragmentation in DTNs, proactive fragmentation and reactive fragmentation [27]. Reactive fragmentation creates some security issues [27], such as confidentiality and integrity of sub-bundles [34], [35]. Few researchers proposed the ''toilet paper '' [36] to handle confidentiality and integrity of sub-bundles. However, due to high processing powers and limited resources, the ''toilet paper'' is not an efficient solution. Therefore, reactive fragmentation is an open research problem in ICV-DTNs.

8) NETWORKS TRAFFIC/DATA MANAGEMENT

In VANETs, vehicles generate and process huge amount of data. The data management such as storing, retrieving, and processing are an important tasks for efficient/fair utilization of networks resources. However, the networks data management is not an easy task. Nonetheless, few researchers proposed an efficient schemes to handle this issue (machine learning, data mining, and big data analytics). However, this is still a challenging research problem in vehicular networks.

9) RESOURCES SCARCITY

The scarcity of resources are one of the most important issue of ICV-DTNs (which is already mentioned in this article). DTNs nodes have limited resources, such as buffer space, energy, processing power (outlined in this article). This issue creates some new issues such as various security attacks, energy consumption, and packet loss ratios/packet delivery ratios, etc [34]. Therefore it is an open research problem.

10) PACKETS ROUTING/PACKETS FORWARDING

The packets routing are also very important research question in ICV-DTNs. Designing an efficient routing protocols are very difficult in ICV-DTNs due to unique nature/characteristic of ICV-DTNs (open research issue in vehicular networks). Few researchers proposed various efficient routing protocols [5], [37] to handle issues of ICV-DTNs. Each routing algorithm has pros and cons (to the best of our knowledge no perfect solution have been proposed till date). Additionally, few proposed routing algorithms/protocols create some security issues. To the best of our knowledge, the security issues due to routing protocols have not been adequately addressed in the literature. Fig. 1 shows various challenges/issues of ICV-DTNs.

B. SECURITY CHALLENGES

The deployment of ICV-DTNs nodes under typical harsh conditions, nodes face numerous security challenges [38], [39], [40], [41], [42], [43], [44]. Bundle Security Protocols (BSPs) provide basic security services such as confidentiality, integrity, and authentication by including a particular security header in ''BPs''. There are four security headers in ''BSPs'' that enhance the security of ICV-DTNs. These are, Bundle Authentication Block (BAB), Payload Integrity Block (PIB), Payload Confidentiality Block (PCB) and Extension Security Block (ESB) [21], [45].

- Bundle Authentication Block:- BAB provides authentication hop-by-hop. Actually, BAB authenticates a bundle from one security-aware (SAN) node to another SAN which may be multiple nodes in the transmission path. BAB-HMAC is mandatory cipher- suite for BAB.
- Payload Integrity Block:- PIB provides integrity and authentication of a payload end-to-end, which ensures the authenticity and integrity of the payload. PIB-RSA-SHA256 is a mandatory cipher-suite for PIB.
- Payload Confidentiality Block:- PCB provides end-to-end confidentiality of a payload, which ensures that the bundle payload is confidential that is kept secret. PCB-RSA-AES128-PIB-PCB is mandatory cipher-suite for PCB.
- Extension Security Block:- ESB is use for non-payload blocks (not primary blocks and payload blocks). ESB-RSA-AES128 is a mandatory cipher-suite for ESB.

As outlined already in this article that BSPs provide some basic security services [45], [46] but due to the unique nature of DTNs, it is very challenging to achieve full security services. Also, due to the challenging nature of DTNs, nodes are vulnerable to various attacks. Such as ''BlackHoleAttack'' [47], ''WormHole'' [48], ''PacketDropsAttack'' [49], [50], ''FaultyNodeAttacks'' [51], [52], ''ColludingAttacks'' [53], ''FakePacketAttacks'' [54], [55], and ''DistributedDenialOfServices (DDOS)''/''FloodAttacks'' [56], [57], [58].

Misbehavior malicious and selfish nodes [44], [59], [60], [61] launch various attacks [62], [63] (already outlined in this article), flood attack is one of them. In this type of attacks, misbehavior nodes send/forward a large number of messages/packets, that overuse the meager resources of ICV-DTNs nodes [64], [65]. These limited resources includes, buffer-space [56], [57], [58], bandwidth, and energy resources of benign nodes [66], [67], [68]. Due to this attacks, ''PacketDeliveryRatios (PDRs)'' are decrease, while ''PacketLossRatios (PLRs)'' are increase. Moreover, resources consumption which includes ''TotalBufferConsumption (TBCs)'', ''TotalBandwidthConsumption (TBWCs)/''TotalWastedTransmission (TWTs)'', and ''TotalEnergyConsumption (TECs)'' are increase. Apart from this, nodes' unavailability issue also arises in the networks. Traditional routing protocols, detection/mitigation protocols for VANETs [9], [69], [70], UWSNs [71], [72], Internet [73], Autonomous-Vehicular-Networks [74], MobileAd-hocNetworks (MANETs) [75], and WirelessSensorNetworks (WSNs) [76], [77], [78] are cannot be applicable in ICV-DTNs, due to the unique nature of ICV-DTNs.

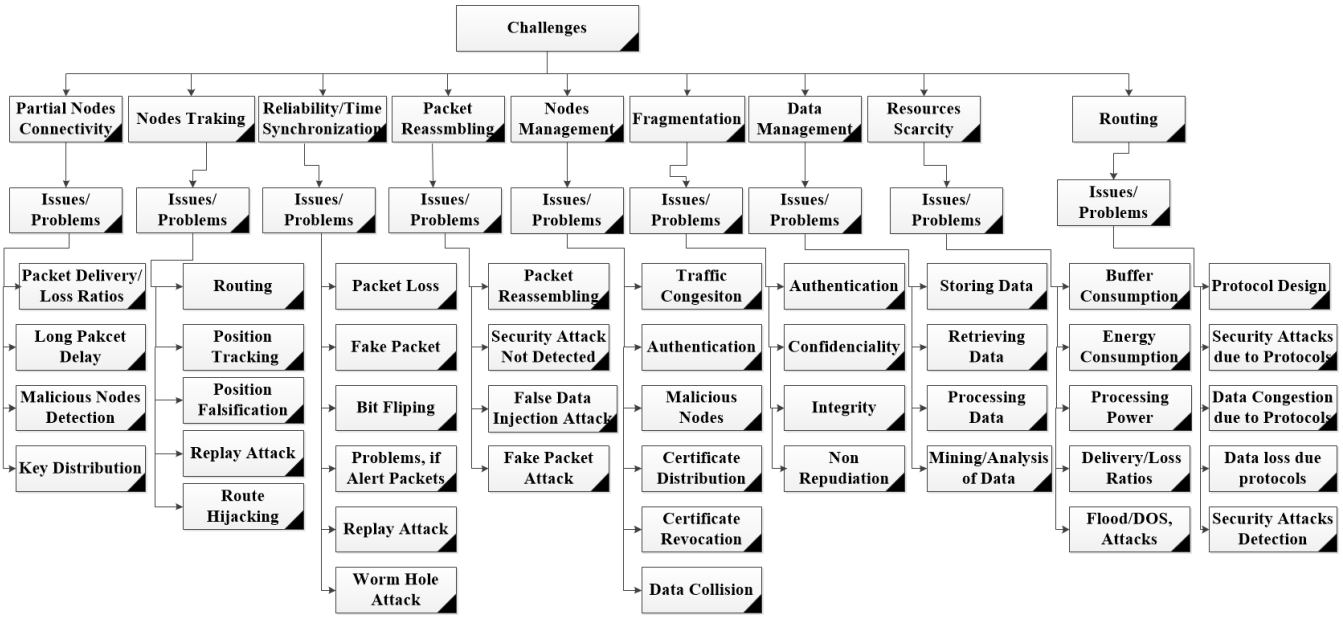

FIGURE 1. Various challenges/issues of ICV-DTNs.

Researchers proposed various techniques to tackle flood attacks [79]. Nevertheless, each algorithm has its own pros and cons. According to the analyses of this article, the perfect solution to flood mitigation is still a challenging and open research issue in ICV-DTNs. Detection-Time, Detection-Rate, High-Detection-Cost, Centralized/Sole mitigation algorithms (In sole mitigation algorithms, one node is responsible for attacks detection and mitigation), High-Resources-Consumption and lack of proper definition of flood attacks are among the main problems of existing proposed algorithms.

Few researchers proposed various survey papers such as researchers in article [80], discussed security-related research problems/issues in opportunistic networks, however with lack of detail on flooding attacks. Researchers presented a very comprehensive survey in article [81] which is related to MANETs. However, the reviewed algorithms are not practically applicable in ICV-DTNs. Researchers in article [54] discussed misbehaving nodes taxonomy (Nodes which launch various attacks) very comprehensively with a lack of details on flood attacks. Researchers in the survey article [38] discussed the advantages and disadvantages of only three research schemes of flood mitigation. Researchers in article [82] briefly defined various misbehaving attacks (BlackHole, GrayHole, Identity Theft, Sybil, Replay attacks, etc) in DTNs with lack of details on flooding attacks. In comparison, this article proposed a unique taxonomy of flood attacks, which will open up new research directions to confront flood attacks (Due to this taxonomy, flood mitigation will open new research ideas for researchers to handle misbehavior malicious nodes which launch flood attacks in networks). Also, according to our knowledge, this article discussed the pros and cons of previously proposed research articles on flood mitigation in ICV-DTNs (unlike [38]). Moreover, this article gives buffer-consumption code for simulator unlike previously proposed articles. Following are some of the main contributions of this article.

- Novel/Unique taxonomy of flood attacks in ICV-DTNs.
- Unique taxonomy of previously proposed mitigation schemes.
- Cryptanalysis of previously proposed algorithms.
- Analytic analysis of previously proposed algorithms and various flood attacks scenarios.
- Buffer Consumption calculation Code, this article modified the existing code of EpidemicRouter for bufferspace consumption, which calculates buffer consumption of all nodes with a run time in simulation (few researchers claim that due to flood attacks lot of buffers are consumed, however, according to our knowledge researchers did not show with simulation results that how much buffers are consumed and how to calculate this in real simulation).
- Open research issues in the subject research domain.

Rest of the paper is organized as follow. Section II discusses literature reviews on flood attacks. Section III discusses taxonomy of flood attacks mitigation schemes. Section IV discusses Cryptanalysis of previously proposed algorithms of flood attacks detection/mitigation. Section V discusses Motivation and Problem Statement. Section VI is related to Flood Attacks Taxonomy (Revised definition of flood attacks, contribution of this article). Section VII discusses Analytic Analyses of previously proposed schemes in flood mitigation and Various Flood Attacks Scenarios. Section VIII is related to open research issues, Followed by

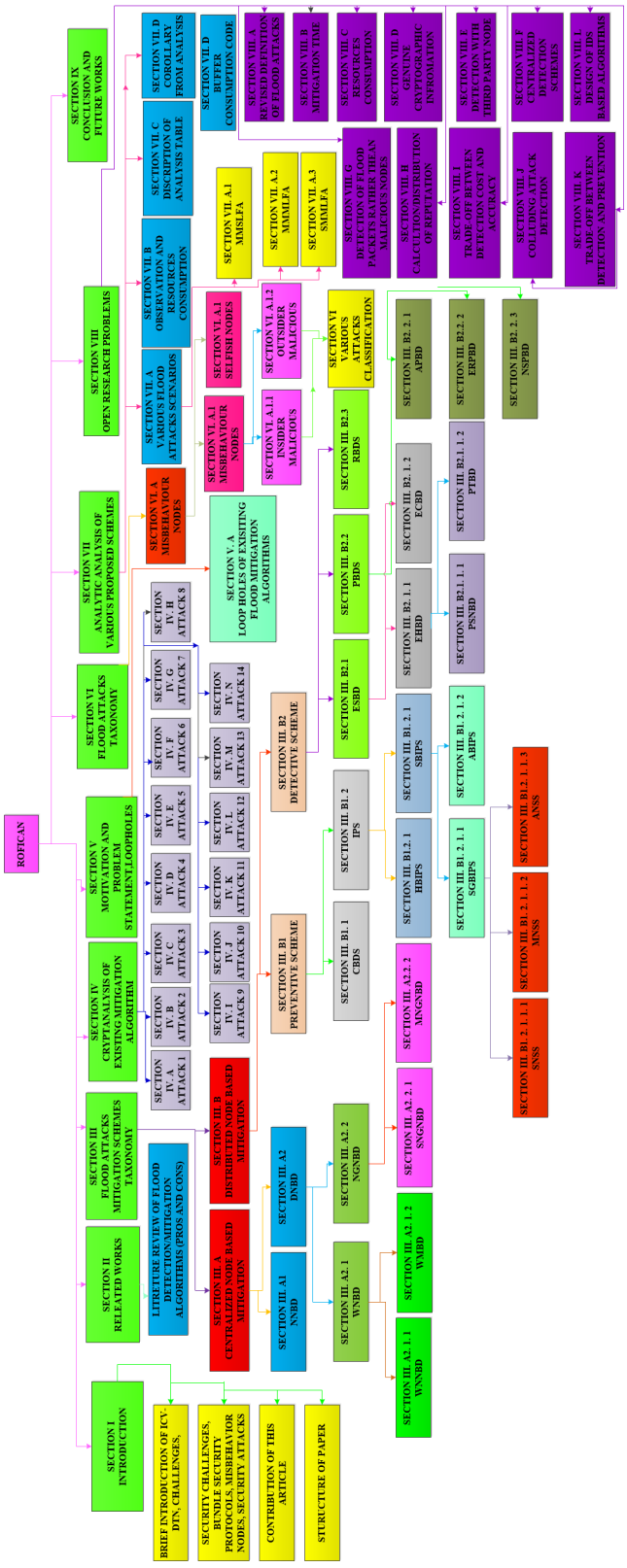

FIGURE 2. Structure of paper.

conclusion and future work in Section IX. Fig. 2 shows detail structure of this article.

II. RELATED WORKS

Bad behavior malicious nodes are an audacious threat for ICV-DTNs because malicious nodes waste precious resources such as buffer, bandwidth, and energy (already mentioned in this article). Researchers proposed various algorithms to detect and mitigate misbehavior nodes. This section discusses existing proposed schemes/algorithms (according to our knowledge) for flood attacks detection/mitigation.

To mitigate intruder nodes Li et al. proposed [28] distributed algorithm. In this scheme, every node participates in the detection of malicious nodes. Researchers proposed a Packet-Rate-Limiting-Scheme (PRLS) to mitigate intruder nodes. In this article, all nodes in networks forward packets for Packet-Rate-Limit-Certificate (PRLC) (initial setup phase of network) to trusted-authority (TAs). In response to this request, TAs allocate PRLC to a particular node in networks (According to nodes forwarding requirement). In this scheme, all nodes create message-claims (claim of forwarded packets, known as MCs) and count their own messages. During the communication phase, all nodes send PRLC along with original messages/packets and MCs. In the attack detection phase, destination nodes crosscheck all MCs in the whole networks. Proposed PRLS detects/mitigates flood attacks according to the pigeonhole principle. The proposed algorithm is very efficient to detect/mitigate this catastrophic flooding attacks. However, High Detection Time (HDT) is the downsides of this scheme (Detection Time is very high because the destination cannot detects attacks until the destination crosscheck all packets), This ultimately causes more resources consumption. The researchers in the article [83] improved the work [28] by adding learning automata-algorithm along with PRLS to modify the existing PRLS algorithm. This approximately counts the packets of every node according to the researchers.

Researchers in article [84] proposed a centralized algorithm to mitigate flood attacks. Through this scheme single node in network is responsible for the detection of attacks. In this algorithm, every node in the network shares its persistence buffer picture to designated ''GateWayNode (GWN)''. GWN counts forwarded packets of each node in the networks. In this scheme authors proposed a threshold value for each node, if a particular node violates the pre-defined threshold limit, GWN blacklist that particular malicious attacker node. The proposed scheme mitigates/detects both packetflood (intruder nodes forward large numbers of different packets) and replicaflood (in this attack, misbehavior nodes forward replicas of the same packets) attacks deterministically. Moreover, researchers in this article also proposed, probabilistic mitigation/detection scheme for replicaflood attacks, which according to the researchers improved the detection time. This is a very good scheme, however, the proposed scheme is difficult to deploys (all messages/packets are passed from one designated node, which is not suitable in DTNs) in DTNs, this is because of the disconnection of nodes in DTNs. This scheme is ideal for TCP/IP networks, where end-to-end connection is ensured but it is not optimal for DTN because of intermittent connection among nodes. Hence, it is

obviously a shortcoming of this particular scheme, according to the findings of this article.

Researchers of the article [85] proposed a scheme to detect flood attacks. In the proposed scheme, researchers proposed, that if a particular node in a network infrequently encounters other nodes in the network, and it forwards a large number of packets, it indicates maliciousness of the nodes (according to researchers). Hence, a few buffer space is allocated to the malicious nodes whereas more buffer space is reserved/dedicated for benign nodes. In this algorithm, researchers proposed a specific formula, which delete packets from the nodes' persistence memory. Although the proposed algorithm is an efficient to detect malicious nodes. However, falsepositive and falsenegative ratios are very high in this particular scheme. Also, this particular algorithm applies to specific routing protocol (Prophet [86]), which is an obvious disadvantage. An algorithm is required, which applies to all routing protocols.

Researchers of article [87] proposed a reputation scheme to thwart attacker malicious nodes. According to the assumption of the proposed scheme, misbehavior intruder nodes can flood whole networks with fake-messages/bogus-messages, however, malicious nodes do not create genuine packets. During the initial phase, nodes create a genuine message/packet and forwards that genuine message/packet to TAs for reputation. TAs allocate reputation to that particular node assuming that when a node creates genuine packet it will be innocent not an attacker. However, TAs do not allocate specific reputation value to all nodes in networks, which cannot create valid/genuine packets. In the attack detection phase, all receiver nodes verify the reputation value of all nodes in networks, if reputation is less than a pre-defined threshold value (proposed algorithm defined threshold value for nodes), the receiver does not accept packets from that particular node. Although this is a very good scheme to mitigate misbehavior attacks. However, according to the analyses of this article, researchers proposed an ideal preventive-based scheme to prevents an intruder nodes. This paper does not addresses answers to a few important questions. Such as Why intruder nodes cannot create benign messages? How TAs distinguished between benign and fake messages? What exactly are the real criteria for a benign message?

Researchers of article [45] proposed an algorithm that detects flood attacks. The proposed algorithm uses cookies, which are created from RandomNumber (RN), TimeStamp (TS), and SourceIdentifier (SI) to detect malicious nodes. Moreover, researchers also improved the detection probability of cookies by using HMAC and XOR. The proposed scheme detects/mitigates misbehavior nodes by a process of cookies verification on the destination. Although, this is a very efficient scheme to mitigates flood attacks in DTNs. However, the proposed algorithm detects only external misbehavior malicious nodes (A particular node in networks which does not have a key and other cryptographic credentials are known as, an external misbehavior node), which is a very important shortcoming of this particular scheme (because this scheme cannot detects all those intruder nodes which have a valid cryptographic credentials).

Article [88] proposed StreamNode (SN) to weed-out malicious nodes from the networks. It is a centralized algorithm, in which one node is taking responsibility for detecting misbehaving intruder nodes. In this research article, researchers proposed SN for the detection and mitigation process. SN have three tables which includes, BlacklistingTable (BTs), PacketDeliveryProbabilityTable (PDPTs), and PacketRateLimitingTable (PRLTs). In the proposed scheme, SN calculates the actual delivery probability from PRLTs. SN compares actual delivery probability with calculated probability from PDPTs. If there is any inconsistency, proposed algorithm assume it is malicious. Although this is a very good algorithm to thwart misbehavior attacker nodes. However, in the proposed scheme, SN moves like a mobile police guards with all packets. The issues of this algorithm are high costs and hard to practically implementation in ICNs due to the intermittent connection between nodes in DTNs.

Researchers in research article [89] proposed an efficient scheme to cope with malicious nodes. The proposed algorithm piggybacks the previously proposed encounter-record (ER) algorithm with PRLS to detects misbehaving intruder nodes. In this scheme, misbehaving nodes launch attacks on ER, but it fails. As misbehaving nodes either alter packet timestamp (TS) or change message sequencenumbers (SN) to launch attacks. However, through these alterations, ER becomes inconsistent. The proposed scheme can detects alteration in ER. The proposed piggybacks scheme detects those misbehaving nodes which changed ER. Although this is a very good scheme to chuck-out misbehaving intruder nodes, however, it has a high detection time and cost. In this algorithm, nodes share encounter history(EH) with all nodes in networks, which consume buffer space and bandwidth of all nodes, this ultimately cause low PDRs and high PLRs. These are a few shortcoming of the proposed piggybacks scheme.

Researchers in [90], [91], and [92] proposed algorithms quite similar to [28] to mitigate flood attacks. Researchers in [93] enhanced [28] to generates key, using Advance-Encryption-Standard (AES) algorithm. According to the authors, malicious nodes are not identified in article [28] when they send/forward packets less than the allowed numbers. Researchers proposed a key for those attacker nodes. However, according to the analyses of this article, there is no needs for a key, because article [28] already has a key. Article [94] enhanced the work [28] by using DNS query and MYSQL database along with PRLC [28] (according to the researchers). According to the researchers, the proposed algorithm detects and mitigates application-level flood attacks, which consume server resources. However, application-level flood attacks are not very effective in DTNs. That is why the malicious nodes use a Network/Transport-level flood attacks, which consume networks resources.

In article [95] researchers proposed algorithm like [28]. Researchers added the RSA algorithm which according to researchers enhanced the performance of [28] which finds exact malicious nodes. The extra cost of RSA is the shortcoming of this algorithm, which is not required (according to the study of this article) because article [28] can exactly identifies intruder misbehavior nodes.

Researchers in an article [35] proposed an efficient algorithm to thwart flood attacks in ICNs. It is a resources efficient algorithm, i.e. buffer, energy, and bandwidth. Authors in this article proposed three algorithms, ''Revamp to Lie or Comply (RTOC)'', ''Inter-Site-Flood-Attack-Mitigation (IFAM)'', and ''Holistic-Flood-Attack-Mitigation (HFAM)''. ''RTOC'' is the improved version of the algorithm [28]. In this scheme, researchers proposed Huffman coding for packets compression. Proposed ''RTOC'' compresses packets payload without ''MCs''. Algorithm [28] cross-check ''MCs'' along with original packets to detects flood attacks. According to the mathematical and simulation-based analysis of algorithm [35], algorithm [28] consumes more resources, which further increases packet-loss-ratios and decreases packet-delivery-ratios (This assumption is proved in article [35]). ''RTOC'' enhances resources consumption, which further enhanced packet-delivery-ratios and reduces packet-loss-ratios. However, ''RTOC'' works like algorithm [28] which is susceptible to some attacks as mentioned earlier in the shortcoming of article [28].

In article [35] researchers proposed ''IFAM'', which detects flood attacks in a specific scenario (Specific scenario of two-sites). In this particular scheme, authors deployed ''IDS'' in some specific nodes, which forward packets between two sites. In this particular algorithm, ''IDS'' based nodes generate a key (''TAs'' have that specific algorithm that creates the same key). In the initial phase, all nodes forward the request packet to ''TAs'' for ''PRLS'' except ''IDS'' based nodes, which append key along with packet for rate-unlimited-certificate. ''TAs'' grant ''PRLS'' to all nodes except ''IDS'' based nodes, which are assigned rate-unlimited-certificate. In the forwarding phase, all nodes append the ''PRLS'' along with the packets payload and sign (encrypt with private key) the packets. When an ordinary node (Nodes in networks except IDS-based nodes) forwards a packet to ''IDS'' based nodes, ''IDS'' based nodes verify the signature, and ''PRLS'', then decrease the count value by one of that particular node. Although this is an efficient scheme to mitigates misbehaving nodes which launch flood attacks in two-sites scenario. However, when malicious nodes forge/compromise the ''TAs'' key, obviously it will create the ''PRLS'' for themselves, which is obviously a problem/shortcoming of this particular scheme.

Researchers an article [35] modified the ''IFAM'' algorithm to propose ''HFAM'' for a generic scenario in which all nodes have IDS, and every node ''IDS'' generates a key. In the forwarding phase, sender node ''IDS'' verifies the packet's signature, generates a specific number (key), appends with the packets to creates ''Message Authentication Code (MAC)''. Receiver nodes ''IDS'' verify all credentials by a reverse process to detect flood attacks. Although this is a very efficient scheme, however, ''IDS'' is deployed in all nodes which counts packets for all nodes, this makes the system vulnerable to attacks, as all ''IDS'' based nodes create the same key and malicious nodes can easily guess the key and can launch some certain attacks (downside, not fair system).

A. ANALYSIS

This section analyzes and summarizes the related works on our proposed parameters list mentioned in Table 1. Misbehavior nodes launches various attacks outlined already in this article. Flooding attack overuse the limited resources and also create nodes unavailability issues in the networks. Moreover, significantly degrades the network performance (decreases packet delivery ratios and throughput). We take various parameters to summarized the misbehaved nodes which is discussed as follow.

- **Algorithms-Type (AT):** Generically there are three types of algorithms proposed in the research articles, that is Detective-Algorithms (DAs), Preventive-Algorithms (PAs), and some are hybrid (DAs/PAs), which uses both.
- **Algorithms-Methodology (AM):** The researchers proposed various detection methodology to cope with malicious nodes, such as Probabilistic-Methodology (PM), Deterministic-Methodology (DM), and some are hybrid (PM/DM at the same time). Few researchers proposed very efficient and straight-forward method to thwart malicious nodes, which enhanced the detection time, and detection probability.
- **Trusted-Nodes (TN):** Few researchers proposed TN along with proposed algorithms to weed-out malicious nodes. The TN in various proposed algorithms plays various role. The role of TN is very important because the algorithms without TN have high false positive/false negative ratios. TN have various role (TNR) in various proposed algorithms/schemes, such as Certificate-Allocation (CAs), Black-Listing (BL), Key-Generation (KG), Algorithm-Detection (ADs), Reputation-Calculation (RCs), Reputation-Allocation (RAs), and Probability-Calculation (PC).
- **Algorithm-Procedure (AP):** Some of the researchers proposed an efficient procedure to cope with misbehaving nodes. However, few proposed algorithms have complex detection procedure, which is not time efficient to detect malicious nodes (long time to detect malicious nodes). This article categorized various proposed algorithms into two categories, such as Complex-Algorithm (CA) and Non-Complex-Algorithms (NCA).
- **Algorithm-Efficiency (AE):** In few research articles, researchers proposed an efficient mitigation algorithms which is suitable for DTNs, however, some of the proposed mitigation algorithms are inefficient to weed-out malicious nodes and costly. This article categorized

algorithms into three categories, such as Efficient-Algorithms (EA), Very-Efficient-Algorithm (VEA), and Non-Efficiency-Algorithms (NEA).

- **Detection-Scheme (DS):** Few researchers proposed algorithms which detect malicious nodes with collaboration of various nodes. This article divided Detection-Scheme into two categories. such as Detection-With-Collaboration (DWC) and Detection-Without-Collaboration (DWOC). In the DWC schemes the detection responsibility is distributed among all the nodes unlike DWOC schemes in which the detection responsibility on one specific node.
- **Mitigation-Action (MA):** The researchers proposed various mitigation action against malicious nodes which launch flooding attacks (Blacklisting (BL), Buffer-Allocation (BA).
- **Detection-Accuracy (DA):** This article categorized the Detection-Accuracy into four categories, such as Poor, Good, Better, Best.
- **Routing-Protocol (RP):** Few researchers proposed mitigation algorithm which is applicable in some specific routing protocol, however some schemes are applicable in all routing protocols of DTNs.

III. FLOOD ATTACKS MITIGATION SCHEMES TAXONOMY (FAMST)/CLASSIFICATION OF FLOOD ATTACKS

Misbehavior nodes are catastrophic for ICV-DTNs. Researchers proposed various algorithms to cope with misbehavior nodes (which is already discussed in the previous section of this article) in DTNs [96], [97]. This section discusses mitigation techniques to handle misbehavior nodes in DTNs. This article critically analyzed previously proposed mitigation algorithms to propose a unique taxonomy of various mitigation schemes. Here, few schemes are previously proposed and some are the unique classification of this article. Fig. 3 shows the unique taxonomy of flood attacks mitigation schemes [56]. Following are the two main categories of previously proposed mitigation schemes.

A. CENTRALIZED/SINGLE-NODE-BASED-MITIGATION (CNBM)

A few researchers proposed CNBM algorithms to cope with misbehaving nodes [54], [98]. In CNBMS, researchers proposed a single node for mitigation of misbehaving nodes [84]. In these schemes, researchers select a single node among multiple nodes in networks for the mitigation of misbehaving nodes. This article further classified CNBM schemes into two categories [35], [54].

1) NETWORK-NODE-BASED-DETECTION (NNBD)

In NNBD, all nodes participate equally to detect malicious nodes. When malicious nodes forward malicious packets to benign nodes, benign nodes have a built-in capability to detect malicious flood attacks.

2) DESIGNATED-NODE-BASED-DETECTION (DNBD)

In DNBD schemes, researchers proposed designated/specific node in networks for malicious attacks detection. Unlike NNBD, in these schemes, researchers specify a single node for attacks detection (In NNBD, detection responsibility is not assigned to a specific node) [54]. In DNBD schemes, researchers assign various responsibilities to designated node. A node either monitors a single node or the whole networks [99], based on this observation, DNBD is further classified into the following two categories.

* Watcher-Node-Based-Detection (WNBD):- In WNBD, a designated node either monitors a nearer single node or monitors a communication channel/medium [99]. Based on this observation, WNBD schemes are further classified into the following classes.
  - Watcher-Neighbor-Node-Based-Detection (WNNBD):- In WNNBD, the designated node monitors only connected/neighbor nodes for malicious attacks [54].
  - Watcher-Medium-Based-Detection (WMBD):- In this category, the designated watcher node monitors a single channel/medium for malicious attacks.
* Network-Guard-Based-Detection (NGNBD):- In NGN BD, the designated monitoring node has the responsibility to monitors whole networks for fraudulent attacks. The monitoring node either statically monitors the whole networks or dynamically moves in the networks to detects malicious nodes [54], [100]. Based on this finding/analysis, this article further classified NGNBD into the following sub-categories.

- Static-Network-Guard-Node-Based-Detection (SNGN BD):- In SNGNBD, the designated guard node is static in a specific position in the network to monitors whole networks. All packets/bundles pass through this designated node (the designated node inspects all packets for malicious attacks) [54]. This type of scheme is ineffective in DTNs because passing all packets are very difficult to deploy in DTNs, due to the intermittent connectivity and the sparse nature of nodes in ad-hoc networks [35].
- Mobile-Network-Guard-Node-Based-Detection (MNGN BD):- Unlike SNGNBD, in MNGNBD designated guard node is dynamic, and moves along with all packets to detects malicious attacks. Few researchers proposed this type of scheme. However, according to the analyses of this article, this is almost impossible to practically implements in ad-hoc networks (Not possible to efficiently and effectively implemented in DTNs) [54].

B. DISTRIBUTED/COOPERATIVE-NODES-BASED-MITIGATION (DNBM)

According to the critical examinations of this article, Some researchers proposed DNBM algorithms to smash malicious nodes, which launch flood attacks [101]. In DNBM algorithms, multiple nodes detect malicious nodes with collaboration. On a positive note, DNBM schemes are very efficient

TABLE 1. Analyses of literature review.

Article	AT	AM	TN	TNR	AP	AE	DS	MA	DA	RP
[86]	DAs	PM	No	Nill	CA	EA	DWC	BA	Good	Prophet
[85]	DAs	PM/DM	No	Nill	CA	NEA	DWOC	BL	Good	All
[29]	DAs/PAs	PM	Yes	CAs, BL	NCA	VEA	DWC	BL	Best	All
[84], [91]–[94]	DAs/PAs	PM	Yes	CAs,BL, KG	NCA	NEA	DWC	BL	Poor	All
[46]	DAs	DM	No	Nill	NCA	EA	DWC	BL	Better	All
[88]	PAs	DM	Yes	RCs, RAs	CA	NEA	DWC	BL	Good	All
[90]	PAs/DAs	PM	Yes	CAs	CA	VEA	DWC	BL	Best	All
[89]	DA	DM	Yes	ADs, PC	NCA	NEA	DWOC	BL	Poor	All
[36]	Pas/DAs	DM	Yes	CAs, BL	NCA	EA	DWC	BL	Better	All

in detecting malicious nodes. The proposed schemes reduce the ratios of false positive and false negative. Researchers proposed both preventive and detective-based distributive algorithms to glitch malicious nodes [54]. That is why this article further classified DNBM algorithms/schemes into the following two categories.

1) PREVENTIVE-APPROACH (PA)

As mentioned earlier in this article, few researchers proposed preventive-based algorithms to crumble misbehaving malicious nodes in DTNs [102], [103]. Preventive-based algorithms prevent various attacks, which minimize the catastrophic consequences of various attacks. The Studies of this article suggests that preventive measures can be put in place to prevent attacks (DTNs have limited resources, thus a good approach for DTNs). According to the findings of this article, flood prevention is preferable to flood detection due to the scarcity of resources [35], [54]. According to the critical analyses of this paper, few research articles proposed pure preventive schemes. However, few researchers assign rate-limit-certificate to latch malicious nodes. Based on this observation, this article further classified PA into the following two types [35], [54].

- Certificate-Based-Detection-Scheme (CBDS):- In this category, researchers proposed a hybrid rate-limit-certificate along with a preventive strategy to hinder malicious attacks. This type of approach mitigates misbehaving nodes which launch flood attacks [28], [54]. In such algorithms, researchers have predefined a threshold (rate-limit-certificate) for all nodes in order to control the number of packets for malicious nodes. If malicious nodes violate this limit, the proposed algorithms black-list those malicious nodes. This article calls this type of scheme CBDS.
- Intrusion-Prevention-Schemes (IPS):- IPS-based schemes are powerful enough to contend with malicious nodes in ad-hoc networks. Few researchers proposed IPS schemes to thwart malicious nodes which launch flood attacks in DTNs [35], [104]. This article further categorized IPS-based schemes/algorithms into the following classes.
  * Hardware-Based-IPS (HBIPS):- In this type of IPS scheme, designated hardware is designed to cope with misbehaving nodes. However, HBIPS are expensive. It has a high manufacturing costs, but HBIPS are fast and efficiently detect various attacks (the quality of this category). This further minimize false positive and false negative ratios [54].
  * Software-Based-IPS (SBIPS):- In this kind of IPS, the programmers develop a set of instructions (programs) to deal with nodal misbehaving attacks. Unlike HBIPS, SBIPS schemes are easily develop and have low manufacturing cost [35], [54]. That is why SBIPS have low detection accuracy/efficiency relative to HBIPS. Both HBIPS and SBIPS use various strategies to detect malicious attacks, which are discuss below.
    + Signature-Based-IPS (SGBIPS):- Few researchers proposed SGBIPS schemes to muddle with misbehaving nodes. SGBIPS schemes detect attacks with known signatures of various attacks. It is a powerful methods to weed-out malicious nodes from networks. But it has a high development costs in terms of times [54]. Security engineers/ programmers spend a lot of time collecting the signatures of various attacks. Furthermore, SGBIPS schemes are inefficient in the detection of zero-day attacks, this is the downside of SGBIPS. As, intruders developed new viruses/worms/spywares/ransomwares, and new attacks strategies every day. SGBIPS schemes are either implemented in a single node or multiple nodes. It is further classified into the following categories.
      @ Single-Node-Signature-Scheme (SNSS):- In this sort of signature scheme, researchers suggested signature-based IPS in a single node, which is responsible for the detection of various attacks. However, SNSS is inefficient in ad-hoc networks (detects attacks only when all packets pass through this designated signature node, which is almost impossible in ad-hoc networks) [35], [54].

@ Multiple-Nodes-Signature-Scheme (MNSS):- Few researchers offered MNSS. In MNSS, researchers implemented signature-based IPS in multiple nodes instead of signal node [35]. This sort of scheme is an efficient to detects various attacks relatives to SNSS.

@ All-Nodes-Signature-Scheme (ANSS):- Few researchers proposed the signature scheme in all participating network nodes [35], [105]. On a positive note, the detection rate of various attacks are higher than SNSS, and MNSS. However, it is costly and difficult to deploy in ad-hoc networks.

+ Anomaly-Based-IPS (ABIPS):- Unlike SGBIPS, ABIPS detects various attacks with attackers/malicious nodes' behavior. According to the verdicts of this article, it is an efficient approach to cope with malicious attacker nodes (detects zero-day attacks) [54]. However, the detection of attacks with nodes' behavior are tough task, which is obviously the hitch of ABIPS. ABIPS schemes need a lot of effort to develop (high development cost, depends on programmer efficiency, wastes a lot of programmer energies).

2) DETECTIVE-APPROACH (DA)

Few researchers proposed detective approach to mitigates flood attacks in DTNs. In DA, researchers proposed algorithms, which detect misbehavior nodes before weed-out/black-list malicious nodes from the networks [34], [45], [49], [55], [89]. This is a very optimal strategy to thwart various malicious nodes (exactly detects malicious nodes and black-list the malicious nodes), however slow detection is the downside [106]. According to the critical study of this article, various researchers proposed various detective strategies to set aside malicious nodes. That is why this article further classified DA into the following three categories.

@ Encounter-Scheme-Based-Detection (ESBD):- Encounter(s) is the meeting (contact(s)) between two DTNs nodes. When encounter(s) occurs between two nodes, all nodes save encounter(s) history information. Based on the encounter(s), some researchers have proposed detection and mitigation algorithms to cope with misbehaved nodes [34], [35], [54]. This article calls this type of approach ESBD. It is a very good approach to handle misbehavior nodes, which launch both flood and packet drop attacks. According to the investigations of this article, researchers detect malicious nodes with various encounter(s) information. Based on this observation, this article further classified ESBD into two categories.

- Encounter-History-Based-Detection (EHBD):- In EHBD schemes, researchers proposed, packet history information (Node Identity, Packet-Sequence-Number, and Packet-Time-Stamp (arrival Time)) to detect malicious nodes [54]. This article subdivides EHBD into the following two categories.

+ Packet-Sequence-Number-Based-Detection (PSNBD):- In such algorithms, researchers proposed packet-sequence-number to eliminate malicious nodes from the networks.

+ Packet-Time-Based-Detection (PTBD):- In PTBD scheme, researchers use time-stamp (packet arrival time) to mitigate misbehavior nodes attacks.

- Encounter-Counter-Based-Detection (ECBD) Few researchers proposed counter-based detection schemes. Through these algorithms, researchers count the number of encounter(s) (contact(s)) of various nodes to deal with malicious nodes [54].

@ Protocol-Based-Detection-Scheme (PBDS):- When some extra capability is plugged into an existing security protocol to detects and mitigates misbehavior nodes, we call it protocol-based defense scheme [54]. Few researchers proposed protocol-based defense schemes to diminish misbehaved nodes. Researchers proposed various strategies to cope with misbehaving nodes based on PBDS. That is why this article further categorized PBDS into the following categories.

* Architecture-Protocol-Based-Detection (APBD):- Few researchers proposed security architecture-based schemes to handle misbehaving nodes which launch malicious attacks. In these schemes, researchers modify an existing security protocol (bundle security protocol) to cope with misbehaving nodes. We call it APBD.

* Existing-Routing-Protocol-Based-Detection (ERPBD):- Some of the researchers modified an existing routing protocols (FirstContact, Prophet, SparyAndWait, SprayAndFocus, etc) to chuck-out malicious nodes, which launch various malicious attacks. These detection schemes are termed ERPBS.

* New-Security-Protocol-Based-Detection (NSPBD):- In this category of mitigation schemes, researchers proposed novice routing algorithms to handle malicious attacks. We term these detection schemes as NSPBS.

@ Reputation-Based-Detection-Scheme (RBDS):- To handle selfish nodes in DTNs, researchers proposed various reputation-based schemes [50]. In reputation-based schemes, reputation is given to nodes, to clutch the selfish behavior of the selfish nodes. The researchers proposed a variety of strategies to calculate nodal reputation, such as TAs directly calculating nodal reputation or researchers calculate nodal reputation from acknowledgment packets [54]. Although, these types of schemes/algorithms are very efficient in detecting a special category of misbehaving nodes, which are known as selfish nodes. However, the proposed schemes are inefficient in detecting malicious nodes which launch flood attacks, which is the drawback of the proposed algorithms [54].

IV. CRYPTANALYSIS OF EXISTING MITIGATION ALGORITHMS/POSSIBLE ATTACKS ON PREVIOUSLY PROPOSED SCHEMES

This section will critically and briefly analyzes previously proposed algorithms in this particular security research domain. Actually, in this section, this article launches various theoretical attacks on previously proposed algorithms, which are quite possible/practical.

A. ATTACK SCENARIO 01

Consider an attack scenario on article [85]. According to this article, the nodes which encounter(s) infrequently and forward lot of packets are the indicator of malicious behavior. However, according to the analysis of this article, this is not the case. Consider sparse networks of five vehicular nodes, ''V1'', ''V2'', ''V3'', ''V4'', and ''V5''. Node ''V2'' is moving near all other nodes in networks (which is encountered frequently) and forwards many/sufficient packets (attacker place ''V2'' near all nodes in networks, which is encounter(s) frequently Or malicious nodes quickly move to change have location near all other nodes). The proposed scheme assumes ''V2'' is benign, and allocates a significant amount of buffer space (high false negative rate). Unlike ''V2'', ''V1'' is moving far away from other nodes, and forwards a lot of messages. The proposed algorithm assumes, ''V1'' is malicious and allocates less amount of space (after sometime black list this node). However, this is obviously the wrong decision (high false positive rate).

B. ATTACK SCENARIO 02

Consider a second attack scenario on the algorithm proposed in article [85]. In this scheme, one particular routing protocol (Prophet) is used. Consider an attack scenario in which one particular malicious node (say ''M1'') using routing protocol Epidemic, FirstContact, DiretDelivery, SprayAndWait, and SprayAndFocus, etc. Obviously the proposed scheme cannot detects this attack (successful attack launch), which is a shortcoming of this scheme.

C. ATTACK SCENARIO 03

Consider an attack scenario on the scheme [84]. There are hundreds of nodes in ICV-DTNs, which are deployed in sparse network environments. There are five malicious nodes (''M1'',''M2'', ''M3'', ''M4'', and ''M5''). If malicious nodes do not share memory pictures with the designated detection nodes (gateway nodes). The designated nodes obviously cannot collect buffer information from all nodes (Due to sparse density). This particular algorithm cannot detects all malicious nodes (In this scheme, all nodes share a buffer picture with the designated nodes, and the designated nodes have threshold values. If some nodes violate a certain threshold, so algorithm detects it has malicious intent).

D. ATTACK SCENARIO 04

Consider another attack scenario on [84]. Intruder node ''I1'' targets the designated nodes to overflow the buffer space. In this scenario, the designated nodes which are responsible for collecting buffer space information (detect malicious nodes) from all nodes, do not accommodate in their buffer (due to overflow, so cannot detect malicious nodes, single point of failure).

E. ATTACK SCENARIO 05

Consider an attack scenario on proposed scheme [28]. If one malicious node (say''M1'') creates ''PRLS'' and forwards that bogus/fake ''PRLS'' to another malicious node (say ''M2''). If ''M2'' appends that fake certificate along with the original message, so the benign nodes cannot verify this certificate (due to scarce resources and sparse network). Alternatively, if a malicious node creates a fake certificate for himself, so it is very difficult for innocent nodes to verify that certificate.

F. ATTACK SCENARIO 06

Consider an another attack scenario on [28]. If malicious nodes forge ''MCs'', and forward them to innocent nodes. The benign nodes do not have the capability to detect this attack (very difficult for a benign nodes to verify ''MCs''). This type of attack is not detected, because this particular scheme detects flood attacks with ''rate-limit-certificate'' along with ''MCs''.

G. ATTACK SCENARIO 07

Consider another theoretical attack scenario on [28]. Assumes, ''MCs'' and rate limit certificate are genuine. However, if the malicious node (''M1'') violates the rate limit (trusted authority assign rate limit), and forwards the packet to the benign node (''N1''). So in this case innocent node ''N1'' does not detects the attack until all nodes in network cross-check ''MCs'', which is very difficult (due to a large number of nodes and large distance between nodes).

H. ATTACK SCENARIO 08

Assumes an attacker launches attacks on the proposed scheme [45] from the inside network, which is quite possible (Most probable attack). Insider nodes have valid cryptographic credentials (node identification key, random number, and valid time-stamp), in this case, the proposed algorithm [45] is not capable to detects flooding attacks.

I. ATTACK SCENARIO 09

Consider malicious node ''A1'' launches attacks on the proposed algorithm [45] from outside of the network. If malicious node uses/creates benign nodes key (''B1'' key), and fresh time-stamp (quite possible attacks, which is known as Sybil attack). In this case, the proposed algorithm detects and blacklists benign node ''B1'' as an attacker node (High false positive and false negative ratio).

J. ATTACK SCENARIO 10

Consider an attack scenario in which particular malicious node ''IN'' launches an attack on the proposed scheme [87]

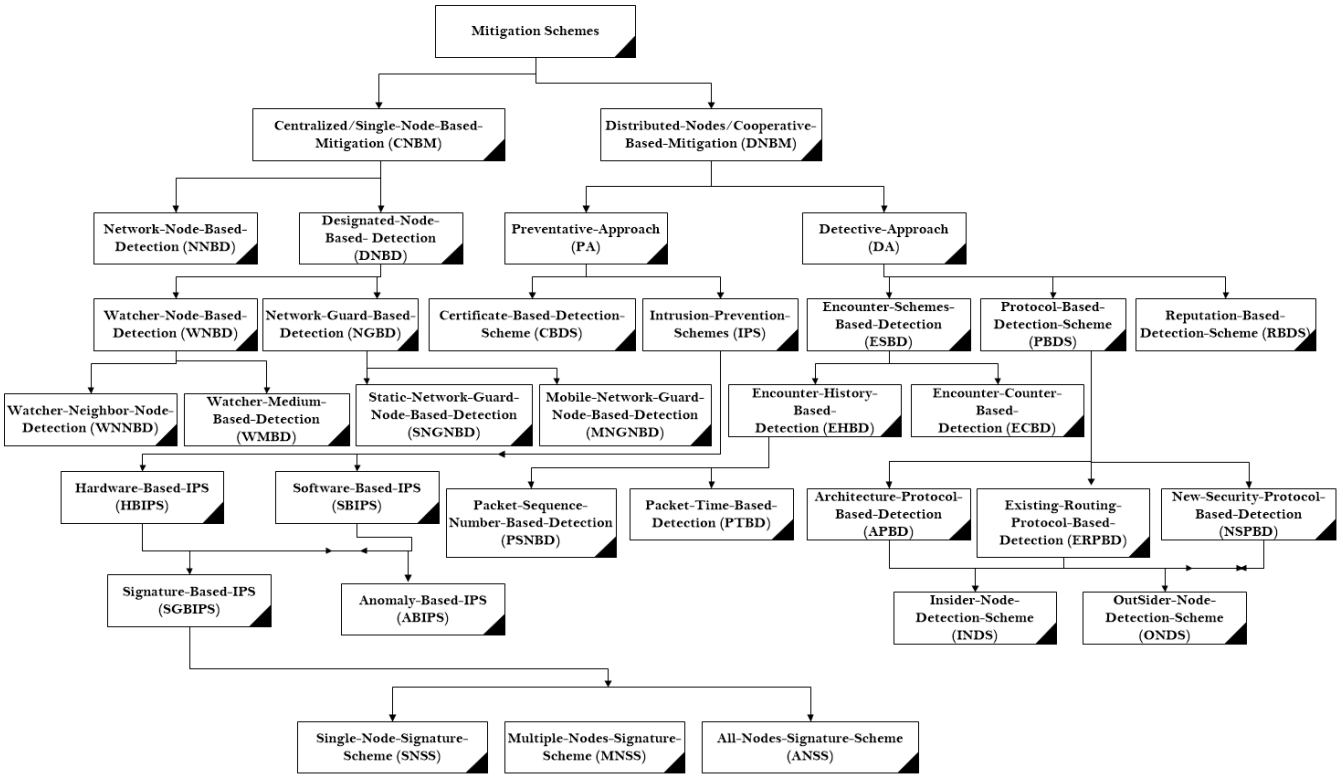

FIGURE 3. Flood attacks mitigation schemes taxonomy (FAMST).

by creating a genuine message. ''IN'' forwards that genuine message to ''TA'' for reputation. Once ''TA'' received the genuine message, ''TA'' assigns good reputation value to ''IN''. After getting a reputation from ''TA'', ''IN'' uses this reputation, and other nodes also verify the reputation, which is already verified, so all nodes in the networks build trust on ''IN'' is benign, however in reality ''IN'' is malicious.

K. ATTACK SCENARIO 11

Consider another attack scenario on the proposed algorithm [87]. A network that contains ten nodes. If two nodes ''B'' (benign node), and a malicious node ''M'' forward the request packet (genuine packet) to ''TA'' for reputation. In this case, ''TA'' assigns a good reputation to both benign and malicious nodes (it has high false positive and false negative ratios). Actually ''TA'' cannot recognize fake and genuine packets. This is not defined in this particular paper, as how ''TA'' recognized genuine and fake packets.

L. ATTACK SCENARIO 12

Consider sophisticated attack scenario on [87]. Assumes, malicious node ''N1'' creates a fake reputation for himself (which is quite possible). If ''N1'' forwards some packets to benign nodes in the network, the benign nodes will accept packets from ''N1'', because benign nodes assume node ''N1'' has valid reputation value (high false positive). The benign nodes do not have the ability to verify the reputation in the proposed algorithm [87] (very difficult to verify because nodes are scattered, and may have a very large distance between ''TA'' and other nodes in networks).

M. ATTACK SCENARIO 13

Consider an attack scenario on the proposed scheme [89]. The proposed scheme [89] is similar to the proposed scheme [28]. So Attack Scenario 05, Attack Scenario 06, and Attack Scenario 07 are quite possible to launch on this scheme (Attack Scenarios are already mentioned in this article).

N. ATTACK SCENARIO 14

Consider an attacker node launches attacks on the proposed algorithm [88]. The attacker node targets a stream node (''SN''), which is designated for attacks detection. It overflows the buffer of ''SN'' through flooding attacks. In this particular scenario, the proposed scheme will unable to detects even a single attack (single point of failure). Also according to the researcher in this article, ''SN'' calculates actual delivery probability and estimated probability. However, according to the examinations of this article, which is very difficult for ''SN'' to calculates in vehicular networks (almost impossible due to attacks on ''SN'').

O. ATTACK SCENARIO 15

Consider an attack scenario on the proposed algorithm [35]. If the intruder nodes target ''IDS'' based-nodes, which

overwhelm/fail "IDS" based-nodes. If the "IDS" based-nodes fail, which will cause the failure of whole networks (single point of failure). Also, if an attacker replaces some nodes with malicious nodes, which can create keys like genuine "IDS", in this case, the proposed scheme will unable to detects/mitigates attacks.

V. MOTIVATION AND PROBLEM STATEMENT

ICV-DTNs are vulnerable to numerous security challenges/attacks, already mentioned in this article. Specifically, the use of open wireless links to forwarding bundles provides straightforward opportunities for misbehaving nodes to attacks [107], [108], [109]. For example, in ICNs, misbehaving nodes can insert a large number of fake-bundles into the networks [55]. If benign nodes further forward these fake/false packets, the attacker creates large numbers of forged messages/packets to the networks. Due to the resource scarcity characteristics of ICNs, the extra messages/packets may lay serious security issues on the operation of ICV-DTNs. These loop-holes on ICV-DTNs security are more challenging as compare to traditional networks like MANETs, and WSNs, this is due to their unique security nature. Unlike Ad-hoc, and TCP/IP-based networks, ICV-DTNs have unique network protocol architecture (bundle protocol architecture), therefore they have new research issues.

ICV-DTNs have many problems, which are already outlined in this article. Misbehaving nodes are one of the research issue in ICV-DTNs. Misbehavior nodes launch attacks to waste precious resources, increase throughput (selfish nodes) (Selfish nodes drop other nodes packets to save their own's resources), spread bogus packets, and create nodes unavailability problems.

Misbehavior intruder nodes launch flood attacks to waste precious resources of ICV-DTNs. Misbehavior Selfish nodes usually drop packets of other nodes. Also, selfish nodes launch flood attacks to increase throughput. Researchers study the impact of misbehaving flood attacks on PDRs, PLRs, TBWCs, and TBCs [35], [54]. Due to flood attacks, PDRs are decreased, while PLRs are increased significantly (due to resources consumption) [10], [28], [35], [110].

Flood attack are a very challenging research issue in ICV-DTNs security. Researchers proposed some efficient algorithms to thwart this problem/issue. However, every algorithm has own merits and demerits. No perfect solution to this problem is proposed yet (according to our knowledge). This is still a big challenging research issue in DTNs. So it is urgent to propose an efficient algorithms to tackle this research problem. Below are a few issues of existing proposed algorithms (previously proposed algorithms for flood attacks detection and mitigation), which are discussed in this section.

A. LOOP HOLES OF EXISTING FLOOD MITIGATION ALGORITHMS

Few researchers proposed very efficient algorithms to combat flood attacks. However, some of the solutions are applicable only in constrained environments [48]. Researchers proposed Guard-Node [84] (Central-Guard in which all packets are passed through a single node, and Mobile-Guard-Node/StreamNode (SN) [88] in which designated node monitors whole networks) which is not a feasible solution (Centralized based solution is not efficient in DTNs, DTNs need distributed algorithms) due to intermittent connectivity. Also, if Central-Guard-node is compromise, the whole networks will be compromise (single point of failure). Also, Guard-Node-based algorithms have a high cost (Need extra nodes for detection). Some of the researchers proposed PRLS-based [28] algorithms, which use crosschecking strategy to mitigate/detect misbehavior intruder nodes, however, they always need a connected environment. The second problem with PRLS-based algorithms are high detection time because malicious nodes are not detected until other nodes crosscheck all packets, which ultimately cause more resource consumption until detection (high detection time, which further decreased PDRs).

Few researchers proposed ER-based [89] algorithms for flood mitigation, However like PRLS-based they always need connected environment (Nodes are disconnected in DTNs frequently). ER algorithms share EH information with all nodes in networks, which consume the buffer-space of those particular nodes. This ultimately cause low PDRs and high PLRs. The second problem with ER-based algorithms are an inability to detect colluding attacks (a particular type of attack in which misbehavior nodes collaborate to launch flooding attacks). The third problem with ER-based algorithms are high detection time like PRLS-based algorithms. ER-based algorithms have also a high cost (high cost in terms of TBWCs and TBCs, because they share EH packets with all nodes in networks, this consume a lot of memory space and bandwidth). Some of the researchers proposed protocol-based [45] detection, however, it only detects outsider misbehavior nodes (details of outsider misbehavior nodes are already mentioned in the literature review section of this article). Few researchers proposed [85] algorithm for flood mitigation, but [85] only works for Prophet protocol (DTNs need algorithms, which are applicable in all routing protocols). Also, the false-positive and false-negative ratios of this algorithm are very high.

Apart from the above-mentioned issues, researchers claim that due to flooding attacks resources (TBWCs, TBCs, and energy) are consumed [35], [54]. However, according to our knowledge researchers did not show with simulation results how much resources are consumed (Research articles did not demonstrate resources consumption calculation code). Furthermore, most of the researchers defined that there are two types of flood attacks (packetflood (PFA) and replicaflood (RFA)). However, according to the critical observations and analyses of this paper, there are so many other categories of flood attacks. According to the verdicts of this paper, if researchers correctly define different types of flood attacks (define all/various categories of flood attacks), then their mitigation will be easy for new researchers in this

field of research. Table 2 summarizes Loop-Holes, Detection Delay/Detection Accuracy, Feasibility/Scalability, and Overhead of previously proposed schemes [35], [54].

VI. FLOOD ATTACKS TAXONOMY/OUR PROPOSED CLASSIFICATION OF FLOOD ATTACKS

Mitigating flood attacks are one of the most challenging research problem of ICV-DTN security (which is already drafted in this article). The researchers proposed a few efficient algorithms to fray misbehavior attacker nodes that launch flood attacks [35], [87], [89], [111]. However, each algorithm has its own advantages and disadvantages, as already outlined in this article. According to the findings of this article, the detection of flood attacks are difficult, this is only because of the absence of the appropriate definition of flood attacks. Most of the researchers believe that there are two types of flood attacks, i.e. PFA and RFA [28], [84], [85], [88] (already mentioned in this article, few researchers defined some other categories of flood attacks).

Nevertheless, according to this article's analyses, poorly behaved nodes use a variety of strategies to launch flood attacks. If the researchers correctly define malicious nodes strategies that launch flood attacks or split a big problem into small pieces. Then try to solve problems with some new methods like divide-conquer, machine learning-based algorithms, and computational thinking-based algorithms, so according to the verdicts of this article, its solution will not be too much difficult. Moreover, if researchers try to solve atleast the sub-part of the problem (divide-conquer), this will be a good solution (according to the observations of this article). Furthermore, according to the critical analyses of this article, the solution based on computational thinking/Machine learning based is the best solution to challenging problems [112], [113]. Computational thinking-based solutions contain the following steps.

* Decomposition:- Decomposition is the process of breaking down a complex/big problem into smaller sub-problems.
* Abstraction:- Abstraction is a particular model of an existing system that leaves out unnecessary details.
* Pattern Recognition:- During the solution of a problem, find all those parts that are similar to existing problems, which are already solved by some brilliant researchers. Then researchers may use an existing solution or tweak an existing solution to solve the particular/current problem (in our case, flood attacks).
* Brand New Algorithm:- After applying above all activities/steps, researchers try to propose a brand new algorithm (novel) to solve a particular problem (in our case flood attacks).

This section discusses the various strategies of malicious nodes which launch flood attacks (Some of the attack types are already existing flood attacks and some are possible attacks (unique contribution of this article).

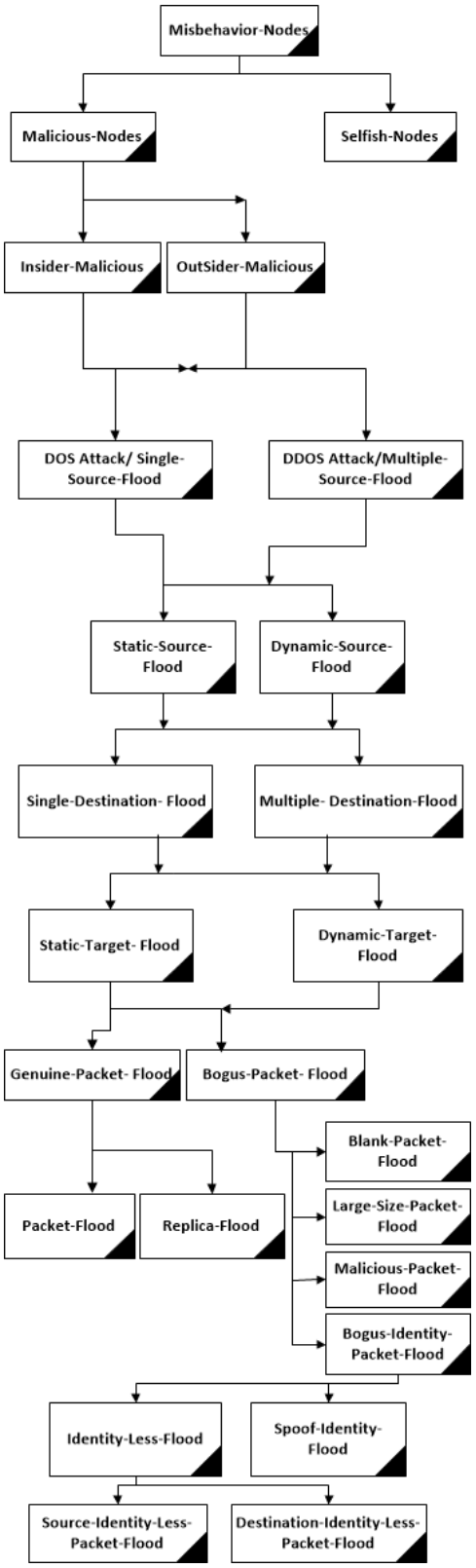

FIGURE 4. Malicious nodes flood attacks taxonomy.

A. MISBEHAVIOR NODES

Ad-hoc Networks routing/forwarding is based on the assumption that the host forwards all packets from other nodes and

TABLE 2. Summery of previously proposed schemes.

Proposed Scheme	Problems/Loop-Holes	Detection Delay/Accuracy	Overhead	Feasibility/Scalability
Central Guard Node Scheme	1. Centralized schemes are not feasible in DTNs 2. Single point of Failure (due to centralized) 3. High Deployment Cost, High false positive ratios 4. Need additional Node for Detection	High/Medium	High	Lower/No
Mobile Guard Node Scheme	1. Extra Node For Detection 2. Detection node move along with packet 3. Not feasible solution in DTNs 4. High Detection Time, High false negative ratios	High/Lower	High	Lower/No
Rate Limit Certificate Scheme	1. High Detection Time due to cross checking 2. Nodes always need to be connected 3. Resources Consumption until detection 4. Low packet delivery ratios	Moderate/Utmost	Low	High/Yes
Encounter Scheme	1. Always need Connected environment 2. High Buffer Consumption (store encounter history) 3. High packet loss ratios (due to buffer overflow) 4. In ability to detects Colluding flood attacks	Moderate/Utmost	Medium	High/Yes
Protocol Based Scheme	1. Inability to detects insider malicious nodes 2. High Cost due to cookies creation and verification 3. Modification of Bundle Protocols, High false negative 4. Work only for specific protocol (not generalized)	Low/Medium	Low	Medium/Yes

does not inject a large number of packets for over-exploitation of limited resources. However, at times certain nodes violate this hypothesis/assumption [34], [54]. A specific node that violates this assumption (launches various attacks) is known as misbehavior node/poorly behaved node [54], [114], [115], [116]. There are two types of misbehavior nodes, which are followed as.

1) MALICIOUS NODES

Nodes in ICV-DTN, which inject a large number of bundles/packets to over-exploit the scarce resources of ICV-DTNS are referred to as malicious nodes (outlined already in this article) [35], [54], [117], [118]. Usually, the behavior of misbehavior malicious nodes are to forward many packets into the networks (sometimes malicious nodes drop(s) bundles/packets to induce attacks). This type of security attack is formally known as a flood/DOS attack, which overuses scarce resources (buffer space, bandwidth, energy resources), and also create nodes' unavailability issues in networks [35], [54]. The detection and mitigation of flood attacks are one of the most difficult issue in ICV-DTNs (already mentioned in this paper). Many researchers proposed various algorithms to fracas flood attacks, however, every algorithm has its merits and demerits (already outlined in this article). So flood attacks mitigation are an open research problem in DTNs.

This article further classified malicious nodes into two types, based on the cryptographic credentials (user-name, key, certificate), which are presented as follow.

a: INSIDER-MALICIOUS/INTERNAL-MALICIOUS NODES

Those nodes which have valid cryptographic credentials, such as valid user-name, valid key, and valid certificate (not expired/forge) are called Insider-Malicious nodes [12]. Detection, prevention, and mitigation of Insider-Malicious nodes are very challenging task in ICV-DTNs [54]. Internal-Malicious nodes can launch flood attacks and their mitigation are not possible through authentication only. Researchers proposed algorithms to detect and mitigate internal malicious nodes. But still, this is a challenging research issue in ICV-DTNs [54].

b: OutSider-MALICIOUS/EXTERNAL-MALICIOUS NODES

Unlike Insider-Malicious nodes, OutSider-Malicious nodes do not have valid cryptographic credentials [12]. Detection, prevention, and mitigation of OutSider-Malicious nodes are easy task as compared to Insider-Malicious nodes. OutSider-Malicious nodes problems/attacks are easily solve by nodes authentication [54].

The Insider-malicious and OutSider-Malicious nodes usually launch two different types of attacks, which are followed as [54].

* DOS-Flood/Single-Source-Flood (SSFA): In this type of attack, a single malicious node launches flood attacks.
* DDOS-Flood/Multiple-Source-Flood (MSFA): In this type of attack, multiple malicious nodes carry out collaborative flood attacks.

The malicious nodes use various strategies to launch SSFA/MSFA attacks. Based on the various strategies this article further categorized SSFA (DOS)/MSFA (DDOS) attacks into two classes, which are presented as follow [35].

- Static-Flood-Attack (SFA): In this category of flood attacks, malicious nodes are static to launch attacks.
- Dynamic-Flood-Attack (DFA): In this kind of attacks, malicious nodes are dynamic (in motion) to initiate attacks.

During flood attacks, multiple nodes can target a single node as well as multiple nodes [54]. From this analysis, this article breaks down such attacks into two different categories.

+ Single-Destination-Flood-Attack (SDFA): In this category, malicious nodes target a single destination. This article further classified this into two categories [54].
  * Single-Source-Single-Destination-Flood (SSSDFA): In this category of flooding, a single source targets a single destination.
  * Multiple-Source-Single-Destination-Flood (MSSDFA): In MSSDFA, multiple malicious nodes target only one destination.
+ Multiple-Destination-Flood-Attacks (MDFA): In this category of flood attacks, malicious nodes always launch flood attacks on multiple destinations, which is further classified into the following categories.
  - Single-Source-Multiple-Destination-Flood (SSMDFA): In this class of flood attacks, a single malicious source node targets multiple innocent nodes to launches flood attacks.
  - Multiple-Source-Multiple-Destination-Flood (MSMDFA): Under this category of flood attacks, several malicious nodes target several benign nodes for catastrophic flood attacks [54].

In either case, single destination or multiple destinations (mentioned above in this article), malicious nodes can launch attacks on static nodes as well as dynamic nodes. This article gives names to these types of attacks, Static-Target-Flood-Attack (STFA) and Dynamic-Target-Flood-Attacks (DTFA) [54].

@ Static-Target-Flood-Attack (STFA): In such flood attacks, the targeted nodes are always static (the attacking nodes are static and dynamic, both categories are possible, however, the targeted nodes are always static) [54].
@ Dynamic-Target-Flood-Attack (DTFA): Within this category of flood attacks, targeted innocent nodes are always dynamic, but intruder nodes may be dynamic or static (both cases are possible).

As mentioned previously in this article, the invading nodes' target either dynamic nodes or static nodes. However, malicious nodes use various types of packets to target innocent nodes. Based on this findings (bundles/packets), this article categorized flood attacks into the following categories.

@@ Genuine-Packet-Flood-Attack (GPFA):- In GPFA, malicious intruder nodes use genuine packets (packets that have a valid format, bitsize, control information, valid size payload, valid header, time-stamp, and signature) to launch attacks. Sometimes intruder nodes use different packets and sometimes use the same packets (replica of the original packet) to launch flood attacks [35], [54]. Based on this analyses this article further categorized GPFA into the following two categories.
  - Packet-Flood-Attack (PFA):- In PFA, the attacker nodes send/forward large number of different packets [28], [83], [84].
  - Replica-Flood-Attack (RFA):- In this category of attacks, intruder nodes forward a large number of replicas (copies) of the same packets [28], [83], [84].

@@ Bogus-Packet-Flood-Attacks (BPFA):- Unlike in GPFA, in this category of attacks, malicious nodes use bogus packets (which do not have valid packet size, header information, payload, etc) to launch catastrophic flood attacks. According to our knowledge, the researchers did not identified BPFA, however, according to the studies of this article BPFA attacks are quite possible. This article further classified BPFA into the following four categories.
  + Blank-Packet-Flood (BLPFA):- In this category of flood attacks, attackers launch attacks with blank packets to waste the processing resources of benign nodes.
  + Large-Size-Packet-Flood (LSPFA):- In this type of attack, the attacker launches attacks by large packet size to overuse scarce resources (buffer, bandwidth, and energy) of innocent nodes.
  + Malicious-Packet-Flood (MPFA):- In this category of attacks, intruder nodes launch attacks by malicious packets [34] like Botnet on the Internet, which divert the behavior of innocent nodes.
  + Bogus-Identity-Packet-Flood (BOIPFA):- In BOIPFA, the attackers use a bogus identity to launch flood attacks. This article further classified BOIPFA Attacks into the following two categories.
    * Identity-Less-Packet-Flood (ILPFA):- In this kind of attack, the malicious nodes discard identity (Address) from the packets header to launch flood attacks. Malicious nodes either discard source identity information or destination identity information from packets to launch attacks. Based on this observation, this article further classified ILPFA into the following categories.
      @ Source-Identity-Less-Packet-Flood (SILPFA):- In this category of attacks, malicious nodes discard their own identity from the packets.
      @ Destination-Identity-Less-Packet-Flood (DILPFA):- In such a category, malicious nodes discard the destination identity from the packets. There are two possibilities according to the studies of this article, malicious nodes either discard the identity of the destination, then forward packets, which overuse innocent nodes' resources, or malicious nodes use bogus destination identity to launch attacks [85]. The packets will travel but do not reach the destination, which overuse the scarce resources of

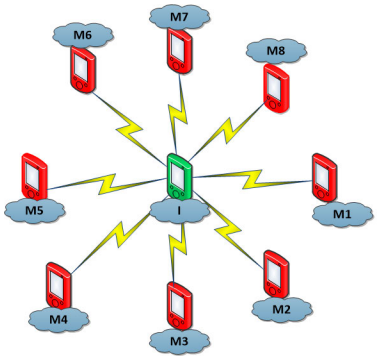

FIGURE 5. MMSLFA/wicked-flood-attack (WFA).

innocent nodes (a lot of bandwidth consumption) [34], [35], [54].

* Spoof-Identity-Flood Attacks (SIFA):- In SIFA, attackers use the identity of other nodes in the networks to launch flood attacks [85].

2) SELFISH NODES

A specific category of misbehaving nodes, which drop(s) packets are known as selfish nodes [34]. There are so many reasons for packet drop(s). Few nodes drop(s) packets due to memory overloading, insufficient processing power, hardware/software issues (all those nodes are innocent, not selfish) [35], [54]. However, some nodes intentionally drop(s) packets due to selfish behavior (There are various categories of selfish nodes). Such as Wicked-Selfish (Nodes which have free buffer space and sufficient processing/forwarding capability, but drop(s) packets are known as Wicked-Selfish nodes) [54]. Wicked-Selfish are further classified into Deaf-Dumb-Selfish (intentionally do not receive packets from forwarder nodes to save its resources) and hypocritical-Selfish nodes (a type of selfish nodes which received packets from forwarder nodes, but silently drop(s) packets to save their processing/forwarding power/energy) [54].

Fig. 4 shows unique taxonomy of malicious nodes which launch flood attacks.

VII. ANALYSES (ANALYTIC AND QUANTITATIVE ANALYSES OF FLOODING ATTACKS)

This section analyzes/summarizes the related works and various flood attacks scenarios on our proposed parameters rigorously. Literature reviews on flood attacks are summarized in Table 3 and Table 4 [35], [54]. The following parameters were used to analyze and evaluate the related works [54].

- Detection Procedure:- This parameter discusses the detection procedures of previously proposed algorithms (Researchers proposed various detection procedures to cope with misbehaving nodes).
- Mitigation:- In this parameter, this article discusses the mitigation of proposed algorithms (which are different in various proposed mitigation schemes).
- Drawback:- Shortcomings of the previously proposed detection schemes are highlighted in this parameter.

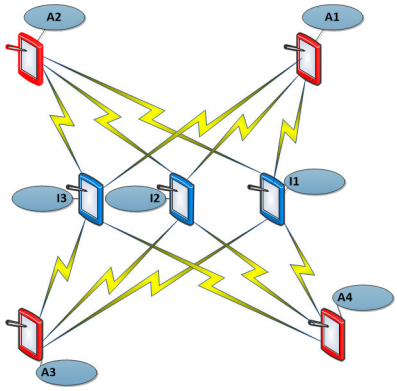

FIGURE 6. MMMLFA/collaborative-flood-attack (CFA).

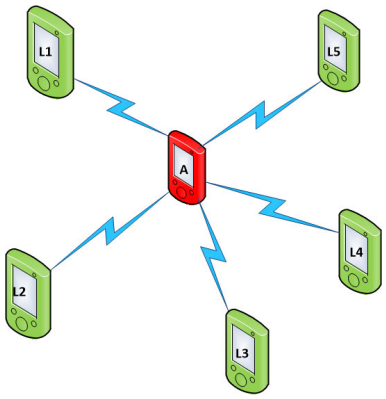

FIGURE 7. SMMLFA/super/bold-flood-attack (S/BFA).

- Algorithm Type:- Researchers proposed broadly two types of algorithms (Centralized and distributed) to cope with misbehaving nodes, which launch flood attacks. In centralized schemes, one node is responsible for attacks detection, unlike distributed schemes in which many nodes collaborate to detect flood attacks (already outlined in this article). In this parameter, this article categorized various detection algorithms types.
- Practical Implementation (Deployment):- This parameter analyzes the practical implementation of the proposed schemes. This article categorized previously proposed schemes into three categories i.e Low, medium, and high.
- Strategy:- This parameter analyses the strategies of previously proposed algorithms, this article classified strategies into four groups i.e good, better, best, and average.
- Detection Methodology:- In this parameter this article analyzed the detection methodology of various proposed algorithms for flood attacks (which is different in various proposed algorithms)
- Classification (According to Proposed Taxonomy):- This parameter classifies previously proposed algorithms according to the proposed taxonomy of this article.

TABLE 3. Analyses of previously proposed mitigation algorithms 01.

Paper	Algorithm Type	Deployment	Strategy	In our Taxonomy	Detection Methodology
[86]	DNBMA	Medium	Better	DNBMS /DA/PBDS /ERPBD	Detects Malicious Nodes with number of encounters and number of forwarded packets
[85]	CNBMA	Low	Better	CNBMS /DNBD /NGNBD /SNGNBD	Attacks detector node counts packets of all nodes to detect attacks.
[29]	DNBMA	High	Best	DNBMS/PA /CBDS	All nodes cross checks RLCs to detects flood attack.
[95], [97]	DNBMA	Low	Average	DNBMS/PA /CBDS	All nodes cross checks RLCs along with AES/ RSA to detects attack.
[96]	DNBMA	Low	Average	DNBMS/PA /CBDS	All nodes cross checks RLCs along with MySql and DNS query to detects flood attack.
[46]	DNBMA	Medium	Better	DNBMS /DA/PBDS /APBD	Protocol based detection. Nodes verify pre-defined packets format to detect flood attack.
[88]	DNBMA	Medium	Good	DNBMS/DA/ RBDS	Nodes compare pre-defined threshold value to detect attack.
[90]	DNBMA	High	Best	DNBMS/DA /ESBD /EHBD	Nodes checks encounter record along with RLCs to detects flood attack.
[89]	CNBMA	Low	Average	CNBMS /DNBD /NGNBD /MNGNBD	Specific node in networks compares actual delivery probability with estimated delivery probability to detect flood attack.
[36]	DNBMA	High	Better	RTOC:-	RTOC:
				DNBMS /PA/CBDS	All nodes cross checks RLCs to detects attacks.
				IFAM:- DNBMS/PA /IPS/SBIPS /SGBIPS/SNSS	IFAM: IDS in Some nodes counts packets to detect
				HFAM:-	HFAM: (IDS in all nodes)
				DNBMS/PA /IPS/SBIPS /SGBIPS/MNSS	

A. ATTACKS SCENARIOS/DEMONSTRATION OF VARIOUS FLOOD ATTACKS SCENARIOS

The misbehaved nodes use various strategies to launch flood attacks. For illustration purposes, this article considers three attacks scenarios. Multiple-Malicious-Sole-Legitimate-Flood-Attacks (MMSLFA), Multiple-Malicious-Multiple-Legitimate-Flood-Attacks (MMMLFA), and Sole-Malicious-Multiple-Legitimate-Flood-Attacks (SMMLFA) [54].

* MMSLFA:- In this category of flood attacks, multiple malicious nodes target one legitimate/innocent node. This article calls this Wicked-Flood-Attack (WFA). Consider an attack scenario of malicious nodes in Figure 5. "M1", "M2", "M3", "M4", "M5", "M6", "M7", and "M8" are malicious nodes, which target one legitimate node "I" to launch flood attacks.
* MMMLFA:- Within this category of flood attacks, multiple malicious nodes target multiple legitimate nodes. Consider second attack scenario in Figure 6. "A1", "A2", "A3", and "A4" are malicious attacker nodes, which target legitimate nodes "I1", "I2", and "I3" to launch flood attacks. This article gives a name to this type of attack as Collaborative-Flood-Attack (CFA).
* SMMLFA:- In this class of flooding attacks, one malicious node targets multiple innocent nodes. Consider a third attack scenario in Figure 7. "A" is malicious attacker node, which targets legitimate nodes "L1", "L2", "L3", "L4" and "L5" to launch flood attacks. This article calls this attack as Super/Bold-Flood-Attack (S/BFA).

1) OBSERVATIONS AND RESOURCES CONSUMPTION OF FLOOD ATTACKS SCENARIOS

As already pointed out in this article that DTNs have scarce/limited resources, however, due to flood attacks, too

TABLE 4. Analyses of previously proposed mitigation algorithms 02.

Paper	Detection Procedure	Mitigation	Drawback
[86]	Nodes which encounter infrequently and forward large number of packets.	Few buffer spaces are allocated to malicious nodes. Proposed formula which deletes packets from memory to enhance packet delivery ratios.	Proposed for specific routing protocol (Prophet), high false positive/false negative ratios.
[85]	Designated node (DN) defines threshold for all nodes. DN counts packets of all nodes, if node violate, DN detects flood attacks.	Black-list malicious nodes.	All packets pass through one designated node, which is impractical in ICN, due to intermittent connectivity.
[29]	All nodes have RLCs. All nodes forward packets along with RLCs and message claims (MCs) (how many packets they already forwarded).Destination cross check MCs to check validity of MCs	Black-list malicious nodes.	High detection time due to cross checking. High resources consumptions due to high detection time, which further dis-improves PDR/PLR. If TA compromised then whole network compromised (Single point of failure).
[95], [97]	Same scheme like , AES/RSA key	Black-list malicious nodes.	No need of AES/RSA, burden of AES
[96]	Same scheme like , only add MySql database and DNS query along with .	Detects application level flood attacks, which consumed server resources. Black-list intruder nodes which launches this attack.	Due to the intermittent connectivity most of attacker launches Network level flood attacks which is not detected in this scheme.
[46]	Generate/Check Cookies (Source-ID, Time-Stamp, Random-Number) to detect malicious nodes, which do not have valid cryptographic credential.	If Cookies verification failed, those malicious nodes are Black-listed	Detects only outsider malicious nodes (which do not have valid cryptographic credential). Insider malicious nodes are not detected in this scheme.
[88]	Node creates/forwards genuine packet to TA, TA assign specific threshold/reputation value. All nodes check reputation value before accepting messages from particular node	Destination node check reputation of forwarder node before accepting messages, when reputation value is less than pre-defined threshold value, destinations do not accept packets	If malicious node creates genuine message so in this case TA assign reputation, if not why not (High false positive/false negative). How TA recognized between fake packets and genuine packets? Ideal preventive.
[90]	Piggy back encounter record scheme. Add encounter record with . Share encounter history with all nodes to detects various attacks.	If malicious nodes forge encounter record, so receiver node easily detect this (due to inconsistency in encounter record), and Black-list malicious nodes	High detection time, because do not detects malicious nodes until sharing encounter history. Also it consume more resources due to encounter history sharing, which causes high packet loss ratios and low packet delivery ratios
[89]	Stream node (SN)) move like patrolling police, SN has three tables. SN compare actual delivery probability with calculated delivery probability to detects attacks	Black-list malicious nodes.	Hard to practically implement in intermittently connected networks due to intermittent connectivity. Also high false positive/false negative rates.
[36]	This article proposed three algorithms, RTOC, IFAM, HFAM. RTOC is the enhance version of , which compress packets to improves resources consumption. In IFAM IDS is deployed in some nodes which counts packets to control malicious nodes. In HFAM, IDS are deployed in all packets, MAC is generated to mitigates attacks.	Black-list malicious nodes in all three algorithms after detection	RTOC have high detection time. High cost and single point of failure (if TA key compromised), so in this case IFAM will failed. If malicious nodes guess/calculate IDS key in HFAM, so in this case HFAM will failed.

many benign nodes resources are consume. The scarce resources includes, TBCs and TBWCs. Also, PDRs and PDRs are dependent upon resources consumption. TBCs are directly proportional to ''NumberOfPackets'' under some constant value [35], [54]. Also, TBWCs increase with ''NumberOfMessages'' up to some certain limit (depends on constant value) [35], [54]. Furthermore, ''NumberOfMessages'' are directly proportional to ''NumberOfNodes'' [35], [54]. However, when the nodal TBCs become maximum/high, the availability of nodes therefore become minimum/low, which are inversely linked. This is due to the fact, that nodes can neither process incoming messages nor accept/accommodate other messages/packets in memory. So this further implies, that victim nodes become unavailable for all other nodes in networks [35]. Moreover, TBCs are directly proportional to PLRs [35]. Based on these findings, the Table 5 is created, which summarizes buffer consumption, bandwidth consumption, availability, and message delivery/loss ratios in various attacks scenarios (already mentioned in this article) [35], [54].

B. ANALYTIC ANALYSIS OF VARIOUS FLOOD ATTACKS SCENARIOS

As already stated in the attacks taxonomy section of this article, there are various types of flood attacks. This section

analytically analyzes a few flood attack scenarios for illustration purposes [35], [54].

1) DESCRIPTION OF TABLE 5

Table 5 is created on the basis of analyses and observations. This article will simulate attacks scenarios in the future to calculates the exact resources consumption used in Table 5.

In attack scenario one (MMSLFA/WFA), when multiple malicious nodes target one node so TBCs will be the maximum of that particular legitimate node. Because several attacking nodes are routing multiple packets simultaneously to a single node, which completely destroy the buffer of that particular node [35], [54]. If TBCs will be maximal, then this particular node becomes completely unavailable for other nodes. Moreover, due to attacks, benign nodes will be unable to accept a single packet from other nodes, resulting in low PDRs and high PLRs. Furthermore, TBWCs between malicious and legitimate nodes will be medium (TBWCs between one malicious and one legitimate node will be consume medium) [35], [54].

In attack scenario two (MMMLFA/CFA), when multiple malicious nodes target several benign nodes, TBWCs will be high. Because several malicious nodes route multiple packets to several innocent nodes, this will consumes the maximum bandwidth between the nodes [35], [54]. TBCs will be Moderate for that particular node, because the probability of malicious nodes forwarding packets to legitimate nodes are almost fifty percent approximately, unlike in attack scenario one, which was maximum. If almost fifty percent buffer is consumed so availability will be fifty percent approximately of that particular node (this article does not consider that case in which multiple malicious nodes target one node) [35], [54]. This analyses further imply that the node is partially available (not completely down) for other nodes. If node buffers are consumed at almost fifty percent, this implies that the PDR and PDR will be medium [35], [54].

In attack scenario three (SMMLFA/BFA), when a single malicious node targets multiple legitimate nodes, TBWCs and TBCs between malicious and legitimate nodes will be low. For justification purposes, consider an attack scenario in which one malicious node targets five legitimate nodes. If the transmission capability of a malicious node is five, the malicious node probably routes a packet to all the nodes (single packet to all nodes). So TBCs will be low, which further imply that PDRs and PLRs will be less affected [35], [54]. PDRs will be high-middle (above the middle and below the maximum) and PLRs will be low in this case. Additionally, this also means that the particular node will be available for other nodes [35], [54].

C. SIMULATION/QUANTITATIVE BASED ANALYSIS OF VARIOUS FLOOD ATTACKS SCENARIOS

This section will analyses various flood attacks scenarios. This article consider four attack scenarios for simulation based analyses (This article evaluates PDRs/PLRs, and TBCs for simulation based analyses, the use cases are already mentioned in attack taxonomy section of this article) [35], [54]. This includes SSSDFA, SSMDFA, MSSDFA, and MSMDFA. The ratios of misbehavior nodes and benign nodes are vary from case-to-case, which are followed as, SSSDFA (1:1), SSMDFA (1:4), MSSDFA (4:1), MSMDFA (4:8) [35], [54]. The ratios of message/packet creation interval (messages forwarding interval) between benign and misbehavior intruder nodes are 1:4 [35], [54]. Opportunistic Network Environment (ONE) [119] simulator is used for simulation which is specifically designed for DTNs.

1) SIMULATION SETUP

The simulation is performed with specific-parameters which are summarized in Table 6. This article consider two scenarios for each approach: Epidemic WithOut Malicious nodes (EWOM (Without malicious nodes means without flood attacks)), and Epidemic With Malicious nodes (EWM (With malicious means in which malicious nodes launches flood attacks)), First Contact WithOut Malicious nodes (FCWOM), First Contact With Malicious nodes (FCWM), Direct Delivery WithOut Malicious nodes (DDWOM), Direct Delivery With Malicious node (DDWM), SprayAndWait WithOut Malicious node (SWWOM), and SprayAndWait With Malicious node (SWWM) [35], [54].

2) EVALUATION METRICS

Simulation is performed with evaluation metrics below.

* Packet/Message-Delivery-Ratios (P/MDRs): P/MDRs are the ratios between total delivered messages to total generated messages in the simulation. If the Total-Delivered-Messages are TDM and Total-Generated-Messages are TGM then P/MDRs will be calculated with following equation.

$$\text{P/MDRs} = \text{TDM}/\text{TGM} \tag{1}$$

* Packets/Messages-Loss Ratio (P/MLRs): P/MLRS are the number of total drop messages in the simulation. P/MLRs will be calculated as follows.

$$\text{P/MLRs} = (\text{TGM} - (\text{TDM}))/\text{TGM} \tag{2}$$

* Total-Buffer-Consumption (TBCs): It is the total buffer-space consumed during the simulation (calculated with particular time/any time). If Buffer-Space-Consumption (BSC/BCs), Total-Buffer-Space (TBS), and Unused-Buffer-Space (UBS) then buffer consumption will be calculated as follows.

$$\text{BSC/BCs} = (\text{TBS - UBS}) \tag{3}$$

3) SIMULATION RESULTS

Simulation Results demonstrate that due to misbehaving flooding attacks, the MDRs are decreased while MLRs are increased under all evaluated routing protocols (For illustration purposes this article only shows simulation results of MDRs only, MLRs will be easily calculated from eq. 2. This article calculated MDRs in percentage like [35], [54], and [34].

TABLE 5. Analytic analyses of flood attacks.

Attacks Scenarios	Bandwidth-Consumption	Buffer-Consumption	Availability	Packet-Delivery-Ratio	Packet-Loss-Ratio
MMSLFA/WFA	Average	Utmost	Not available	Minimum/Almost-zero	Maximum/Top-Level
MMMLFA/CFA	Uttermost	Intermediate-Level	Partial availability	Mediate	Intermediate-Level
SMMLFA/BFA	Medium	Low	Highly Available	High Middle	Low-Level

TABLE 6. Simulation parameter stable.

ParameterName	AssignValue	ParameterName	AssignValue
SimulationTime	50,000	WaitTime	0-120 Seconds
MovingSpeed	1-1.6	UpdateInterval	0.1 Seconds
TransmitRange	10Meter	TimeToLive	300 Seconds
Bandwidth	2Mbps	MobilityModel	RandomWayPoint
BufferSpace	5MB	NodesStatus	Mobile
NumberOfGroup	2	SimulationArea	500 by 500

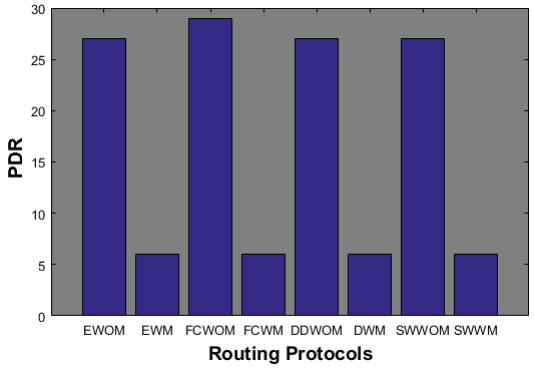

FIGURE 8. Impact of SSSDFA on MDRs.

Figs 8 shows MDRs of SSSDFA, where simulation results show that approximately 25 to 30 percent of MDRs are decreased and MLRs are increased due to misbehavior flooding attacks [35], [54]. Moreover, SSSDFA almost have same effect on all evaluated routing algorithms [35], [54].

Figs 9 illustrates MDRs of SSMDFA. Simulation Results show that due to SSMDFA, almost 40 to 58 percent MDRs are decreased, and MLRs are increased.

The Fig 10 shows simulation results MDRs of MSSDFA. Results show that flood attacks have 35 to 40 percent decreased in MDRs. The effect of MSSDFA are almost the same in all evaluated routing algorithms (FirstContact is slightly below 35 percent) [35], [54].

Fig 11 shows the impact of malicious nodes flooding attack on MDRs in MSMDFA. The simulation results graph clearly demonstrate that due to MSMDFA, MDRs are decreased while MLRs are increased [35], [54]. It is clear from simulation results that due to MSMDFA, MDRs are decreased from 2 to 18 percent approximately [35], [54].

As mentioned earlier in this article that due to misbehaving nodes flooding attacks buffer-space of benign nodes are consumed. Due to this BSCs, MDRs are decreased while MLRs are increased [35], [54] (already proved in this article).

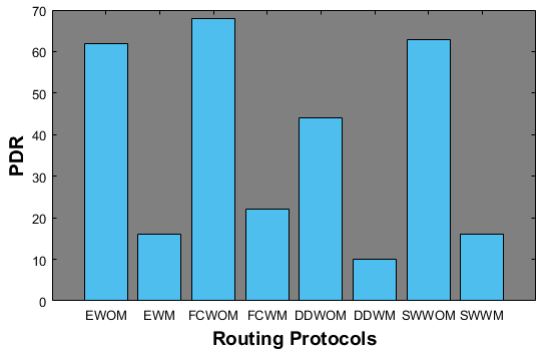

FIGURE 9. Impact of SSMDFA on MDRs.

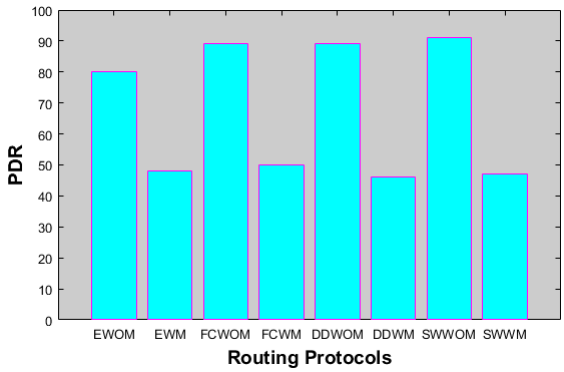

FIGURE 10. Impact of MSSDFA on MDRs.

This article simulates SSSDFA, SSMDFA, MSSDFA, and MSMDFA to calculates BSCs (for illustration purpose this article only shows simulation results of SSMDFA and MSSDFA, other categories show similar simulation results) [35], [54]. During initial set-up of the simulation, every node has assign 5M buffer-space. This article calculates BSCs with various time in simulation, however, for demonstration this article only shows simulation results of BSCs after 4100 seconds in simulation (BSCs are increased with increased in simulation time which is quite obvious) [35], [54]. Also, for demonstration purposes this paper simulates BSCs for EpidemicRouter, all other routing protocols shows similar results [35], [54].

Fig 12, and Fig 13 illustrate simulation results of BSCs in SSMDFA and MSSDFA respectively. The horizontal-side of the simulation graph represents various nodes in scenario, and the vertical-side represents the BSCs in various flood attacks in Bytes. In horizontal-side, node in simulation are given specificIdentifier (SIDs), that is S0, S1, S2, R1, R2 etc.

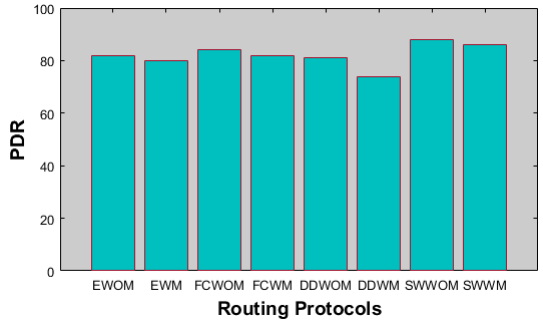

FIGURE 11. Impact of MSMDFA on MDRs.

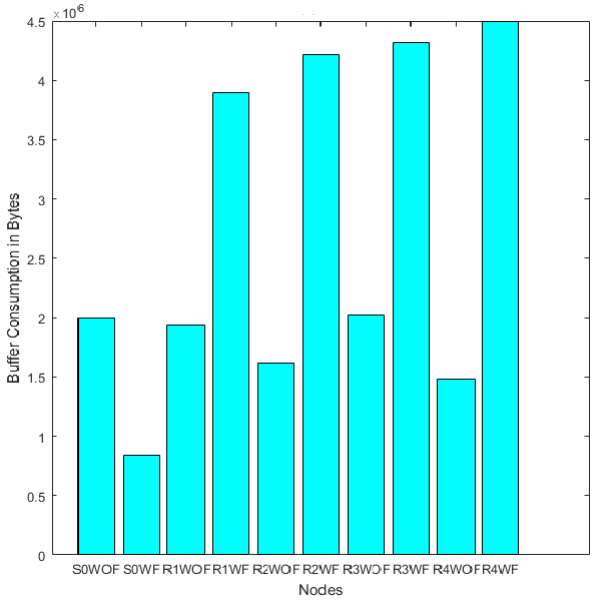

FIGURE 12. Impact of SSMDFA on BSCs.

S0 with out flood Attack (S0WOF), S0 with flood Attack (S0WF), R1 without Flood Attack (R1WOF), R1 With Flood Attack (R1WF), etc. Simulation results clearly illustrate that due to flooding attacks buffer are consumed of all nodes in the simulation. The simulation results clearly indicate that due to flood attacks almost 2MB to 3.2MB and 1.8MB to 3.5MB extra buffer are consumed in case of SSMDFA and MSSDFA respectively [35], [54]. Due to this extra buffer consumption (due to flooding attacks) the MDRs are significantly decreased, while MLRS are increased (already mentioned, prove is already given in this article by simulation results) [35], [54].

D. COROLLARY FROM ANALYSES

This article looks critically at node attacks that behave badly. From these few analyses, this article concluded that node buffers-space have a direct impact on delivery ratios/loss ratios. If a particular node in the networks consumes minimal buffers-space, so it will improve drop(s) ratios. Furthermore, the ratios of PDRs will be maximum. Moreover, according

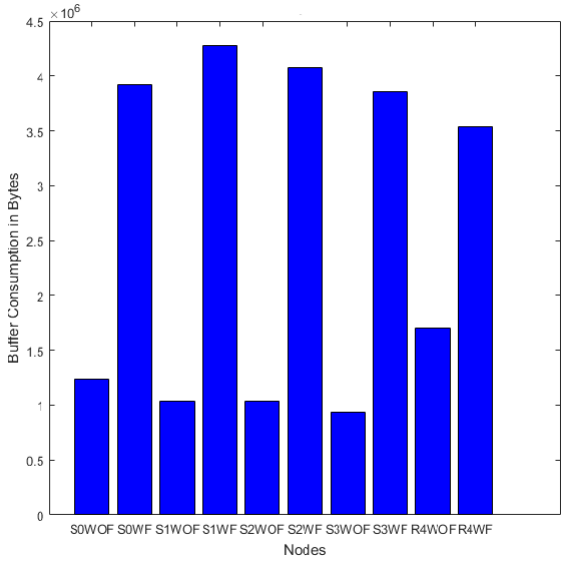

FIGURE 13. Impact of MSSDFA on BSCs.

to this article's studies, resources consumption depend on the size of the packets and the number of packets. This article concluded if researchers either reduce messages/packets size or prevent a large number of packets, this will enhances the ratios of PDRs/PLRs.

In addition, some researchers detect nodes of poor behavior (PRLS and ER schemes), but the detection precision of the proposed algorithms are not very accurate. The detection of proposed algorithms depend on nodes encounter-time and encounter/contact-duration. According to the findings of this article, if researchers design algorithms that improve nodal encounter-time and encounter-duration (if researchers propose some new detection methods other than previously proposed methods such as packet-claims exchange and encounter-history sharing), it will probably enhance attacks detection accuracy, which will further improve resources consumption (this will further enhance PDRs/PLRs).

E. CALCULATION OF BUFFER CONSUMPTION

As mentioned earlier in this article, most of the researchers claim that due to flood attacks nodes' buffers are consumed, however, researchers did not mention how much buffers are consumed, and how to calculate buffers consumption in real simulation. This article demonstrates how to calculates the buffer consumption in the actual simulation. As an illustration, this article shows the Epidemic-Router buffer consumption code with simulation time (Simulation time defined in code, this code calculates the node buffer consumption with different simulation times). Figure 14 shows buffers consumption simulation code.

VIII. OPEN RESEARCH LOOP-HOLES (PROBLEMS)

There are so many research issues that are already discussed in this article. Following are some of the open research issues

```
/*
 * Copyright 2010 Aalto University, ComNet
 * Released under GPLv3. See LICENSE.txt for details.
 */
package routing;

import core.*;

import java.io.*;
/**
 * Epidemic message router with drop-oldest buffer and only single
transferring
 * connections at a time.
 */
public class EpidemicRouter extends ActiveRouter {

    /**
     * Constructor. Creates a new message router based on the settings in
     * the given Settings object.
     * @param s The settings object
     */
    public EpidemicRouter(Settings s) {
        super(s);
        //TODO: read&use epidemic router specific settings (if any)
    }

    /**
     * Copy constructor.
     * @param r The router prototype where setting values are copied from
     */
    protected EpidemicRouter(EpidemicRouter r) {
        super(r);
        //TODO: copy epidemic settings here (if any)
    }

    @Override
    public void update() {

    if (SimClock.getIntTime()==4500//SimulationTime here for
BufferConsumptio) {

    File file=new File("C:\\Users\\This-PC\\Desktop\\one_1.4.1\\reports\\
file.txt");
    int sze=this.getBufferSize(); // Total Buffer Size of nodes will be save in
variable sze.
    int fr=this.getFreeBufferSize(); // Free Buffer Size which is not consumed
will be save in fr.
    int tot=sze-fr;//Total BufferSize-FreeBufferSize, will get consumed buffer
will be stored in tot.
    String totl=Integer.toString(tot);
    BufferedWriter bw=null;
    FileWriter fw=null;

    try {
    fw=new FileWriter(file.getAbsoluteFile(),true);
    bw=new BufferedWriter(fw);
    bw.write("\n"+this.getHost()+totl); // will calculates consumed buffer space
of particular node.
    }
    catch (IOException e) {
    e.printStackTrace();
    }
    finally {
    try {
    bw.close();
    fw.close();
    }catch (IOException ex) {

    ex.printStackTrace();
    }
    }


    }

        super.update();
        if (isTransferring() || !canStartTransfer()) {
            return; // transferring, don't try other connections yet
        }

        // Try first the messages that can be delivered to final recipient
        if (exchangeDeliverableMessages() != null) {
            return; // started a transfer, don't try others (yet)
        }

        // then try any/all message to any/all connection
        this.tryAllMessagesToAllConnections();
    }


    @Override
    public EpidemicRouter replicate() {
        return new EpidemicRouter(this);
    }

}
```

FIGURE 14. Buffer consumption calculation codes, epidemic router.

in the broad areas of vehicular networks security and particularly malicious nodes, which launch flood attacks [35], [54].

A. REVISED DEFINITION OF FLOOD ATTACKS

As outlined earlier in this article, most researchers have a view that there are two types of flood attacks, i.e Packet-Flood-Attacks, and Replica-Flood-Attacks. However, according to the findings of this article, there are so many other categories of flood attacks. Most of the researchers in the literature proposed detection/mitigation solutions for the above two attacks (did not detect various categories of flood attacks). Also, most of the researchers have the opinion that flood attacks mitigation are top among (the most difficult problem to handle) in various attacks in this research domain. However, according to the studies in this article, if researchers properly define flood attacks (revised the definition of flood attacks), therefore, the solution for flooding attacks are not very difficult (at least if researchers try to solve the sub-categories of flood attacks, so it will be a good solution in this security research domain).

B. MITIGATION TIME

Most researchers detect flood attacks by sharing packet-claims (rate limit certificates with packet-claims) along with original packets. Also, few researchers proposed, sharing encounter-history packets with all nodes in the networks (encounter history-based algorithms) for the detection of flood attacks. However, due to the intermittent connectivity, previously proposed schemes suffered from long detection delay, which further cause high packet loss ratios and low packet delivery ratios until detection [54]. Therefore, an efficient detection/mitigation time is still an open research issue in this security research domain.

C. RESOURCES CONSUMPTION

As mentioned earlier in this article that few researchers proposed very efficient algorithms to thwart with malicious nodes which launch flood attacks with encounter-history sharing. However, this category of networks have scarce resources (buffer, energy resources) [120], [121]. If mitigation schemes share encounter-history packets along with original packets, this ultimately consumes more resources (particularly buffer). Buffer consumption has a direct relation with packet delivery ratios and packet loss ratios [35], [54] (consumes buffer which further degrades network due to low packet delivery ratios and high packet loss ratios). Therefore, resource efficient detection/mitigation algorithms are still an open research issue in flood mitigation in intermittently connected vehicular networks.

D. GENUINE CRYPTOGRAPHIC INFORMATION

Few researchers proposed protocol-based detection schemes [45], which weed-out those malicious nodes which have invalid cryptographic credentials (key, outsider intruder nodes) [122]. However, intruder nodes that belong to networks (insider attacker nodes that have a valid key) are not detected in this scheme. Therefore, researchers need to

propose algorithms that can thwart insider malicious nodes (open research problem).

E. DETECTION WITH THIRD PARTY NODE

Most of the researchers proposed algorithms that detect malicious nodes with third-party nodes (trusted authority (TA)) [54]. TA distributes RLCs and keys, this will be very difficult to deploys an intermittently connected environment due to the frequent disconnection of nodes. Also, if TA is compromised so the whole network will be compromised (single point of failure). Therefore, detection with a third-party nodes are a very important issue to be revised.

F. CENTRALIZED DETECTION SCHEMES

Some of the researchers in the literature proposed centralized-based algorithms to glitch malicious nodes (single node which is responsible for the detection of flood attacks). As mentioned earlier in this article that there are two broad categories of centralized-based schemes i.e static guard-node and mobile guard-node. In the former category, all packets pass through this node, and in later category guard node moves with all packets [54]. According to the analyses of this article, both categories are very difficult to practically deploy in an intermittently connected environment. So therefore it is urgent to revise centralized detection schemes (open research problem)

G. DETECTION OF FLOOD PACKETS RATHER THAN MALICIOUS NODES

Most of the researchers proposed detection algorithms that detect/mitigate malicious nodes which launch flood attacks. However, according to the verdicts of this article, negligible works are noted to detect malicious packets rather than malicious nodes [23], [123]. According to the findings of this article, if researchers proposed malicious packet detection schemes rather than malicious nodes detection schemes, therefore it will be an efficient algorithms. Therefore, malicious packets detection are still an open research problem in this security domain.

H. CALCULATION AND DISTRIBUTION OF REPUTATION/THRESHOLD

Few researchers proposed detection algorithms based on reputation/threshold. Researchers proposed various strategies to calculate/distribute reputation/threshold, that is global reputation, and personalized reputation [54]. In global reputation schemes, TA calculates nodal reputation values from all nodes in the networks, while in personalized reputation schemes TA calculates reputation from specific group nodes in the networks. This is a very challenging tasks due to intermittent connectivity and may be biased (which may have high false positive and false negative ratios). Therefore, the calculation and distribution of reputation/threshold is still a very challenging research problem in intermittently connected networks.

I. TRADE-OFF BETWEEN DETECTION COST AND DETECTION ACCURACY

Few researchers proposed mitigation schemes, which need extra nodes for the detection and mitigation. For example, Rate-limit-Certificate-based schemes need an extra node i.e TA for the creations and distributions of certificates (extra node costs, certificate creations, and distributions costs). Also, the proposed schemes verify the certificate (verification cost). Guard-node-based detection schemes need an extra node for the detection (extra node costs, that is guard-node). Nonetheless, few researchers proposed schemes that do not need an extra node for the detection. However, this category of schemes are not very accurate (low detection accuracy and high value of false positive/false negative) as compared to TA/certificate-based schemes, which have high detection accuracy [34], [35], [54]. As such, there is a need to see a trade-off between detection cost and detection accuracy.

J. COLLUDING ATTACKS DETECTION

Few researchers proposed very efficient algorithms to counter malicious nodes which launch catastrophic flood attacks. However, if malicious nodes launch colluding flood attacks (a type of flood attacks in which malicious nodes launch flood attacks with collaboration), this category of attacks are not detected in previously proposed algorithms [54]. Therefore, an efficient algorithms are required to handle colluding attacks (very difficult to detect). Therefore, colluding attacks detection are still an open research problem in ICV-DTNs.

K. TRADE-OFF BETWEEN DETECTION AND PREVENTION

As mentioned earlier in this article that few researchers proposed very good schemes to mitigate malicious nodes. However, the detection time of all those algorithms are very high, which ultimately cause resources consumption, this further dis-improves packet delivery ratios/packet loss ratios. According to the analyses of this article, preventive-based algorithms are a remedy for the detection time improvement [35], [54]. Furthermore, preventive-based algorithms have lower cost than detective-based algorithms (no need for extra nodes for detection). Apart from these issues, preventive-based algorithms solve the most important problem of intermittently connected networks (disconnection of nodes, in preventive-based algorithms frequent disconnection have no impact) However, the design of an efficient preventive-based algorithms are difficult, therefore it is still an open research problem for researchers in ICV-DTNs.

L. DESIGN INTRUSION DETECTION BASED ALGORITHMS (IDBA)

Like preventive-based algorithms, IDBA are a very good idea to hitch catastrophic flood attacks in ICV-DTNs. Because they improve detection time (no need for sharing rate limit certificates and encounter history), have a low cost (no need for extra node for detection), and no need for extra information in packets for detection [35], [54]. Also, according

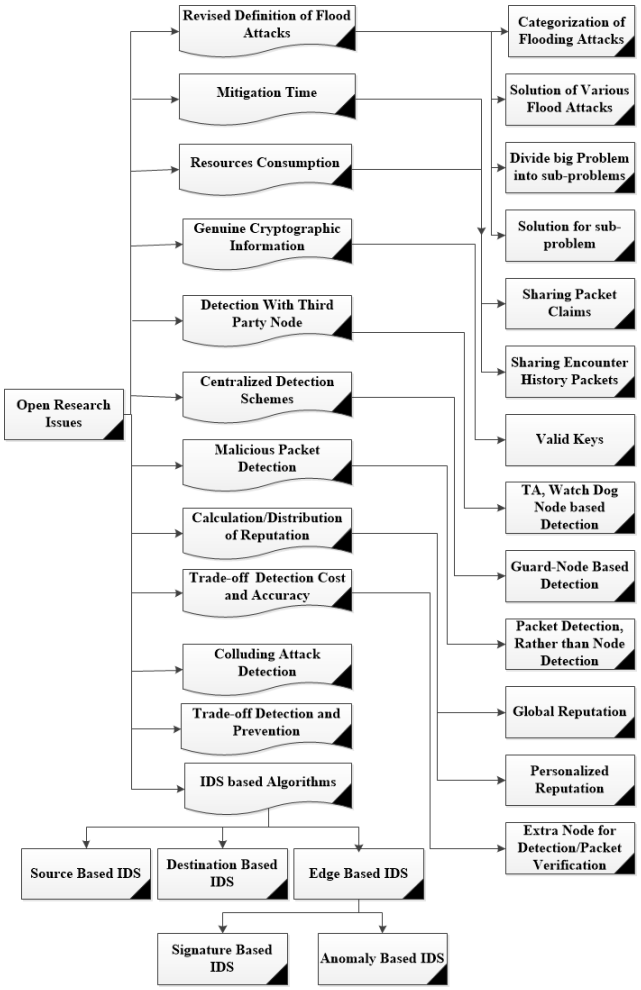

FIGURE 15. Open research issues.

to the studies of this article, IDBA significantly improve false positive/false negative ratios. Apart from this, IDBA are a very good idea for ICV-DTNs because they detect various attacks without connectivity of all nodes (this is very important because we know that intermittent connectivity is the biggest issue, and most of the detection schemes suffer from intermittent connectivity (high false positive/false negative ratios due to disconnection). However, the design of a low-cost and an efficient IDBA are still a very challenging issue, therefore, it is urgent to propose an efficient IDBA for flood attacks mitigation in ICV-DTNs. Fig. 15 shows various open research issues [35], [54].

IX. CONCLUSION AND FUTURE WORKS

Malicious nodes with erroneous behavior are a major challenge in ICNs. These nodes launch various attacks, including fake packet attacks, packet drop attacks, and flood attacks. Flood attacks are the most common type of attack in DTNs. They consume scarce resources, such as buffer space, bandwidth, and processing power, which degrades the network's performance. This can lead to a decrease in packet delivery ratio (PDR) and an increase in packet loss ratio (PLR).

Researchers have proposed various algorithms to mitigate flood attacks. However, no single algorithm is perfect. This article provides a critical analysis of the existing algorithms and proposes a new taxonomy of flood attacks. The taxonomy is based on the following criteria:

The type of attack (e.g., packet flood attack, replica flood attack), the target of the attack (e.g., nodes, links, or the entire network), the motivation of the attacker (e.g., to disrupt the network, to steal data, or to gain unauthorized access). The new taxonomy will help researchers to better understand flood attacks and to develop more effective mitigation strategies. The article also presents a buffer consumption code for the ONE simulator. This code will help researchers to more accurately simulate the impact of flood attacks on network performance.

In the future, researchers will need to develop new algorithms to mitigate the various types of flood attacks identified in the taxonomy. These algorithms should be distributed, machine learning-based, and intrusion detection system-based. Additionally, researchers should focus on detecting attacks bundles/messages/packets rather than misbehavior nodes that launch the flood attacks.

We hope that this article will motivate new investigators in this area of security and highlight the following directions for future research:

* Critical analysis of flood attacks in ICNs such as DTNs.
* Critical analysis of various categories of flood attacks identified in the flood attacks taxonomy, and development of novel algorithms for various types of flood attacks (especially distributed, machine learning, and intrusion-detection-system-based algorithms).
* Detection of attacks bundles/messages/packets rather than misbehavior nodes that launch the flood attacks.

ACKNOWLEDGMENT

The authors would like to thank Prince Sultan University for paying the Article Processing Charges (APC) of this publication. They would also like to thank Prince Sultan University for their support.

REFERENCES

[1] J. F. Naves and I. M. Moraes, "Mitigating the ACK counterfeiting attack in delay and disruption tolerant networks," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Jul. 2017, pp. 1015–1020.

[2] C. Velásquez-Villada and Y. Donoso, "Delay/disruption tolerant networks based message forwarding algorithm for rural internet connectivity applications," in *Proc. 6th Int. Conf. Comput. Commun. Control (ICCCC)*, May 2016, pp. 16–22.

[3] J.-H. Cho and I.-R. Chen, "PROVEST: Provenance-based trust model for delay tolerant networks," *IEEE Trans. Depend. Sec. Comput.*, vol. 15, no. 1, pp. 151–165, Jan. 2018.

[4] A. Mallorquí, A. Zaballos, and D. Serra, "A delay-tolerant network for Antarctica," *IEEE Commun. Mag.*, vol. 60, no. 12, pp. 56–62, Dec. 2022.

[5] Y. Cao and Z. Sun, "Routing in delay/disruption tolerant networks: A taxonomy, survey and challenges," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 2, pp. 654–677, 2nd Quart., 2013.

[6] S. Yasmin, "Cost-effective routing & cooperative framework for opportunistic networks," Ph.D. thesis, Dept. Comput. Sci., Capital Univ. Islamabad, Pakistan, 2016.

[7] 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 Commun. Mag.*, vol. 41, no. 6, pp. 128–136, Jun. 2003.

[8] Y. Guo, S. Schildt, T. Pögel, and L. Wolf, "Detecting malicious behavior in a vehicular DTN for public transportation," in *Proc. Global Inf. Infrastruct. Symp.*, Oct. 2013, pp. 1–8.

[9] M. Arshad, Z. Ullah, M. Khalid, N. Ahmad, W. Khalid, D. Shahwar, and Y. Cao, "Beacon trust management system and fake data detection in vehicular ad-hoc networks," *IET Intell. Transp. Syst.*, vol. 13, no. 5, pp. 780–788, May 2019.

[10] J. Partan, J. Kurose, and B. N. Levine, "A survey of practical issues in underwater networks," *ACM SIGMOBILE Mobile Comput. Commun. Rev.*, vol. 11, no. 4, pp. 23–33, Oct. 2007.

[11] K. Matsuo, E. Kulla, and L. Barolli, "Effect of transporter autonomous underwater vehicles for underwater optical wireless communication considering delay tolerant networks," in *Proc. Int. Conf. Netw.-Based Inf. Syst.* Japan: Kwansei Gakuin Univ., 2022, pp. 172–181.

[12] P. Asuquo, H. Cruickshank, Z. Sun, and G. Chandrasekaran, "Analysis of DoS attacks in delay tolerant networks for emergency evacuation," in *Proc. 9th Int. Conf. Next Gener. Mobile Appl., Services Technol.*, Sep. 2015, pp. 228–233.

[13] D. Falcão, R. Salles, and P. Maranhão, "Performance evaluation of disruption tolerant networks on warships' tactical messages for secure transmissions," *J. Commun. Netw.*, vol. 23, no. 6, pp. 473–487, Dec. 2021.

[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," *ACM SIGPLAN Notices*, vol. 37, no. 10, pp. 96–107, Oct. 2002.

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

[16] 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 Comput. Commun. Rev.*, vol. 37, no. 5, pp. 95–100, Oct. 2007.

[17] P. K. Gautam, R. Johari, A. K. Yadav, R. Dahiya, I. Kaur, R. Bhatia, and S. Chaudhary, "PRiDE: Priority and reliability based routing in delay tolerant network," in *Proc. ICETIT*. India: Springer, 2020, pp. 1016–1027.

[18] L. Kulkarni, J. Bakal, and U. Shrawankar, "Energy based incentive scheme for secure opportunistic routing in vehicular delay tolerant networks," *Computing*, vol. 102, no. 1, pp. 201–219, Jan. 2020.

[19] E. Rosas, F. Garay, and N. Hidalgo, "Context-aware self-adaptive routing for delay tolerant network in disaster scenarios," *Ad Hoc Netw.*, vol. 102, May 2020, Art. no. 102095.

[20] C. Choudhari and D. Niture, "Disruption tolerant network (DTN) for space communication: An overview," in *Proc. IEEE 7th Int. Conf. Converg. Technol. (I2CT)*, Apr. 2022, pp. 1–5.

[21] P. K. Gantayat, S. Mohapatra, and S. K. Panda, "Secure trust level routing in delay-tolerant network with node categorization technique," in *Intelligent Data Engineering and Analytics*. India: Springer, 2022, pp. 453–458.

[22] Y. Azzoug and A. Boukra, "Enhanced UAV-aided vehicular delay tolerant network (VDTN) routing for urban environment using a bio-inspired approach," *Ad Hoc Netw.*, vol. 133, Aug. 2022, Art. no. 102902.

[23] C. Chakrabarti and S. Pramanick, "Implementing data security in delay tolerant network in post-disaster management," in *Computational Advancement in Communication, Circuits and Systems*. Springer, 2022, pp. 77–92.

[24] W. Li, L. Galluccio, M. Kieffer, and F. Bassi, "Distributed faulty node detection in DTNs," in *Proc. 25th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Aug. 2016, pp. 1–9.

[25] L. Cao and R. Viswanathan, "Average operation time of bundle protocol in delay/disruption-tolerant networks," *IEEE Trans. Wireless Commun.*, vol. 21, no. 8, pp. 5801–5813, Aug. 2022.

[26] S. Rashid, Q. Ayub, and A. H. Abdullah, "Reactive weight based buffer management policy for DTN routing protocols," *Wireless Pers. Commun.*, vol. 80, no. 3, pp. 993–1010, Feb. 2015.

[27] M. Pitkanen, A. Keranen, and J. Ott, "Message fragmentation in opportunistic DTNs," in *Proc. Int. Symp. World Wireless, Mobile Multimedia Netw.*, Jun. 2008, pp. 1–7.

[28] Q. Li, W. Gao, S. Zhu, and G. Cao, "To lie or to comply: Defending against flood attacks in disruption tolerant networks," *IEEE Trans. Depend. Sec. Comput.*, vol. 10, no. 3, pp. 168–182, May 2013.

[29] S. Perumal, V. Raman, G. N. Samy, B. Shanmugam, K. Kisenasamy, and S. Ponnan, "Comprehensive literature review on delay tolerant network (DTN) framework for improving the efficiency of internet connection in rural regions of Malaysia," *Int. J. Syst. Assurance Eng. Manage.*, vol. 13, pp. 764–777, Jan. 2022.

[30] A. Altaweel, R. Stoleru, G. Gu, A. K. Maity, and S. Bhunia, "On detecting route hijacking attack in opportunistic mobile networks," *IEEE Trans. Depend. Sec. Comput.*, vol. 20, no. 13, pp. 2516–2532, May/Jun. 2023.

[31] F. R. C. Araújo, A. L. R. Madureira, and L. N. Sampaio, "A multicriteria-based forwarding strategy for interest flooding mitigation on named data wireless networking," *IEEE Trans. Mobile Comput.*, early access, Sep. 12, 2022, doi: 10.1109/TMC.2022.3206167.

[32] C. Caini, "Delay-tolerant networks (DTNs) for satellite communications," in *Advances in Delay-Tolerant Networks (DTNs)*. Amsterdam, The Netherlands: Elsevier, 2021, pp. 23–46.

[33] L. Wu, S. Cao, Y. Chen, J. Cui, and Y. Chang, "An adaptive multiple spray-and-wait routing algorithm based on social circles in delay tolerant networks," *Comput. Netw.*, vol. 189, Apr. 2021, Art. no. 107901.

[34] W. Khalid, N. Ahmad, S. Khan, N. U. Saquib, M. Arshad, and D. Shahwar, "FAPMIC: Fake packet and selective packet drops attacks mitigation by Merkle hash tree in intermittently connected networks," *IEEE Access*, vol. 11, pp. 4549–4573, 2023.

[35] W. Khalid, N. Ahmed, M. Khalid, A. U. Din, A. Khan, and M. Arshad, "FRID: Flood attack mitigation using resources efficient intrusion detection techniques in delay tolerant networks," *IEEE Access*, vol. 7, pp. 83740–83760, 2019.

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

[37] 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 Trans. Veh. Technol.*, vol. 64, no. 4, pp. 1548–1564, Apr. 2015.

[38] M. Shah and P. Khanpara, "Survey of techniques used for tolerance of flooding attacks in DTN," in *Information and Communication Technology for Intelligent Systems*. Singapore: Springer, 2019, pp. 599–607.

[39] S. K. Dhurandher, A. Kumar, and M. S. Obaidat, "Cryptography-based misbehavior detection and trust control mechanism for opportunistic network systems," *IEEE Syst. J.*, vol. 12, no. 4, pp. 3191–3202, Dec. 2018.

[40] 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 Netw. Appl.*, vol. 10, no. 2, pp. 377–394, Mar. 2017.

[41] T. Le and M. Gerla, "A security framework for content retrieval in DTNs," in *Proc. Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Sep. 2016, pp. 7–12.

[42] N. Dang and X. Bai, "Content delivery mechanism in delay tolerant network," in *Proc. 7th IEEE Int. Conf. Softw. Eng. Service Sci. (ICSESS)*, Aug. 2016, pp. 493–496.

[43] Y. Cai, Y. Fan, and D. Wen, "An incentive-compatible routing protocol for two-hop delay-tolerant networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 1, pp. 266–277, Jan. 2016.

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

[45] G. Ansa, H. Criuckshank, Z. Sun, and M. Al-Siyabi, "A DOS-resilient design for delay tolerant networks," in *Proc. 7th Int. Wireless Commun. Mobile Comput. Conf.*, Jul. 2011, pp. 424–429.

[46] S. Symington, S. Farrell, H. Weiss, and P. Lovell, "Bundle security protocol specification," Internet Res. Task Force (IRTF), SPARTA, Inc., Tech. Rep. RFC 6257, May 2017.

[47] P. Nagrath and A. Kumar, "Analysis of malicious activity in delay tolerant networks," in *Proc. Int. Conf. Innov. Challenges Cyber Secur. (ICICCS-INBUSH)*, Feb. 2016, pp. 17–20.

[48] S. Chatterjee, M. Nandan, A. Ghosh, and S. Banik, "DTNMA: Identifying routing attacks in delay-tolerant network," in *Cyber Intelligence and Information Retrieval*. Springer, 2022, pp. 3–15.

[49] L. Lin, Y. Huang, L. Xu, and S.-Y. Hsieh, "Better adaptive malicious users detection algorithm in human contact networks," *IEEE Trans. Comput.*, vol. 71, no. 11, pp. 2968–2981, Nov. 2022.

[50] R. Sharma and S. K. Dinkar, "Selfish node detection by modularized deep NMF autoencoder based incentivized reputation scheme," *Cybern. Syst.*, vol. 54, no. 7, pp. 1172–1198, 2022.

[51] 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 *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2017, pp. 1–6.

[52] R. Skowronski, "Fully distributed GRIDNET protocol, with no trusted authorities," in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, Jan. 2017, pp. 569–574.

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

[54] W. Khalid, Z. Ullah, N. Ahmed, Y. Cao, M. Khalid, M. Arshad, F. Ahmad, and H. Cruickshank, "A taxonomy on misbehaving nodes in delay tolerant networks," *Comput. Secur.*, vol. 77, pp. 442–471, Aug. 2018.

[55] Y. Shimizu, T. Kimura, and J. Cheng, "Performance evaluation of a hash-based countermeasure against fake message attacks in sparse mobile ad hoc networks," *IEICE Trans. Commun.*, vol. E105.B, no. 7, pp. 833–847, 2022.

[56] N. Nishanth and A. Mujeeb, "Modeling and detection of flooding-based denial of service attacks in wireless ad hoc networks using uncertain reasoning," *IEEE Trans. Cogn. Commun. Netw.*, vol. 7, no. 3, pp. 893–904, Sep. 2021.

[57] S. Bansal, J. S. Sivia, and H. S. Bindra, "SPRP: A secured routing protocol for delay tolerant networks," *Int. J. Sensor Netw.*, vol. 31, no. 3, pp. 156–171, 2019.

[58] S. Bansal, J. S. Sivia, and H. S. Bindra, "Design, implementation and analysis of routing based attack model for delay tolerant networks for prophet routing protocol," *Int. J. Sensor Netw.*, vol. 31, no. 4, pp. 238–252, 2019.

[59] A. K. Gupta, J. K. Mandal, and I. Bhattacharya, "Mitigating selfish, blackhole and wormhole attacks in DTN in a secure, cooperative way," *Int. J. Inf. Comput. Secur.*, vol. 9, nos. 1–2, pp. 130–155, 2017.

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

[61] H. Abubakar, A. Tekanyi, and S. Sani, "Node cooperation strategy on security aided and group encounter prophet routing protocol of an opportunistic network," *Int. J. Comput. Appl.*, vol. 163, no. 8, pp. 34–38, Apr. 2017.

[62] W. Li, L. Galluccio, F. Bassi, and M. Kieffer, "Distributed faulty node detection in delay tolerant networks: Design and analysis," *IEEE Trans. Mobile Comput.*, vol. 17, no. 4, pp. 831–844, Apr. 2018.

[63] 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 Netw.*, vol. 24, pp. 173–194, Jun. 2016.

[64] T. Small and Z. J. Haas, "Resource and performance tradeoffs in delay-tolerant wireless networks," in *Proc. ACM SIGCOMM Workshop Delay-Tolerant Netw.*, 2005, pp. 260–267.

[65] P. Puri and M. P. Singh, "A survey paper on routing in delay-tolerant networks," in *Proc. Int. Conf. Inf. Syst. Comput. Netw.*, Mar. 2013, pp. 215–220.

[66] C. Chakrabarti, "iCredit: A credit based incentive scheme to combat double spending in post-disaster peer-to-peer opportunistic communication over delay tolerant network," *Wireless Pers. Commun.*, vol. 121, pp. 2407–2440, Aug. 2021.

[67] A. Patel and D. Bhadra, "Priority-based approach to mitigate selfish misbehaviour in delay tolerant network," *Int. J. Commun. Netw. Distrib. Syst.*, vol. 26, no. 2, pp. 176–197, 2021.

[68] T. S. K. Babu and S. Chitnis, "Coalition formation based cooperation strategy for routing in delay tolerant networks," *Mater. Today, Proc.*, vol. 45, pp. 8182–8187, Jan. 2021.

[69] 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*. India: Springer, 2015, pp. 11–19.

[70] M. Arshad, Z. Ullah, N. Ahmad, M. Khalid, H. Criuckshank, and Y. Cao, "A survey of local/cooperative-based malicious information detection techniques in VANETs," *EURASIP J. Wireless Commun. Netw.*, vol. 2018, no. 1, pp. 1–17, Dec. 2018.

[71] M. Khalid, Y. Cao, N. Ahmad, W. Khalid, and P. Dhawankar, "Radius-based multipath courier node routing protocol for acoustic communications," *IET Wireless Sensor Syst.*, vol. 8, no. 4, pp. 183–189, Aug. 2018.

[72] M. Khalid, F. Ahmad, M. Arshad, W. Khalid, N. Ahmad, and Y. Cao, "E^2MR: Energy-efficient multipath routing protocol for underwater wireless sensor networks," *IET Netw.*, vol. 8, no. 5, pp. 321–328, 2019.

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

[74] M. Khalid, Y. Cao, N. Aslam, C. Suthaputchakun, M. Arshad, and W. Khalid, "Optimized pricing & scheduling model for long range autonomous valet parking," in *Proc. Int. Conf. Frontiers Inf. Technol. (FIT)*, 2018, pp. 65–70.

[75] S. A. M. Benazir and V. Umarani, "Detection of selfish & malicious behavior using DTN-chord monitoring in mobile networks," in *Proc. Int. Conf. Inf. Commun. Embedded Syst. (ICICES)*, Feb. 2016, pp. 1–5.

[76] S. U. Maheswari, N. S. Usha, E. A. M. Anita, and K. R. Devi, "A novel robust routing protocol RAEED to avoid DoS attacks in WSN," in *Proc. Int. Conf. Inf. Commun. Embedded Syst. (ICICES)*, Feb. 2016, pp. 1–5.

[77] M. Khalid, A. Adnan, Z. Ullah, W. Khalid, N. Ahmad, and A. Ashfaq, "Comparison of localization free routing protocols in underwater wireless sensor networks," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 3, 2017.

[78] M. Khalid, Y. Cao, M. Arshad, W. Khalid, and N. Ahmad, "Routing challenges and associated protocols in acoustic communication," in *Magnetic Communications: From Theory to Practice*. Boca Raton, FL, USA: CRC Press, 2017, pp. 109–126.

[79] H. Asahina, K. Arai, S. Haruta, P. T. Mathiopoulos, and I. Sasase, "An energy-efficient defense against message flooding attacks in delay tolerant networks," *IEICE Trans. Commun.*, vol. E104.B, no. 4, pp. 348–359, 2021.

[80] Y. Wu, Y. Zhao, M. Riguidel, G. Wang, and P. Yi, "Security and trust management in opportunistic networks: A survey," *Secur. Commun. Netw.*, vol. 8, no. 9, pp. 1812–1827, Jun. 2015.

[81] S. Djahel, F. Nait-Abdesselam, and Z. Zhang, "Mitigating packet dropping problem in mobile ad hoc networks: Proposals and challenges," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 4, pp. 658–672, 4th Quart., 2011.

[82] A. Nayal and S. Jain, "Literature review on security aspects of delay tolerant networks," *Int. J. Comput. Appl.*, vol. 116, no. 9, pp. 34–37, Apr. 2015.

[83] D. S. D. Hepsiba and S. Prabhu, "Enhanced techniques to strengthening DTN against flood attacks," in *Proc. Int. Conf. Inf. Commun. Embedded Syst. (ICICES)*, Feb. 2014, pp. 1–4.

[84] V. Natarajan, Y. Yang, and S. Zhu, "Resource-misuse attack detection in delay-tolerant networks," in *Proc. 30th IEEE Int. Perform. Comput. Commun. Conf.*, Nov. 2011, pp. 1–8.

[85] F. C. Lee, W. Goh, and C. K. Yeo, "A queuing mechanism to alleviate flooding attacks in probabilistic delay tolerant networks," in *Proc. 6th Adv. Int. Conf. Telecommun.*, 2010, pp. 329–334.

[86] A. Lindgren, A. Doria, and O. Schelén, "Probabilistic routing in intermittently connected networks," *ACM SIGMOBILE Mobile Comput. Commun. Rev.*, vol. 7, no. 3, pp. 19–20, Jul. 2003.

[87] P. Nagrath, S. Aneja, and G. N. Purohit, "Defending flooding attack in delay tolerant networks," in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, Jan. 2015, pp. 40–45.

[88] D. Kuriakose and D. Daniel, "Effective defending against flood attack using stream-check method in tolerant network," in *Proc. Int. Conf. Green Comput. Commun. Electr. Eng. (ICGCCEE)*, Mar. 2014, pp. 1–4.

[89] P. T. N. Diep and C. K. Yeo, "Detecting flooding attack in delay tolerant networks by piggybacking encounter records," in *Proc. 2nd Int. Conf. Inf. Sci. Secur. (ICISS)*, Dec. 2015, pp. 1–4.

[90] S. B. Lavanya, S. G. Devi, A. Mary, and M. V. E. Dyana, "Deducing malicious attacks in disruption tolerant networks," *Indian J. Emerg. Electron. Comput. Commun.*, vol. 1, no. 1, pp. 110–115, 2014.

[91] G. Rani and K. S. Kumar, "Defending against flood attacks in disruption tolerant networks," Tech. Rep., 2014. [Online]. Available: https://www.ijcsmc.com/docs/papers/October2014/V3I10201475.pdf

[92] K. Ramaraj, J. Vellingiri, C. Saravanabhavan, and A. Illayarajaa, "Denial of service flood attacks in disruption tolerant networks," Tech. Rep. [Online]. Available: https://www.google.com/search?q=K+Ramaraj%2C+J+Vellingiri%2C+C+Saravanabhavan%2C+and+A+Illayarajaa.+Denial+of+service+flood+attacks+in+disruption+tolerant+networks.&rlz=1C1NHXL_enPK787PK787&oq=K+Ramaraj%2C+J+Vellingiri%2C+C+Saravanabhavan%2C+and+A+Illayarajaa.+Denial+of+service+flood+attacks+in+disruption+tolerant+networks.&aqs=chrome..69i57j69i60.1381j0j15&sourceid=chrome&ie=UTF-8

[93] R. Ezhilarasan and R. Rameshkumar, "Protection and detection of flood attacks in disruption tolerant networks," Tech. Rep. [Online]. Available: https://www.ijetcse.com/admin/uploads/Protection%20and%20Detection%20of%20Flood%20Attacks%20in%20Disruption%20Tolerant%20Networks_1605599805.pdf

[94] C. Balamurugan, M. Viswanathan, T. A. Kumar, and G. S. Raj, "Detection of flood attacks in DTN using rate limiter technique," *J. Comput. Sci.*, vol. 10, no. 7, p. 1216, 2014.

[95] A. J. Bassey and C. Fancy, "Mitigating flooding attacks in disruption tolerant network," Tech. Rep. [Online]. Available: http://www.ijcstjournal.org/volume-3/issue-5/IJCST-V3I5P12.pdf

[96] P. Bisarwal and A. Chauhan, "A study of black hole attacks in delay tolerant network," in *Trends in Wireless Communication and Information Security*. India: Srringer, 2021, pp. 9–17. [Online]. Available: https://link.springer.com/book/10.1007/978-981-33-6393-9, doi: 10.1007/978-981-33-6393-9_2.

[97] J. Singh, I. Woungang, S. K. Dhurandher, and K. Khalid, "A jamming attack detection technique for opportunistic networks," *Internet Things*, vol. 17, Mar. 2022, Art. no. 100464.

[98] Y. Badr, X. Zhu, and M. N. Alraja, "Security and privacy in the Internet of Things: Threats and challenges," *Service Oriented Comput. Appl.*, vol. 15, no. 4, pp. 257–271, Dec. 2021.

[99] A. Roy, T. Acharya, and S. D. Bit, "Social-based reputation-aware data forwarding for improved multicast delivery in the presence of selfish nodes in DTNs," *Int. J. Commun. Syst.*, vol. 33, no. 4, p. e4235, Mar. 2020.

[100] M. J. Kumar, B. S. Rao, N. R. Sai, and S. S. Kumar, "Using QRE-based game model for better IDS," in *Proc. 5th Int. Conf. I-SMAC (IoT Social, Mobile, Analytics Cloud) (I-SMAC)*, Nov. 2021, pp. 1–9.

[101] T. N. D. Pham, C. K. Yeo, N. Yanai, and T. Fujiwara, "Detecting flooding attack and accommodating burst traffic in delay-tolerant networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 1, pp. 795–808, Jan. 2018.

[102] T. A. S. Srinivas and S. S. Manivannan, "Prevention of hello flood attack in IoT using combination of deep learning with improved rider optimization algorithm," *Comput. Commun.*, vol. 163, pp. 162–175, Nov. 2020.

[103] V. Juyal, R. Saggar, and N. Pandey, "An optimized trusted-cluster–based routing in disruption-tolerant network using experiential learning model," *Int. J. Commun. Syst.*, vol. 33, no. 1, Jan. 2020, Art. no. e4196.

[104] R. Chaudhari and M. Deshpande, "Comparative analysis of attack detection methods in delay tolerant network," *Int. J. Eng. Appl. Phys.*, vol. 1, no. 3, pp. 272–277, 2021.

[105] P. Srividya and L. N. Devi, "A trusted approach for prediction of data link failure and intrusion detection in wireless sensor networks," Tech. Rep., 2021. [Online]. Available: https://assets.researchsquare.com/files/rs-903992/v1_covered.pdf?c=1631879252

[106] H. Liang, Y. Shang, and S. Wang, "Study on DTN routing protocol of vehicle ad hoc network based on machine learning," *Wireless Commun. Mobile Comput.*, vol. 2021, pp. 1–10, Oct. 2021.

[107] B. V. Sherif and P. Salini, "Selfish node management in opportunistic mobile networks with improved social based watchdog and dynamic power AODV protocol," *Int. J. Inf. Technol.*, vol. 14, no. 6, pp. 3253–3264, Oct. 2022.

[108] V. Vidhya and M. Madheswaran, "Data compression and transmission techniques in wireless adhoc networks: A review," in *Intelligent Computing and Networking: Proceedings of IC-ICN 2021*. India: Springer, 2022, pp. 194–206. [Online]. Available: https://link.springer.com/chapter/10.1007/978-981-16-4863-2_17

[109] S.-Y. Yu, J. Chen, F. Yeh, J. Mambretti, X. Wang, A. Giannakou, E. Pouyoul, and M. Lyonnais, "Analysis of NVMe over fabrics with SCinet DTN-as-a-service," *Cluster Comput.*, vol. 25, no. 4, pp. 2991–3003, Aug. 2022.

[110] J. Burgess, G. D. Bissias, M. D. Corner, and B. N. Levine, "Surviving attacks on disruption-tolerant networks without authentication," in *Proc. 8th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, Sep. 2007, pp. 61–70.

[111] N. Das, S. Basu, and S. D. Bit, "ReliefChain: A blockchain leveraged post disaster relief allocation system over smartphone-based DTN," *Peer-to-Peer Netw. Appl.*, vol. 15, pp. 2603–2618, Sep. 2022.

[112] T. H. H. Aldhyani and H. Alkahtani, "Attacks to automatous vehicles: A deep learning algorithm for cybersecurity," *Sensors*, vol. 22, no. 1, p. 360, Jan. 2022.

[113] D. Su and Z. Qu, "Detection DDoS of attacks based on federated learning with digital twin network," in *Proc. Int. Conf. Knowl. Sci., Eng. Manage.* Singapore: Springer, 2022, pp. 153–164.

[114] I. Almomani, M. Ahmed, D. Kosmanos, A. Alkhayer, and L. Maglaras, "An efficient localization and avoidance method of jammers in vehicular ad hoc networks," *IEEE Access*, vol. 10, pp. 131640–131655, 2022.

[115] M. Driss, I. Almomani, Z. E. Huma, and J. Ahmad, "A federated learning framework for cyberattack detection in vehicular sensor networks," *Complex Intell. Syst.*, vol. 8, no. 5, pp. 4221–4235, Oct. 2022.

[116] A. Rehman, K. Haseeb, T. Saba, J. Lloret, and Z. Ahmed, "Towards resilient and secure cooperative behavior of intelligent transportation system using sensor technologies," *IEEE Sensors J.*, vol. 22, no. 7, pp. 7352–7360, Apr. 2022.

[117] R. Qaddoura, A. M. Al-Zoubi, I. Almomani, and H. Faris, "A multi-stage classification approach for IoT intrusion detection based on clustering with oversampling," *Appl. Sci.*, vol. 11, no. 7, p. 3022, Mar. 2021.

[118] K. Haseeb, T. Saba, A. Rehman, Z. Ahmed, H. H. Song, and H. H. Wang, "Trust management with fault-tolerant supervised routing for smart cities using Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 22, pp. 22608–22617, Nov. 2022.

[119] A. Keränen, J. Ott, and T. Kärkkäinen, "The ONE simulator for DTN protocol evaluation," in *Proc. 2nd Int. ICST Conf. Simulation Tools Techn.* Brussels, Belgium: Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2009, p. 55.

[120] A. K. Singh, R. Pamula, and G. Srivastava, "An adaptive energy aware DTN-based communication layer for cyber-physical systems," *Sustain. Comput., Informat. Syst.*, vol. 35, Sep. 2022, Art. no. 100657.

[121] S. Perumal, V. Raman, G. N. Samy, B. Shanmugam, K. Kisenasamy, and S. Ponnan, "Enhanced disruption tolerant network (DTN) framework for improving network efficiency in rural areas," *Int. J. Syst. Assurance Eng. Manage.*, vol. 13, no. S1, pp. 710–717, Mar. 2022.

[122] X. Cao, S. Datta, R. C. Bolla, and S. Madria, "Targeted content-sharing in a multi-group DTN application using attribute-based encryption," in *Proc. 23rd IEEE Int. Conf. Mobile Data Manage. (MDM)*, Jun. 2022, pp. 306–309.

[123] E. A. A. Alaoui, S. C. K. Tekouabou, Y. Maleh, and A. Nayyar, "Towards to intelligent routing for DTN protocols using machine learning techniques," *Simul. Model. Pract. Theory*, vol. 117, May 2022, Art. no. 102475.

WAQAR KHALID received the bachelor's degree (Hons.) in computer science from the Institute of Business and Management Study (IBMS), The University of Agriculture, Peshawar, Khyber Pakhtunkhwa, Pakistan, and the Master of Science (M.S./M.Phil.) degree in computer science from the Institute of Management Sciences (IMSciences), Peshawar, Khyber Pakhtunkhwa. He is currently pursuing the Ph.D. degree with the School of Cyber Science and Engineering, Wuhan University, China. He has been a Teacher with the Elementary and Secondary Education, Khyber Pakhtunkhwa, since 2017. His research interests include the design and analyses of secured communication protocols in networks (self organizing networks: DTNs, VANETs, WSNs, SINs, and the IoTs). He designs new cryptographic algorithms and cryptanalysis of the existing algorithms. He is a reviewer in various journals of IEEE and Elsevier.

NAVEED AHMED (Member, IEEE) received the M.Sc. degree in computer science from the Department of Computer Science, University of Peshawar, Pakistan, in 2007, and the Ph.D. degree in computer science from the Center for Communication System Research (CCSR), University of Surrey, U.K., in 2013. He was an Assistant Professor with the Department of Computer Science, University of Peshawar. He is currently an Associate Professor with the College of Computer and Information Sciences, Prince Sultan University, Saudi Arabia. He has more than 45 publications that include international reputed journals, conferences, and workshops. He worked in the area of cyber security, privacy, blockchain technology, and penetration testing. He has managed three research and development grants related to blockchain, transport system for emergency vehicles, and platoon management. He served on the program committee for various national conferences and workshops. He was a reviewer of various research proposals/grants funded by the U.K. Research and Innovation (UKRI). He was a reviewer of various IEEE, Elsevier, Springer, and MPDI journals. He has the honor of serving as the Guest Editor for the Special Issue of the IEEE Internet of Things Journal.

SULEMAN KHAN (Member, IEEE) received the Ph.D. degree (Hons.) in computer science and information technology from Universiti Malaya, Malaysia, in 2017. He was a Faculty Member of the School of Information Technology, Monash University, Malaysia, from June 2017 to March 2019. He was a Faculty Member of the Department of Computer and Information Sciences, Northumbria University, Newcastle upon Tyne, U.K. He is currently a Senior Lecturer with the University of Central Lancashire, U.K. He has published more than 80 high-impact research articles in reputed international journals and conferences. His research interests include network forensics, software defined networks security, and the IoT security. He is a PGCAP and a FHEA.

ZAHID ULLAH received the B.C.S. degree (Hons.) in computer science from KPK, The University of Agricultural, Peshawar, Pakistan, in 2005, the M.S. degree in telecommunication and networking from Gandhara University, Peshawar, in 2008, and the Ph.D. degree from the Institute of Management Sciences, Peshawar. He is currently an Assistant Professor with the Centre of Excellence in IT, Institute of Management Sciences. He has more than 14 years of practical and teaching experience in computer sciences and got hands on experience in different networking related devices. His research interests include wireless sensor networks, underwater sensor networks, wireless body area networks, the Internet of Things, VANETS, and delay tolerant networks. He received several Cisco, Juniper, and Microsoft International Certifications in science field, especially in networks.

YASIR JAVED (Member, IEEE) received the Ph.D. degree. He was an Analyst Programmer with the Prince Megren Data Center, the Center of Excellence, and the Research and Initiative Center, Prince Sultan University. He is an active member of the RIOTU Group, Prince Sultan University. He is a highly qualified Data Scientist and a Senior Programmer of more than 18 years of experience in research, security programming, software development, project management, and analytics. He has published more than 100 peer-reviewed articles in top-tier journals, conference proceedings, and book chapters. With regards to his professional experience, he has undertaken a variety of national and international research funding projects. His research interests include data analytics, forensics, smart cities, network security, education sustainability, instructional development, learning and education sustainability, robotics, unmanned aerial vehicles, vehicular platoons, secure software development, signal processing, the IoT analytics, intelligent applications, and predictive computing inspired by artificial intelligence. He received the Outstanding Ph.D. Student Award from UNIMAS, Sarawak. He was awarded the Rector's Medal for his M.S. degree and the Distinguished Teaching Award from the President. He is listed in Top Researcher Award from PSU in recognition of his research contributions. He serves as the Chair of the ACM Professional Chapter in KSA. He serves as a reviewer for several journals.