IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 31, 2019, accepted June 12, 2019, date of publication June 24, 2019, date of current version July 12, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2924587

FRID: Flood Attack Mitigation Using Resources Efficient Intrusion Detection Techniques in Delay Tolerant Networks

WAQAR KHALID[1], NAVEED AHMED[2], MUHAMMAD KHALID[3], AZIZ UD DIN[4], AURANGZEB KHAN[5], AND MUHAMMAD ARSHAD[1]

[1]Department of Computer Science, Institute of Management Sciences, Peshawar 25000, Pakistan
[2]Department of Computer Science, University of Peshawar, Peshawar 25000, Pakistan
[3]Department of Computer and Information Sciences, Northumbria University, Newcastle Upon Tyne NE1 8ST, U.K.
[4]Seikh Zayed Islamic Centre, University of Peshawar, Peshawar 25000, Pakistan
[5]Department of Computer Science, University of Science and Technology, Bannu 28100, Pakistan

Corresponding author: Muhammad Khalid (m.khalid@northumbria.ac.uk)

ABSTRACT Delay tolerant networks (DTNs) are a special type of intermittently connected networks (ICN) featured by variable delay, frequent disruption, asymmetric data rates, and high-error rates. The DTNs have been primarily developed for interplanetary networks (IPNs), however, it shows applicability to challenged networks. Thus, solutions devised for security and routing for traditional networks do not apply to DTNs due to its unique nature. Moreover, this paper shows less attention particularly in security and its related strings. In DTNs, malicious nodes launch various attacks that include packet drop, a fake packet, and flood attack. These attacks inevitably overuse scarce resources (bandwidth, buffer, and energy) in DTNs, which leads to low packet delivery ratio and high packet loss ratio. Flood attack is listed in top among the challenging attacks in DTNs. The existing techniques to confront flood attack suffered from high-detection time and low-detection accuracy. This paper proposed novel resources efficient (distributed and intrusion detection system-based) algorithms to mitigate flood attack. The simulation results show considerable improvement in detection time, detection accuracy, and resource consumption, and also show enhanced packet delivery ratio and reduced packet loss ratio.

INDEX TERMS Delay tolerant networks (DTNs), flood attack, misbehaving nodes, packet delivery ratio, packet loss ratio and resources consumption.

I. INTRODUCTION

Delay/Disruption Tolerant Networks (DTNs) are type of networks which suffer from frequent disconnection and long/variable delay [1]–[3]. Initially, DTNs were proposed for Deep Space Communication, commonly known as Interplanetary Networks (IPNs) [4]. However, after successful deployment in IPNs, DTNs are used for various others terrestrial applications, such as Vehicular Ad-hoc Networks (VANETs) [5], Underwater Wireless Sensor Networks (UWSNs) [6] and other challanged networks [7].

DTNs supporting heterogeneous networks, characterized by long delay, network partitioning, and asymmetric data rate. Bundles Protocol (BP) is proposed to solve the aforementioned issues of DTNs [8]. The DTNs node uses a custodian forwarding mechanism i.e. Store-Carry-Forward (SCF) method to forwards bundles. [9]. The current issues in DTNs reported in literature are; Reliability [10], [11], Time Synchronization [10], [11], Node Management, Spoof Identity [12], Privacy [13], Key Management [14], Storage Management [15], and Resources Scarcity. The research area of security paid less attention viz-a-viz routing [16] which is the motivation behind this article.

The Bundle Security Protocol (BSP) has been proposed to counter the security issues. However, BSP provides some basic security services [17] and lack scenario/use-cases based specific solutions. In DTNs, nodes are vulnerable to various security attacks i.e. Black Hole [18], Packet Drops [19], Faulty Node [20], Colluding Attacks [21], Fake Packet Attacks [22] and Distributed Denial of Service (DDOS)/Flood Attacks [23].

In flood attack, the malicious node(s) forward a large number of packets, which overuse the scarce resources

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

of DTNs. The scarce resources include the buffer, bandwidth, energy, and processing power. This attack leads to, a decrease in the packet delivery ratios (PDR), contrary to the increase in packet loss ratios (PLR) and node's unavailability for service(s). The traditional routing protocols and detection/mitigation protocols proposed for VANETs [24]–[26], Autonomous Vehicle [27], UWSNs [28], [29], Internet [30], Internet of Things [31], Mobile Ad-hoc Networks (MANETs) [32] and Wireless Sensor Networks (WSNs) [33]–[35] do not apply directly in DTNs.

The algorithms proposed in the literature to counter flood attack suffered from Detection time/detection delay, detection rate/detection accuracy, high cost, and centrality (Centralized algorithms in which one node is responsible for malicious nodes detection) [36]–[39]. The above issues lead to Buffer Consumption (BC), Bandwidth Consumption (BWC)/Total Wasted Transmission (TWT) and Energy Consumption (EC) that ultimately causes low PDR and high PLR. Researchers proposed various algorithms to mitigates misbehaving nodes which launches flood attacks (As mentioned earlier in this article). This section discussed all the proposed algorithms to mitigate flood attacks in DTNs.

The article [37] proposed an algorithm to mitigate flood attacks in DTNs. The proposed algorithm, allocated less memory space to malicious and more space to legitimate nodes by deleting messages from the buffer. However, false positive and false negative ratios are high in this algorithm and only works for probabilistic routing protocol using history of encounter and transitivity (Prophet) [40], which is obviously downside of the proposed algorithm. The [41] proposed a centralized (In which one node is responsible for detection) algorithm to mitigate flood attacks in DTNs. In the proposed algorithm, every node share has memory picture to centralized Gate-Way-Node. Gate-Way-Node counts the number of packets of every node. If node violates the threshold (Pre defined value), Gate-Way-Node blacklist that malicious node. The proposed algorithm detects both packet flood (in packet flood attacks, malicious nodes forwards large numbers of different packets) and replica flood (in replica flood attacks, malicious nodes send replica that is copy of the packets to various innocent nodes) attack deterministically. Researchers also proposed probabilistic detection for replica flood attack, which improved the detection time. The proposed algorithm is difficult to deploy (Every packet pass to the centralized node) in DTNs. This algorithm always needs a connected environment like TCP/IP based, which is downside of the algorithm.

The work in [36] proposed distributed algorithm to mitigate malicious nodes. A rate limiting algorithm is proposed to tackle misbehaving nodes. In the proposed algorithm, during initial set up of the network, every node forward request packet to trusted authority (TA) for rate limit certificate (RLC). TA give RLC to every node according to the requirements. Nodes forwards RLC along with packets and packet claims (every node count has own packets and make a claim of forwarded packets). Destination nodes cross check the packet claims. The proposed algorithm detects malicious nodes according to pigeon-hole principal. Proposed algorithm is very efficient to detect and mitigate flood attacks. Nonetheless, detection time is very high which can not save precious resources until detection and also it waste more resources (because every node forwards packet claims along with original packet, which consumed buffer space, this ultimately cause low PDR and high PLR), which is downside of the proposed algorithm. The work in the research article [42] improved the work [36]. The proposed algorithm adds learning automata algorithm to modify the existing algorithm. The proposed algorithm approximately count the packets (according to the researchers), which enhanced the existing algorithm [36].

The work in [17] proposed the algorithm which detects and mitigate flood attacks. The proposed algorithm used cookies (for mitigation of malicious nodes), which is made of time stamp, source id, and a random number. Further, the researchers add HMAC and XOR with cookies for more randomness (Researchers Strengthen the proposed algorithm to use HMAC and XOR for cookies creation, which tight the security of packets). Algorithm detects malicious nodes by cookies verification. Proposed algorithm detects only out side (nodes without cryptographic credential) malicious nodes, which is a downside of the algorithm (The proposed algorithm do not have the ability to detect insider malicious nodes which have a valid cryptographic key and other credential). The article [43] proposed reputation based algorithm to tackle misbehavior nodes. The malicious nodes have the ability to flood networks with bogus messages but does not create genuine messages (according to the assumption of researchers). During initial set up, nodes create a genuine message and forward to TA. TA give reputation to nodes. However, TA does not give reputation to nodes which does not have the ability to create genuine messages (Malicious nodes). Receiver nodes check the reputation of the nodes, if reputation is less than predefined threshold, receiver does not accept messages from nodes. Authors proposed an ideal preventive algorithm to stop malicious nodes. However, this article does not give an answer to some questions. Why malicious nodes do not have the ability to create legitimate packets?. How TA recognized legitimate and bogus packets?. What are the criterion's for legitimate packets?.

The article [38] piggyback the existing encounter record scheme with rate limit to detect and mitigate malicious nodes. Malicious nodes have two choices, either change timestamp or sequence number. But by doing these alteration encounter record becomes inconsistent. Proposed algorithm detect those malicious nodes which alter encounter record. High detection time and cost (Nodes share encounter history, which consumed buffer and bandwidth which ultimately cause low PDR and high PLR) are the downside of the proposed algorithm. Researchers in [39] proposed a centralized Stream-Node to detect malicious nodes. Stream-Node have three table that is B-list (Blacklist table), DPT-Table

(Delivery probability table) and rate limit table. In the proposed algorithm Stream-Node calculate actual delivery probability from rate limit table. Then compare it with the estimated probability from DPT-Table. If there is any inconsistency Stream-Node detect malicious nodes. In the proposed algorithm stream-node move like patrolling police with every packet. This is costly and difficult to deploy in DTNs.

This article proposed novel algorithms to detect and mitigate malicious nodes [44], that launches flood attacks. The proposed algorithms not only enhance detection rate, and detection time but also reduces resources consumption that ultimately improved PDR and PLR. More specifically, the contributions of this articles are:

- Revamp To lie Or Comply (RTOC): The proposed RTOC algorithm 1 is the enhanced version of the To lie or Comply algorithm [36]. The RTOC thwarts flood attacks by using huffman coding compression without packet claims. Algorithm [36] forwards packet claims along with every packets, which consumed precious resources until detection. Unlike [36] our RTOC forwards compress packets and do not decompress packets until claims verification, which save precious resources (Buffer) and enhanced PDR and PLR.
- Inter site Flood Attack Mitigation (IFAM): The proposed IFAM algorithm 2 mitigates flood attacks using agent-based Intrusion Detection System (IDS). The IFAM counts the number of messages of every node to rule out the malicious node in the inter site scenario/use case.
- Holistic Flood Attack Mitigation (HFAM): The proposed HFAM algorithm 3 further enhance IFAM 2, and detects malicious nodes in the generic scenario. In HFAM, every node deployed IDS that create a key, which is appended with every packet. HFAM makes Message Authentication Code (MAC. Hash with Key) of every packet and then forwards packets to destination nodes. Destination nodes verify MAC.

Th rest of the paper is organized as follow. Section II discusses the Preliminaries/critical analysis of flood attacks. Section III Section IV and Section V are related to proposed algorithms, RTOC (A), IFAM (A2), and HFAM (A3) respectively. Section VI is related to comparison, Followed by conclusion, recommendations and future work in Section VII.

II. PRELIMINARIES

This section analyses existing flood mitigation algorithms with various parameters rigorously, which enable this article to modify one existing algorithm of flood mitigation [36]. Few researchers proposed flood mitigation schemes which send extra information (Packet Claims) along with packets. Few articles proposed flood mitigation algorithms which share encounter history with other nodes. This consumed buffer, creates PDR, PLR and resources consumption problems (already mentioned in this article). Few researchers proposed algorithms which do not detect malicious nodes until all nodes in networks share encounter history or packet claim verification. These algorithms detect malicious nodes, however consumed too much time and dis improve detection accuracy (because nodes are disconnected in DTNs). Based on these few observations, this article analyzed existing flood mitigation algorithms, which is discussed in this section. All constants used in this section are based on observations and analysis, the exact value of constant term used in analysis and its exact relationship with parameters are out of the scope of this article. Table 1 is symbol list, which summarized parameter symbols which are used in this section.

TABLE 1. Symbol list.

Parameter	*Symbol*	*Parameter*	*Symbol*
Packet Delivery Ratio	PDR	Buffer Consumption	BC
Packet Loss Ratio	PLR	Bandwidth Consumption	BWC
Availability	η	Contact Duration	κ
Buffer Size	Θ	Packet Size	ρ
Detection Accuracy	ν	Contact Time	τ
Number Of Packets	γ	Number Of Nodes	ω
Number Of Malicious Nodes	λ	Area	Π
Node Walking Speed	NWS	Transmission Range	TR

A. EXTRA INFORMATION ALONG WITH PACKETS

According to the observation of this article, most of the mitigation algorithms forward some extra information along with packets. That is rate limit based algorithms which forwards packet claims along with packets. Encounter-based algorithms used history information in mitigation. Due to the increased size of extra information included in packet, this ultimately causes PDR and PLR problems. According to analysis "PDR" and "PLR" both depend on Buffer size (θ) and BC, more details can be found in [23], [45].

$$\text{PDR/PLR} = \text{C1} * \theta \tag{1}$$

Eq. (1) implies that PDR is increased and PLR is decreased with buffer size. Where C1 is connectivity constants which depends on connectivity, encounter, and packet processing capability. It implies if there is no connectivity, encounter opportunity and processing capability (node processor is busy in something else). In this case, Eq. (1) will not be applicable. Eq. (1) implies PDR is increased with certain limit. However, according to Eq. (2), PDR is decreased and PLR is increased with BC.

$$\text{PLR/PDR} = \text{C2} * \text{BC} \tag{2}$$

According to analysis, BC depends on packet size "ρ" [46] and number of packets "γ". If packet size is large or malicious nodes forwards large number of packets, it will consume buffer, so ultimately decreases PDR and increases PLR. Eq. 3 shows this relation.

$$\rho * \gamma/\text{C3} = \text{BC} \tag{3}$$

Put the value of Eq. 3 into Eq. 2 we get new relation between packet size, number of packets with PDR and PLR.

$$\text{PLR/PDR} = (\text{C2}) * (\rho * \gamma/\text{C3}) \tag{4}$$

The total BC during communication of networks will calculated as followed.

$$\text{BC}_{\text{Networks}} = \sum_{\gamma=1}^{\text{Packets}} (\rho * \gamma) \tag{5}$$

Energy is required for nodes to forwards and process packets. There are three different types of energy which are required for nodes to communicate, that is Scan Energy (SE) (there are two types of SE, Scan Request Energy and Scan Response Energy, this article take an equal amount of SE for both Scan Request and Scan Response), Transmit Energy (TrE) and Processing Energy (PE).

1) SCAN ENERGY (SE)

A type of energy which is required for scanning (searching) a new nodes/channel for the encounter.

2) TRANSMIT ENERGY (TRE)

A type of energy which is required for transmit of packet to the destination.

3) PROCESSING ENERGY (PE)

A type of energy required to process received packets. Total energy spend in the communication process is the sum of SE, TrE and PE.

$$\text{Total Energy (TotalE)} = (\text{SE} + \text{TrE} + \text{PE}) \tag{6}$$

Total energy required to send packets is equal to the sum of TrE and SE (Sender Side). Total energy consumed to receive packets are equal to the sum of SE and PE (Receiver Side). According to the analysis EC depends on "ρ" [46]. "ρ" is directly proportional to EC and BWC. If the size of the packets are large so it will consume more bandwidth and buffer, which ultimately cause PDR and PLR problems. If the size of packets is large so more TrE and PE are required to transmit and receive packets.

$$\rho = \text{C4} * (\text{EC}) \tag{7}$$

$$\rho = \text{C5} * \text{BWC} \tag{8}$$

Eq. 3, 7 and 8 implies that due to packet size, buffer, bandwidth, and EC are increased. According to observation PDR and PLR depend on EC. If nodes consumed more energy so nodes quickly become down, which create PDR and PLR problems. PDR and PLR also depends on Scan Interval (SI) (The time between two consecutive Scan is called Scan Interval). SI is inversely proportional to EC (if nodes frequently scan nodes it will consume more energy) (The prove of above all equations and statements will be given in simulation section of this article, due to pages limitation). apart from the above some analysis PDR also depends on the transmission range and the transmission speed of nodes. PDR is directly proportional to transmission range (TR) and node walking speed/nodes transmission speed (NWS)

$$\text{PDR} = \text{C6} * \text{Transmission Range (TR)} \tag{9}$$

$$\text{PDR} = \text{C7} * (\text{NWS}) \tag{10}$$

where C6 and C7 are constants which depends on Number-of-encounters. The Number-of-encounters is increased with TR and NWS, which increased PDR and decreased PLR, for more detail this article refer article [23].

B. SHARING OF PACKET CLAIMS AND ENCOUNTER HISTORY

Detection accuracy of algorithms is a very important parameter to analyzed algorithms. Some of the proposed algorithms are not very accurate to mitigate flood attacks in DTNs. The false positive and false negative ratios are high, because those algorithms, share encounter history and claims to detect attacks. However, it took a very long time to detects attacks, due to intermittent connectivity of nodes in DTNs. Consider rate-limit-based and encounter-based algorithms. Both types of algorithms detect malicious nodes only when other nodes encounter, because rate-limit-based algorithms used cross checking strategy and encounter-based-algorithms share encounter history information with other nodes (already mentioned in this article). According to the observations of this article, detection accuracy depends on contact-time/contact-opportunity. That is, if nodes encounter frequently that is less contact-time, so detection accuracy will be high otherwise low. If detection accuracy is (ν) and contact time is (τ), then detection accuracy will be calculated as follow.

$$\nu = \text{C8}/\tau \tag{11}$$

Also if the number of malicious nodes (λ) are high so the probability of detection are high [36]. Which decreased false positive and false negative ratios.

$$\nu = \text{C9} * \lambda \tag{12}$$

But "ν" also depends on contact duration (κ)

$$\nu = \text{C10} * \kappa \tag{13}$$

If nodes meet frequently but κ is less, so definitely it will affect the value of ν (if nodes encounter but duration of encounter is less so there is the probability that nodes do not share an encounter history packets and packets claims or probability of aborted packets will be high). Above observations and analysis implies that "ν" is related to area (Π). "ν" is inversely related to the integral area.

$$\nu \approxeq \frac{\text{C11}}{\int_{\text{a}}^{\text{b}} (\Pi)^n} \tag{14}$$

where "a" and "b" is the lower and upper limit receptively. C11 is constant which depends on mobility pattern/model, nodes walking speed, transmit range, buffer capacity. "n" is

a real number, the value of "n" varies from case to case (The value of n depends on the scenario, walking speed and the number of nodes in the scenario). Eq. 14 implies that if nodes deployed in the small area, which will enhance the ratio of ν. Mobility constant C11 is directly related to ν if nodes move in the opposite direction (towards each others) and inversely related if nodes moves in same direction.

C. RESOURCES CONSUMPTION IN VARIOUS FLOOD ATTACKS

As mentioned earlier in this article that malicious nodes launch flood attacks, which consumed scarce resources, which cause PDR and PLR problems. This section analyzed various flood attack scenarios/use cases.

1) FLOOD ATTACKS SCENARIOS

There are so many types of flood attacks. This article takes three different types of flood attacks for analytic analysis, which are followed as.

a: ATTACK 1

Consider an attack scenario of multiple malicious nodes, which target one benign node to launches flood attack.

b: ATTACK 2

Consider the second attack scenario of multiple attacker nodes, which target multiple legitimate nodes.

c: ATTACK 3

Consider the third scenario of malicious nodes in which one malicious, target multiples innocent nodes.

2) ANALYSIS OF FLOOD ATTACKS

This section analyzed flood attacks. However, before more discussion on flood attacks, this article discussed a mathematical model for analysis.

a: MATHEMATICAL MODEL FOR ANALYSIS

Let BC be a buffer consumption and BWC be a bandwidth consumption and Number of Packets is (Υ).

$$\mathrm{BC} = \mathrm{C12} * \Upsilon \tag{15}$$

$$\mathrm{BWC} = \mathrm{C13} * \Upsilon \tag{16}$$

Under some constant value. But the other hand "Υ" is directly related to Number Of Nodes (ω)

$$\omega = \mathrm{C14} * \Upsilon \tag{17}$$

However, when BC becomes high, so nodes availability becomes low (Nodes do not have the ability to process other packets / accommodate any more packets, so victim nodes becomes unavailable for other nodes), also BC are directly related to PLR.

$$\mathrm{BC} = \mathrm{C15}/\mathrm{Availability}(\eta) \tag{18}$$

$$\mathrm{BC} = \mathrm{C16}/\mathrm{PDR} \tag{19}$$

$$\mathrm{BC} = \mathrm{C17} * \mathrm{PLR} \tag{20}$$

TABLE 2. Analysis of flood attacks.

Scenario	*BWC*	*BC*	*Node-Availability*	*PDR*	*PLR*
Attack 1	Medium	Maximum	Completely down/ Not available	Low/Zero	High
Attack 2	High	Moderate	Medium down/ Partially available	Middle	Medium
Attack 3	Low	Low	Low down/ Available	High Middle	Low

Based on these analysis/observation Table 2 is created. This summarized BC, BWC, Availability, PDR, and PLR in various flood attacks scenarios.

Corollary From Analysis: From the above analysis this article concluded that PDR and PLR depends on buffer, if nodes waste less amount of buffer, so drops ratios becomes less and PDR will be high. This article concluded that resources consumption depends on packet size and number of packets. If number of packets and packets size are reduced, so it will improved the ratios of PDR and PLR (Based on these observation this article proposed RTOC, which consumed less buffer due to compress packets and increased detection accuracy due to contact time with encounter nodes). Furthermore, detection accuracy of rate limit based and encounter based algorithms depends on contact time and contact duration, if researchers enhanced contact time, contact duration, so according to analysis of this article, it will improved detection accuracy. This article recommends, if researchers used new methods other than claims exchange and sharing encounter history, so it will improved detection accuracy and detection time significantly.

D. EVALUATION PARAMETERS

Simulation is evaluated on the basis of parameters discussed below.

1) PDR

It is the ratio between delivered packets and total created packets. If number of delivered packets are NDP and total created packets are TCP then PDR will be calculated as follow.

$$\mathrm{PDR} = (\mathrm{NDP}/\mathrm{TCP}) * 100 \tag{21}$$

2) PLR

It is the total drops packets in the simulation. If a total created packet (TCP), total delivered packet (TDP) then PLR will be calculated with a following formula.

$$\mathrm{PLR} = ((\mathrm{TCP} - \mathrm{TDP})/\mathrm{TCP}) * 100 \tag{22}$$

3) OVERHEAD RATIO (OH)

If total relay packet (TRP) then OH will be calculated as follow.

$$\mathrm{OH} = ((\mathrm{TRP} - \mathrm{TDP})/\mathrm{TDP}) * 100 \tag{23}$$

4) LATENCY

It is the amount of time required from the creation of packets to delivery to destination.

5) AVERAGE BUFFER TIME (ABT)

ABT is the amount of time that messages spend in the buffer. ABT have significant impact on PDR and PLR that why this article considered ABT is very important parameters to judge the efficiency of flood mitigation algorithms (According to our knowledge this one is first article which considered ABT).

6) TOTAL ENCOUNTER (TE)

TE is the total number of the encounters (Contacts) of every node in the simulation (No one calculated TE in proposed mitigation scheme of flood attacks). The ratios of PDR and PLR depends on TE, that is why this article calculates TE in various flood attack scenarios.

7) NUMBER OF ATTACK PACKETS

As mentioned earlier in this article that malicious nodes forwards a large number of packets to overwhelm benign nodes. This article calculated the number of attacks packets of malicious nodes with various strategies (tests, discussed in simulation section).

8) DETECTION RATE/DETECTION ACCURACY

The proportion of attack packets that are detected out of all packets (Malicious nodes forward large number of packets, all packets are not malicious packets. If malicious nodes forward packet above threshold/limit which is actually attack packets. This article detects/calculated malicious packets with various test discussed in simulation section) are called detection rate.

9) DETECTION DELAY

The average time required to detect first malicious packet/malicious node is called detection delay. Detection delay is very important parameter to judge detection algorithms, because few proposed algorithms detects malicious nodes with high time which obviously wastes precious resources until detection. That is why this article calculated detection delay of proposed algorithms.

10) BC

It is total buffer consumed in simulation. If the total buffer is TB, Free buffer is FB and used buffer is UB then UB will be calculated as follow.

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

BC is the most important parameter (because DTNs have scarce resources and the main goal of malicious nodes are to target the buffer of innocent nodes, which ultimately causes PDR and PLR problems). According to our knowledge every researchers in this area claims that due flood attack buffer are consumed, however no one calculates how much buffer are consumed with real simulation results. This article calculated BC of our detection algorithms by various strategies (tests).

11) TWT/BWC

It is the average amount of bandwidth consumed in the simulation. When source node forwards packets to destination nodes obviously it waste bandwidth, which is very important to calculates. This is because malicious nodes forwards large number of packets as compared to benign nodes that is why it waste a lot of bandwidth. According to our knowledge, researchers did not calculated wasted bandwidth in flood mitigation algorithms, however this article calculated bandwidth consumption of nodes in flood attack with various tests. If total relayed packets are TRP, total aborted packets TAP, total sender aborted packets TSAP, total receiver aborted packets is TRAP and size of packets in Kb is (SPK) then TWB will be,

$$\text{TWT} = ((\text{TRP}) + (\text{TAP})) * (\text{SPK}))/1000 \tag{25}$$

1000 in the above formula convert Kb to M directly. In the above formula, TAP are those packets which are relayed but immediately aborted. TAP waste bandwidth but these packets are not included in drops. Actually, there are two categories of aborted packets, that is sender aborted and receiver aborted. TAP in above formula are actually sender aborted. If TAP are receiver aborted then Eq. 25 will becomes

$$\text{TWT} = ((\text{TRP}) + ((\text{TSAP}) - \text{TRAP}) * (\text{SPK}))/1000) \tag{26}$$

III. REVAMP TO LIE OR COMPLY (RTOC)-A1

This article proposed enhanced version (compression based) of existing rate limit [36] based algorithm to thwart PDR and PLR.

In RTOC initially every node send a request message to TA for RLC. TA give sign RLC according to nodes requirements (changes with time). Every node itself counts its own packets like [36]. Nodes create P-Claim (Packet count claim that is how many packets is forwarded), and T-Claim (Transmission count, How many replicas of the same packet are forwarded, Process hop-by-hop), for more detail refer [36]. Nodes append P-Claim and T-Claim with packets. Every node compress packets without P-Claim and T-Claim with Huffman coding. This article chooses loss-less Huffman coding for compression. Then node forwards packets to destination nodes. Destination nodes cross-check P-Claim and T-Claim. If claim verify, node assume the packet (Node) is legitimate, then decompress the packet. If any inconsistency found in packets claim, nodes assume the packet is coming from malicious nodes. Nodes report the signer of that packet to TA. TA create a signed message and forwards to all nodes in the networks about malicious nodes. The proposed algorithm detects and mitigates all those malicious nodes which alter P-claim and T-claim.

Algorithm 1 RTOC-A1Input: Malicious Packet Output: Detection of Malicious Packets

```
0 : PhaseOne :
1 : Every node share Public key with TA and with other nodes.
2 : Every node send RP to TA for RLC
3 : TA Grant RLC to every nodes according to request requirement for specific time/Change with a time
PhaseTwo :
4 : if have a message to forward then
    5 : Generate P-Claim for New Packets and T-Claim for Every Packets, Compress Packets Without P-Claim and T-Claim, Append P-Claim, T-Claim with Compress Packet and Forward Packets else
        Go to Step 4
X : End of If
PhaseThree :
6 : if Receiver Receive message then
    if Verify Sign, P-Claim, T-Claim then
        Go to Step 10
    else
        Go to Step 7
        X : End If
    7 : Attack Detected
    8 : Report to TA
    9 : TA create sign packet and Forward to all node about malicious node
    10 : No Attack Detected
    11 : Decompress Packets
X : End of if
12 : End of Algorithm
```

This article simulates the proposed algorithms an opportunistic network environment (ONE) [47] simulator (ONE is java based simulator which is specifically design for DTNs).Proposed algorithm significantly enhanced PDR and PLR relative to [36]. This is just because of the fact of compression, which consumed little buffer, bandwidth, and energy relative to [36] (Prove of this will be given in the simulation section, how much buffer, bandwidth and energy are consumed in both [36] in our proposed algorithms). Detection accuracy is a little bit enhanced with our RTOC, due to less consumption of resources. The algorithm [36] exchange packet claims along with all packets (which is not compressed), which consumed more buffer. Some time nodes exchange claims which are dropped, due to buffer overloading, which implies that detection accuracy will be low. Unlike algorithm [36] our RTOC forwards compress packets. If claim verify then our RTOC decompress packet, which consumed less buffer of every node. That is why claim verification packets are not dropped due to buffer scarcity, which enhanced detection accuracy and detection time.

A. SIMULATION SET-UP

This article has analyzed the performance of RTOC for misbehavior nodes in DTNs, through various evaluation techniques. Evaluation is completed with the help of simulation. The proposed RTOC is compared with state-of-the-art algorithms. Simulation is carried out on the parameters given in the Table below. Table 3 summarized parameters for RTOC.

TABLE 3. Simulation parameters list for RTOC.

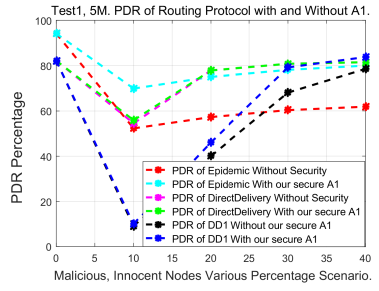
Parameter	Assign-Value	Parameter	Assign-Value
Movement Model	RWP	TTL	300
Area	500 * 500	Message wait time	0, 120
Buffer Size	5 MB	Router	Epidemic
Bandwidth	2 Mbps	Router	Direct Delivery
Moving speed	1, 1.6	Router	DD1
Transmit Range	10 M	Number of Group without malicious	1
Simulation Time	50000	Number of Group with malicious node	2
Number of Nodes	100	update interval	0.1
Simulator	ONE	Packet Compression	Almost 50 Percent

B. SIMULATION RESULTS

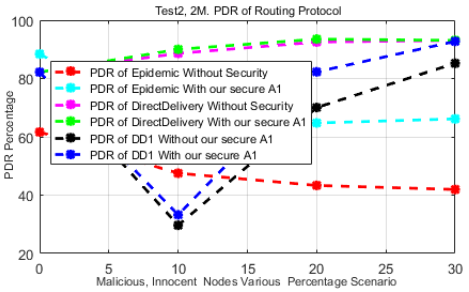
1) EXPERIMENT 1

In experiment 1 this article calculated PDR, AL, and OH by two tests, that is Test 1 (When Nodes have a 5M buffer) and Test 2 (When Nodes have a 2M buffer). Fig. 1(a) and Fig. 1(b) shows PDR with various routing protocols (This article only shows the results of the epidemic, direct delivery and DD1, other protocols show similar results). PDR is approximately 80 to 97 percent (in Test1) and 61 to 80 (in Test2) percent of all routing protocols, when there are no malicious nodes. When five percent of malicious nodes are deployed PDR is suddenly decreased and the graph becomes below fifty percent (this article only shows PDR due to page limitation. PLR = 100-PLR). Simulation result shows our proposed RTOC enhanced PDR and PLR, due to less BC. Simulation results show that there is an almost negligible effect on PDR and PLR, with Direct Delivery. Because, Direct Delivery only transfers message to the destination directly, which do not consume too much buffer. If buffer is not consumed so there is an almost negligible effect. First Contact also shows almost the same results.

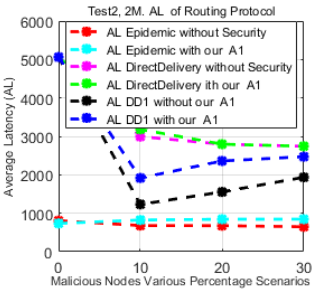
This article enhanced the capability of malicious nodes in direct delivery to forwards more messages as compared to ordinary malicious nodes. This article called this Direct Delivery With Enhance Flood Capability (DD1). This article set the ratios of messages creation of normal, ordinary malicious and extraordinary malicious nodes are 25, 5 and 1 seconds respectively. In case of this extraordinary capability of malicious nodes, buffer are a little bit more consumed than Direct Delivery. Which decreased PDR and increased PLR. Simulation result shows in Fig. 1(a) and Fig. 1(b) our RTOC performs better in term of PDR and PLR. A1 shows approximately 4 to 6 percent (Test1) and 4 to 18 (Test2) enhancement in PDR and PLR.



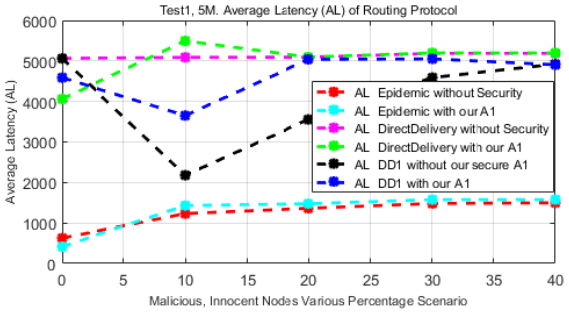
(a) PDR (Test1)



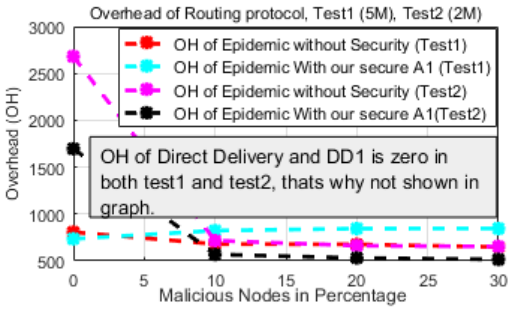
(b) PDR (Test2)



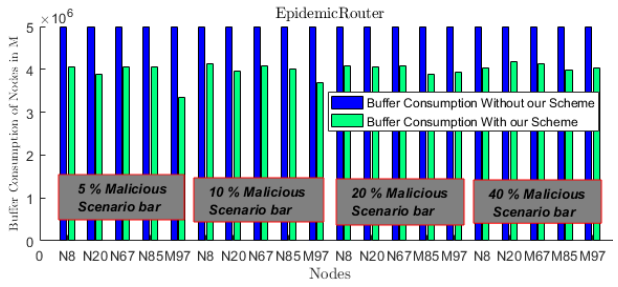
(c) AL (Test2)



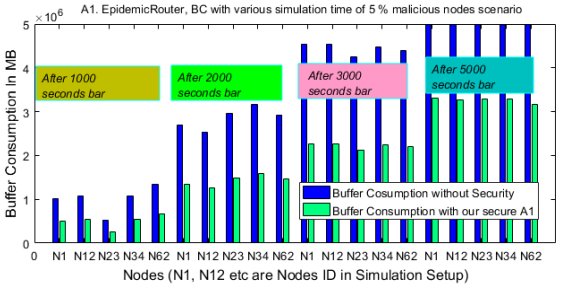
(d) Average Latency (Test1)



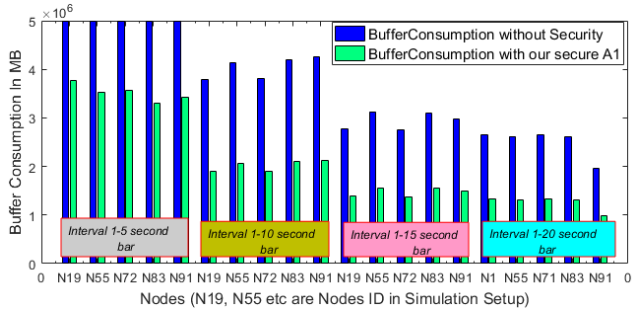
(e) Overhead (Test1, Test2)



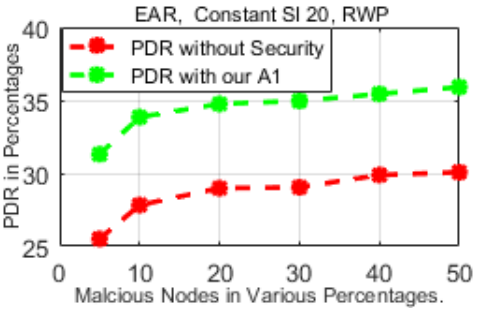
(f) BC with various malicious nodes scenarios (Test1)



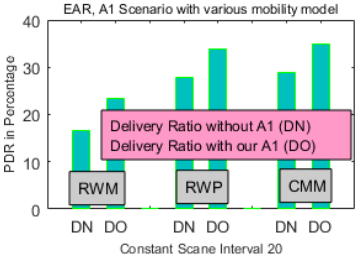
(g) BC after different simulation time (Test2)



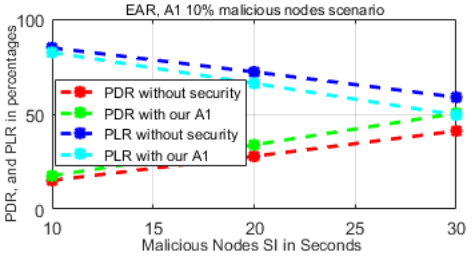
(h) BC with various message creation interval (Test3)



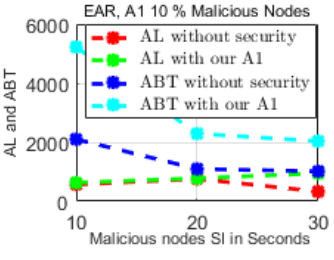
(i) PDR/PLR with various malicious nodes scenario (Test1)



(j) PDR/PLR with mobility model (Test2)



(k) PDR/PLR with various Scan Interval of nodes (Test3)



(l) AL,ABT with SI(Test4

FIGURE 1. Simulation results.

Fig. 1(d) and Fig. 1(c) shows the simulation results of AL of various routing protocols. Simulation results show that AL of RTOC is dis-improves. This is because of the extra processing of huff-man coding in sender side, malicious nodes detection and decompression of packets in the receiver side. The packets spend more time in the buffer that is why AL becomes high. Fig. 1(e) shows simulation results of OH of the epidemic router in both test1 and test2. Simulation results clearly show that OH is improved of A1 because malicious nodes are mitigated (if malicious nodes are detected then OH on link reduced automatically).

Corollary From Experiment 1: Simulation results of various nodes scenarios show different results because scenarios are totally different (In 10 percent malicious nodes scenario, 10 malicious nodes and 90 innocent, in 20 percent malicious scenario there are 20 malicious and 80 innocent etc). From simulation this article concluded that PDR is directly related to buffer size (PDR of 5M is higher than 2M buffer).

2) EXPERIMENT 2

In experiment 2 this article calculated BC with various strategies that is with different malicious nodes scenario (Test1), with various simulation time (Test2) and with various malicious nodes message creation interval (Test3)

Most of the researchers analyzed that due to flood attacks resources (Buffer, bandwidth, and energy) are consumed. However, according to our knowledge, no one shows how much are consumed with simulation results in flood attacks. This article calculated BC of all nodes, however, there are hundred nodes in our scenario in A1. That is why for illustration this article select randomly five nodes in 5, 10, 20 and 40 percent malicious nodes scenario. Fig. 1(f) shows simulation results of BC of various malicious nodes scenarios.

Fig. 1(g) shows BC of 5 percent malicious nodes scenario with various time in the simulation. This article also calculates, BC of 5 percent malicious scenario with various messages creation interval of malicious nodes (after constant simulation time 2000 seconds). This article takes message creation interval of benign nodes 20-30 seconds constant and message creation interval of malicious nodes 1-5, 1-10, 1-15 and 1-20 seconds. For illustration purpose, this article only shows the result of 5 (due to page limitation chose 5 nodes, all nodes show similar results) different nodes which are randomly selected after simulation. Fig.1(h) shows the simulation results of malicious nodes with various message creation interval. For illustration purpose, this article shows BC of epidemic router other routing protocols also shows the same type results.

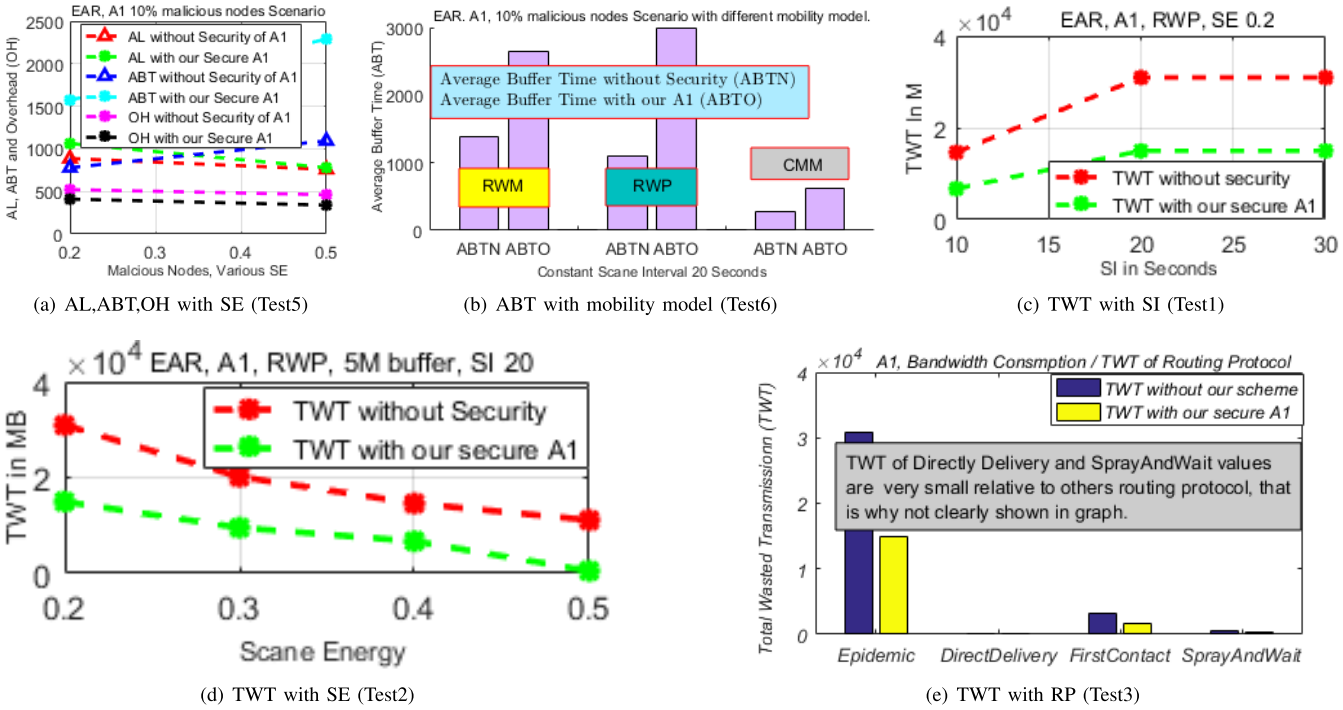
Corollary From Experiment 2: Simulation results show that in each use case RTOC consumed less buffer, that is why PDR and PLR are improved. This article already proved in the analysis section that BC is inversely proportional to PDR. This article also observed from simulation results that BC is increased with simulation time. Simulation results also show that BC is inversely related to message creation interval.

3) EXPERIMENT 3

In experiment 3 this article calculated PDR, PLR, AL, ABT and OH. This article calculated PDR, PLR with various malicious nodes scenarios (Test1), with various mobility model (Test2) and with various Scan Interval (SI) (Test3) of malicious nodes. This article also calculates AL, ABT and OH with nodes SI (Test4), nodes Scan Energy (SE) (Test5) and mobility model (Test6). Most of the researchers claim that due to flood attacks, energy is consumed, however according to our knowledge no one calculated in flood attacks (which is already mentioned in this article). When malicious nodes forward packets in flood attacks it wastes the energy resources of benign nodes, the benign nodes becomes down which create various problems including PDR and PLR. This article simulates various flood attacks scenarios without and with our A1 to give some specific energy to each node. Due to flood attacks, nodes consumed more energy so ultimately cause PDR and PLR problems. Simulation results show that our proposed A1 consumed less energy, which enhanced OH, ABT which further enhanced PDR and PLR. AL is dis-improved due to compression in sender side, detection, and decompression of packets in the receiver side.

This article set different simulation parameters to calculate EC. The parameters are followed as, initial energy 500, EnergyAwareRouter (EAR) is routing protocol and various SE and SI mentioned on top or in the bottom of each simulation graphs. Fig. 1(i) shows our A1 improved PDR significantly with various malicious scenarios. Because A1 consumed less energy so it improved nodes lifetime. Fig. 1(j) shows that our algorithm enhanced PDR in various mobility model. Fig. 1(k) shows our proposed A1 performs well to improved PDR in various SI of nodes, due to less EC. Fig. 1(l) shows the simulation results of AL and ABT with SI. Simulation results show that A1 improved ABT, which further enhanced PDR. AL is dis-improved with A1. Fig. 2(a) shows the simulation results of AL, ABT and OH. Simulation results show A1 improved ABT and OH. Fig. 2(b) shows a simulation of ABT with various mobility model. Simulation results proved that proposed A1 performs well to enhanced ABT with various mobility model.

Corollary From Experiment 3: This article simulates PDR, PLR, ABT and AL with different SE and SI (actually by giving some specific energy this article checked node life time because when nodes consume more energy so it will quickly becomes down which affect the ratios of PDR and PLR). From simulation results, this article concluded that our RTOC prevent a malicious node that is why it consumes less energy so it improved PDR and PLR. From simulation results this article concluded that PDR of CMM are greater than all model (because nodes moves in very small area cluster, it forwards more packets that is number of encounters are higher than all model due to small area) and PDR of RWM is less than all model (In RWM nodes moves randomly in large area). PDR is directly related to a number of encounters. This article also observed from simulation results that PDR are directly related to SI because if SI is high so nodes consumes



(a) AL,ABT,OH with SE (Test5)

(b) ABT with mobility model (Test6)

(c) TWT with SI (Test1)

(d) TWT with SE (Test2)

(e) TWT with RP (Test3)

FIGURE 2. Simulation results.

less energy so ultimately enhanced PDR, PLR and ABT. This article also observed if SE is increase so it will increase the value of ABT. This article also observed from simulation results that ABT of RWP is higher than other movement model because nodes walk randomly in a large area, so the probability of BC is less (forwards fewer packets). Actually, in RWP packets spend more time unlike CMM. In CMM nodes walk in the small cluster so it will forwards more packets to other nodes, which consumed the buffer of that particular node. That is why PLR becomes high in CMM so ultimately it will decrease ABT.

4) EXPERIMENT 4

In experiment 4 this article simulate TWT/BWC with a various Test. This article calculated TWT with SI (Test1), nodes SE (Test2) and with various routing protocol (Test3). Fig. 2(c) shows the simulation results of TWT with nodes SI. Simulation results show A1 consumed minimum bandwidth in flood attacks. Fig. 2(d) shows the simulation results of TWT with various SE. Simulation results clearly show that BWC of A1 is minimum. Fig. 2(e) shows the simulation results of TWT with various routing protocols. Simulation results show that A1 enhanced TWT with routing protocols.

Corollary From Experiment 4: This article observed from simulation results that TWT are directly proportional to SI and inversely related to SE. Because if SI is high so nodes consumed minimum energy and forwards more packets, so ultimately it will increase TWT. If SE is high so nodes consumed more energy it will decrease nodes lifetime (transmit fewer packets, and scan less packets), so ultimately decreased BWC. Simulation results show that epidemic consumed more bandwidth and direct delivery consumed less bandwidth.

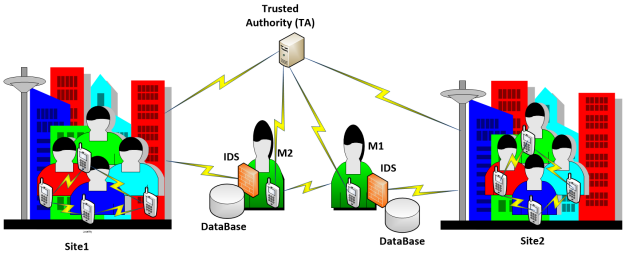


FIGURE 3. Flood attack in two sites/city scenario.

IV. INTER-SITE FLOOD ATTACK MITIGATION (IFAM)-A2

Consider an attack scenario of malicious nodes in Fig. 3 which launches flood attacks. There are two sites of DTNs which are connected by a link.

There are nodes in the middle of the connecting link, which forwards packets between two sites. For illustration this article deployed two nodes, M1 and M2 in the figure, however in reality, there are more than two nodes. The resources of M1 and M2 are very important relative to others. Because the whole network depends on M1 and M2. If M1 and M2 down due to flood attacks, it means the whole network becomes down. Malicious nodes launch flood attacks to target M1 and M2 to overused limited resources of M1 and M2. This article proposed A2 which save resources of M1 and M2 which enhanced PDR and PLR. Before more discussion on the working of A2, this article makes some assumptions which are follow as. During initial set up, IDS are deployed

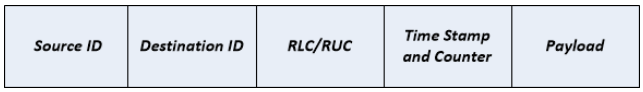


FIGURE 4. Packet format.

in forwarder nodes (M1, M2 etc in this case). Every IDS generates key, Only TA knows that key (TA also have that algorithm which generate that key).

Packet Format: Every node send packets with a specific format. Fig. 4 is a packet format. Every node adds source id, destination id, payload, and RLC/RUC. Every node encrypts only payload part with the private key. When "A" forwards a packet to "B", "B" forwards a packet to "C", so in this case "A" sign a packet then "B" also sign a signed packet ("A" already sign this packet).

Network Set Up Phase: During network set up phase, every node except IDS base nodes send a Request-Packet (RP) to TA for RLC. TA grant sign RLC to every node except IDS based nodes. IDS based nodes generate key and append with RP then forwards RP to TA. TA verify ids key, then grant sign Rate-Unlimited-Certificate (RUC) to IDS based nodes. RUC is an unlimited certificate, which means IDS based nodes have permission to forwards unlimited packets.

Forwarding Phase: In the forwarding phase, every node encrypts only the payload portion with the private key. Every node forwards a packet along with RLC except IDS based nodes, which forwards packets with RUC. IDS based nodes have a database. When nodes forward packets to IDS based nodes, IDS based nodes verify RLC, sender node sign. If both verify then IDS based nodes counts packets, save counts value in front of nodes public key in the database and decrease RLC by 1. Then forwards packets of forwarder nodes to the required destination. If node "A" forwards a packet to "B" and "B" forwards a packet to M1. Both nodes sign a packet, M1 decreased the count of original sources which is "A" in this case (fair system). If any inconsistency found in both RLC and the private key of nodes, IDS based nodes report that node to TA. TA create a signed message forwards to all nodes in networks to blacklist malicious nodes.

A. CRYPTANALYSIS OF A2

Consider an attacks scenario on A2. If malicious nodes forward five packets to one IDS based node and five to other IDS based node and packet limit are five packets, this type of attacks is detected. Because after some specific time IDS based nodes share forwarding history to each other. If one node forwards packets more than limit with the help of more than one IDS based nodes, so after history sharing that particular malicious nodes is detected because of time-stamp. If malicious nodes changed time-stamp, this type of attack is also detected because IDS based nodes add owns (when received packets add receiving time) time-stamp, compare packets with its receiving time. The proposed algorithm exactly detects the malicious nodes and blacklist malicious nodes which launches a flood attack. The proposed A2 also have the ability to detect colluding attacks.

Algorithm 2 IFAM-A2 Input: Malicious Packet Output: Detection/Prevention of Malicious Packets

```
0 : PhaseOne :
1 : Every node share Public key with TA
2 : Ordinary node send RP to TA for RLC
3 : TA Grant RLC to every node except IDS based nodes
4 : IDS base node append key with RP and forward to
TA for RUC
5 : TA generate same key like IDS based nodes
6 : if verify then
|   7 : Grant RUC
8 : else
|_  9 : Goto step 23
X : End If
PhaseTwo :
10 : if have a message to forward then
|   11 : Sign packet and append RLC/RUC then forward
12 : else
|_  13 : GO to Step 10
X : End If
PhaseThree :
14 : if Receiving node is IDS base nodes then
|   15 : Verify RLC and Sender private key
|   16 : if both Verify then
|   |   17 : Save count in Database (Number of packets,
|   |   time stamp, node ID), Decrease RLC by 1 and
|   |   forward packet Go to Step 25
|   |   18 : else
|   |   |_  19 : Goto step 23
|   X : End If
|   20 : else
|   |   21 : Sign packet with Private key (because node
|   |   is not IDS, it is ordinary node)
|   |_  22 : Go to Step 10
X : End If
23 : Report To TA
24 : TA create sign packet forward to all node, and black
list malicious nodes. Go to 28
25 : Node is legitimate, forward its packets.
26 : if If time is specific (defined time) then
|   27 : IDs nodes share history with other IDS nodes
X : End If
28 : End of Algorithm
```

B. SIMULATION SET UP

This article simulates A2 with slightly different parameters used in A1. This article takes total 25 nodes with 5 malicious and 20 legitimate nodes for A2 in three different groups with 3 M buffer size, 25 wait time interval and with RandomWay-Point mobility model in ONE Simulator. Site 1 contains 10 nodes, site 2 contain 10 nodes and 5 nodes in the middle which transfer messages between two sites.

C. SIMULATION RESULTS

In this section results gained of A2 are discussed.

1) EXPERIMENT 5

In experiment 5 this article calculated PDR, PLR, and BC of various nodes with various tests. This article calculated PDR, PLR with routing protocol (Test1) and BC of middle nodes with the epidemic router (Test2). Fig. 5(a) shows simulation results of PDR and PLR. In the horizontal side of the graph, nodes are shown with various routing protocols. Simulation is carried out on Epidemic without our scheme (EM), Epidemic with our secure scheme (EO), FirstContact without our scheme (FM), FirstContact with our secure scheme (FO), DirectDelivery without our scheme (DM), DirectDelivery with our secure scheme (DO), SprayAndWait without our scheme (SM), SprayAndWait with our secure scheme (SO). Simulation results show our proposed A2 enhanced PDR and PLR significantly in flood attacks.

Fig. 5(b) shows the simulation results of BC. Simulation results generated after 1000 seconds. For illustration, this article shows BC of the epidemic router, all others routing protocols shows similar results. Horizontal side of the graph shows the middle (forwarder nodes) and average BC. Simulation results show that our secure A2 saves buffer of middle nodes, that is why PDR and PLR are improved.

Corollary From Experiment 5: Actually malicious nodes target middle nodes. This article observed PDR of SprayAndWait is high relative to other protocols, due to less BC (SprayAndWait, wait sometime after spray phase).

2) EXPERIMENT 6

This article calculated TE, TWT, and the number-of-attack packets with SE (Test1) and SI (Test2). This article also calculated TWT with various routing protocols (Test3). Experiment is done on EAR, with transmitting energy 0.1, SE and SI mentioned at the top of each graph. Fig. 5(c) shows simulation results of TE, TWT, and number-of-attacks packets with various SE. Fig. 5(d) shows simulation results of TE, TWT, and number-of-attacks packets with various SI. Simulation results of both test1 and test2 show that TWT is improved with our A2 (because A2 prevent malicious nodes). Simulation results also show that a number-of-encounters are less in A2 which implies our A2 prevent malicious nodes packets. Fig. 5(e) shows the simulation results of TWT with various routing protocols. Simulation results show that the epidemic consumed more bandwidth relative to other protocols. BWC of Direct Delivery is less relative to all other protocols. Simulation results show that in flood attacks our proposed A2 performs well to consumed less BWC with all protocols.

Corollary From Experiment 6: From simulation results this article observed number-of-encounters are directly related to SI and inversely to SE. Because when SI is high, nodes consumed less energy which enhanced nodes lifetime so number-of-encounters are increased. When SE is high so nodes becomes quickly down, that is why the number-of-encounters decreased, which ultimately decreased PDR. Simulation results also show TWT is directly related to number-of-encounters.

3) EXPERIMENT 7

This article calculated PDR with various mobility model (Test1) and PDR with various SE (Test2). This article also calculated PDR, TE, and number-of-attack-packets with various simulation time (Test3), with nodes walking speed (Test4) and nodes deployments in simulation (Test5).

Fig. 5(f) shows simulation results of both A1 and A2 with various SE. Simulation results show A2 improved PDR. Fig. 5(g) and Fig. 5(h) shows simulation results of PDR, TE and number-of-attack-packets with simulation time and nodes walking speed respectively. Simulation results shows proposed A2 enhanced PDR. Also, TE is less in A2 which proved that our A2 prevent malicious packets. Simulation result also shows a number-of-attack-packets which are detected and prevented in our proposed algorithm. Fig. 5(i) shows the simulation results of PDR with various mobility model. simulation results show A2 enhanced PDR with all model, due to less BC.

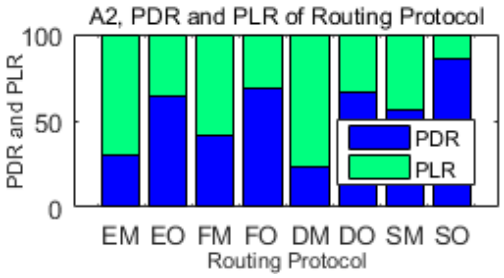
Fig. 5(j) shows simulation results of PDR, TE, and number-of-attack-packets with two different use cases. In case 1, middle nodes are mobile and sites nodes are static. Malicious nodes are deployed randomly but static in this case. In case 2 middle nodes are static, sites nodes are mobile. The attacker nodes are randomly deployed in this case but mobile in this case. Simulation results of both cases show our A2 improved PDR, TE and also detect some attack packets.

Corollary From Experiment 7: Simulation results clearly shows that PDR of CMM are greater than all mobility models and PDR of RWM are minimum relative to other models (reasons are already given in simulation of RTOC). It is also clear if malicious nodes are randomly and dynamically deployed so it detection probability increases because it improved number-of-encounters, which further improved detection probability. From simulation, this article observed that TE is increased with simulation time, which also increased PDR and attack detection. It is clear from a simulation that node walking speed is directly proportional to PDR (Speed improved number-of-encounters).

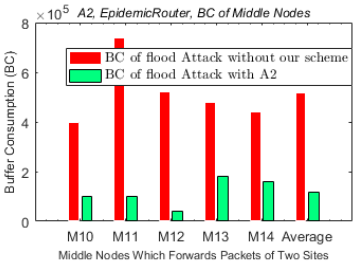
4) EXPERIMENT 8

In this experiment, this article shows AL, ABT and OH with various SE (Test1). Results show that OH and ABT are improved with our A2, which enhanced PDR, PLR, TWT, BC, and EC. AL is dis-improve with A2 because IDS are deployed which checked every packet and create MAC. Fig. 5(k) shows the simulation results of AL, ABT and OH with SE.

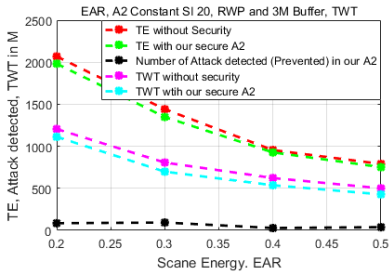
Corollary From Experiment 8: It is clear from a simulation that our IFAM improved ABT because it prevents malicious attacker nodes. BC is minimum so ABT is increased, which further improved PDR. This article observed from simulation that SE is inversely related to OH and TWT. This is because when SE is increased, so nodes quickly died, which decreased TWT and OH.



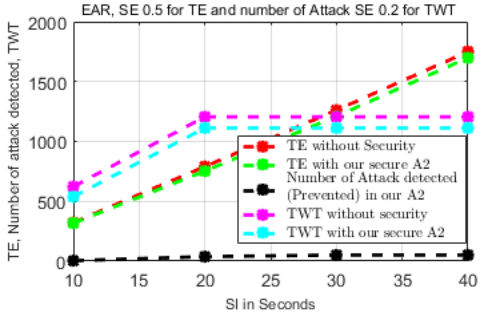
(a) PDR and PLR of A2 (Test1)



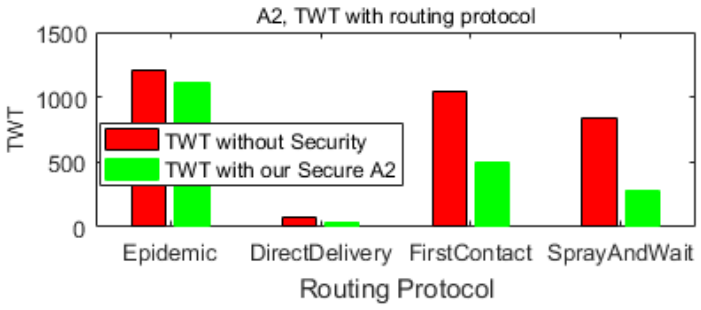
(b) BC of Middle nodes (Test2)



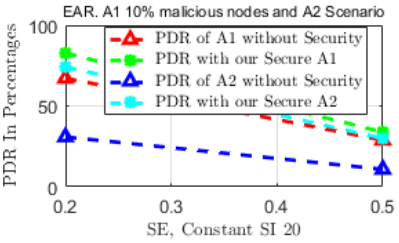
(c) TE, TWT, Attack Packets with SE (Test1)



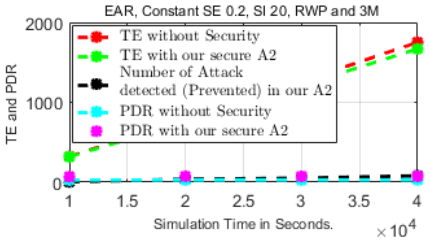
(d) TE, TWT, Attack Packets with SI (Test2)



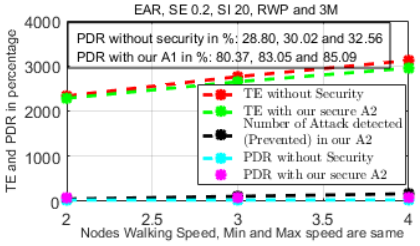
(e) TWT with Routing protocol (Test3)



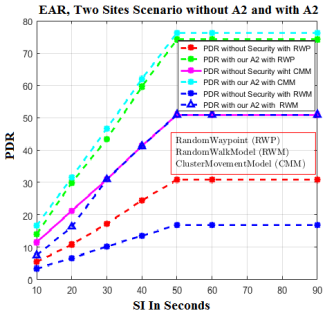
(f) PDR of A1, A2 with various SE



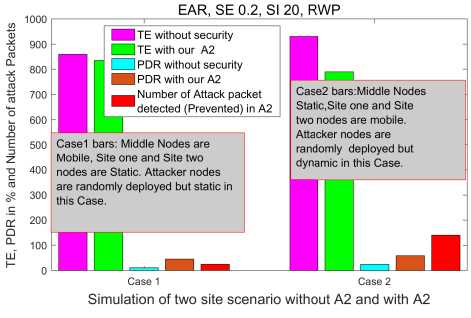
(g) PDR, TE, Attack Packets with simulation time (Test3)



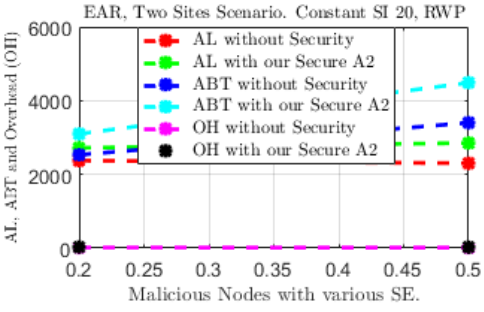
(h) TE, Attack packets with walking speed (Test4)



(i) PDR with mobility model



(j) TE, PDR and Attacks with use cases (Test5)



(k) AL, ABT and OH with nodes SE (Test1)

FIGURE 5. **Simulation results.**

V. HOLISTIC FLOOD ATTACK MITIGATION (HFAM)-A3

Consider a generic attack scenario of malicious nodes in Fig. 6. There are various innocent nodes. Malicious nodes target legitimate nodes to overused scarce resources by launching flood attacks. This article enhanced A2 for the generic scenario. Before more discussion on A3, this article takes some assumptions which are followed as.

- An every legitimate node there is agent-based IDS.
- Every IDS generate a same random number (Key).
- Malicious node does not have the ability to create that key.

Initial Set Up Phase: This article proposed preventive based mitigation algorithm to thwart flood attacks. In the initial set up of the networks, every node shares public key with TA and other nodes. Every node forwards RP to TA for RLC. TA grant RLC sign with the private key to every node for a specific time. During initial set up, IDS is deployed in every node. In IDS there is a database where they store, counts

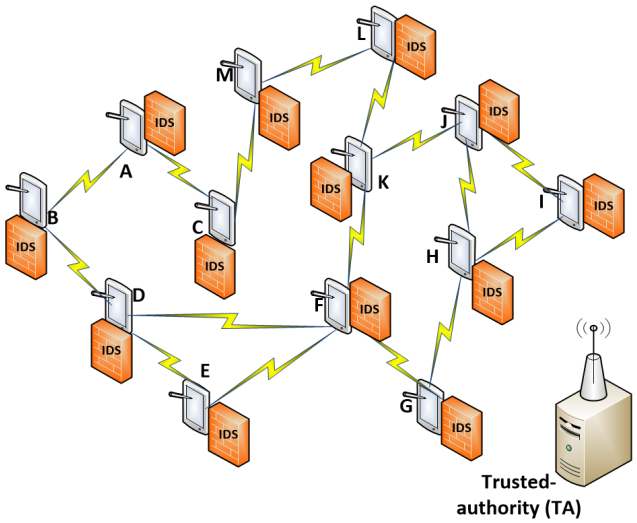


FIGURE 6. Flood attack in generic scenario.

packets of each node. IDS generate a unique key which they append with packets.

Forwarding Phase: Every node appends RLC with sign packets before forwarding. Every packet pass into IDS. IDS verify RLC and generate a unique key with SHA 1 algorithm. Every IDS appends key with packets and make a hash of packets. Actually which is MAC (Hash with Key). IDS forwards original packets along with MAC, and decrease count value by 1 in the database. When the receiver IDS receive packets, they verify sign and RLC. When both sign and RLC verify, IDS generate same key append with packets and make a hash of that packets. IDS compare MAC with original MAC. If verify it means packet (Node) is benign, no attack is detected, otherwise, attack is detected. IDS report malicious node to TA, TA forwards sign packets about malicious nodes in the networks and blacklist the malicious nodes.

A. CRYPTANALYSIS OF A3

Consider an attacks scenario on A3. If malicious nodes either bypass IDS or create its own IDS. But in both cases, malicious nodes are detected because they do not have unique secret key. Also the proposed algorithm detects colluding malicious attacker nodes.

B. SIMULATION SET UP

This article simulates HFAM with slightly different parameters used in RTOC and IFAM. This article takes total 20 nodes with 5 malicious and 15 innocent nodes for A3 in two different groups with 30 wait time interval, group speed 1, 2 and with various mobility model in ONE Simulator. Group 1 contain 15 legitimate nodes, group 2 contain 5 malicious nodes which launches flood attacks.

C. SIMULATION RESULTS

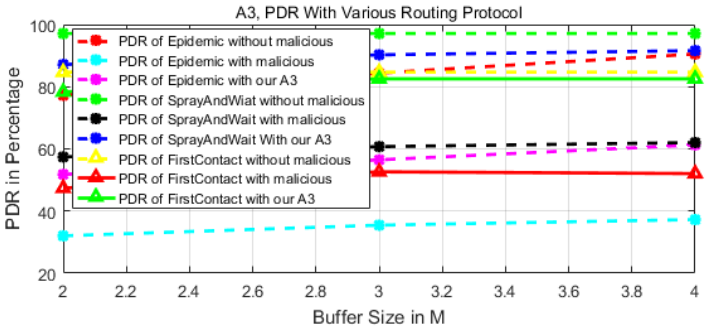
In this section results of A3 are discussed.

Algorithm 3 HFAM-A3 Input: Malicious Packet Output: Detection/Prevention of Malicious Packets

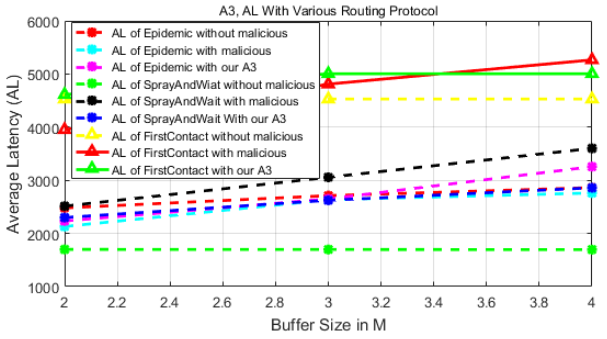
0 : *PhaseOne* :
1 : Every node shares Public key with TA and with other nodes.
2 : Every node send RP to TA for RLC
3 : TA Grant RLC to every nodes according to request requirement for specific time/Change with a time
PhaseTwo :
4 : **if** *if have a message to forward* **then**
  5 : Sign packet and append RLC then forward
6 : **else**
7 : GO to Step 4
X : End If
PhaseThree :
8 : Sender node IDS Verify RLC
9 : **if** *Verify* **then**
  Generate a key append with packet, make hash of Packets (MAC), Decrease count by 1 in Database and forward a packet along with MAC.
10 : **else**
  Goto Step 13
X : End If
PhaseFoure : *Receiverside*
11 : Receiver IDS receive a message
12 : **if** *Verify sender sign, RLC and create MAC of packets with same Key, Compare both MAC, If verify* **then**
  Node is legitimate, No attack detected
  Go to Step 15
else
  Attack Detected.
  Go to Step 13
X : End If
13 : Report to TA
14 : Create a sign message, forward to all nodes about malicious node and black list it.
15 : End of algorithm.

1) EXPERIMENT 9

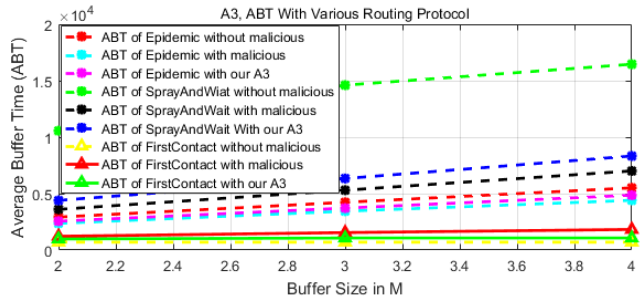
In experiment 9 this article calculated PDR, AL, ABT, TWT, and BC with various tests. PDR (test1), AL (test2), ABT (test3) and TWT (test4) with various routing protocols. Also calculated BC with various simulation time (test5), BC with various mobility model (test6) and BC with the different deployment of normal, malicious nodes in scenarios (test7). Fig. 7(a) (test1) shows the simulation results of PDR. For illustration, this article only shows simulation results of Epidemic, SprayAndWait, and FirstContact. Simulation results clearly show that when malicious nodes launch flood attacks, PDR of all routing protocols is decreased. It is clear from a simulation that our A3 stops malicious nodes, which enhanced PDR. Fig. 7(b) shows simulation results of AL. Simulation results show that AL of our HFAM is dis-improved in case of Epidemic and FirstContact like RTOC and IFAM (reasons of this is already mentioned in



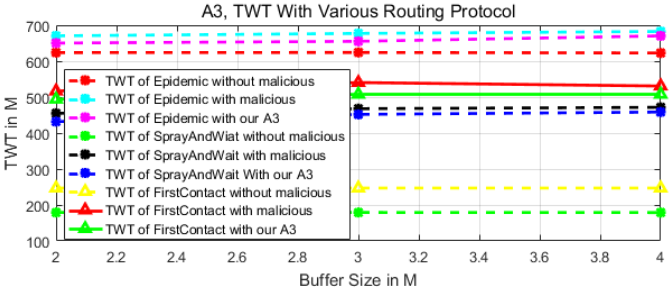
(a) PDR with various routing protocol (test1)



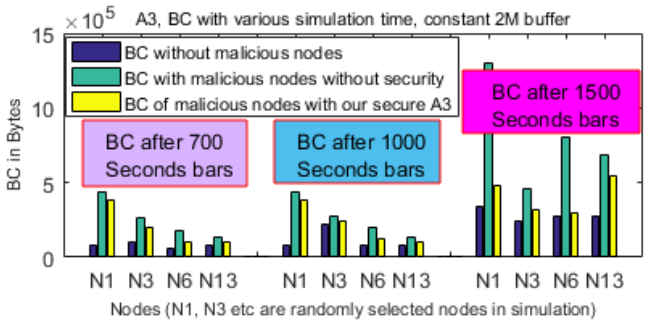
(b) AL of A3 with routing protocol (test2)



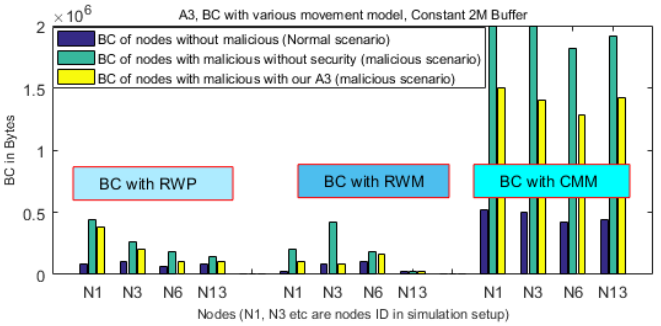
(c) ABT with routing protocols (test3)



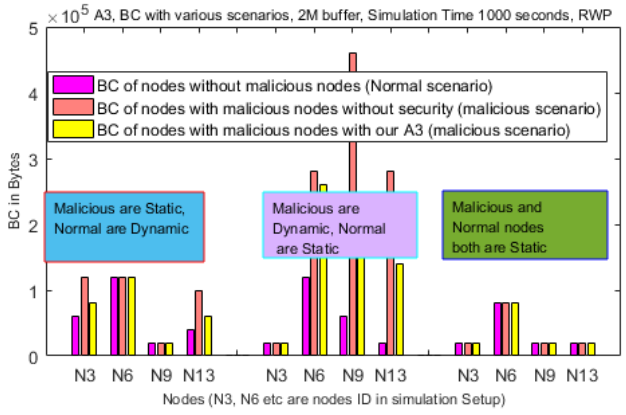
(d) TWT with routing protocols (test4)



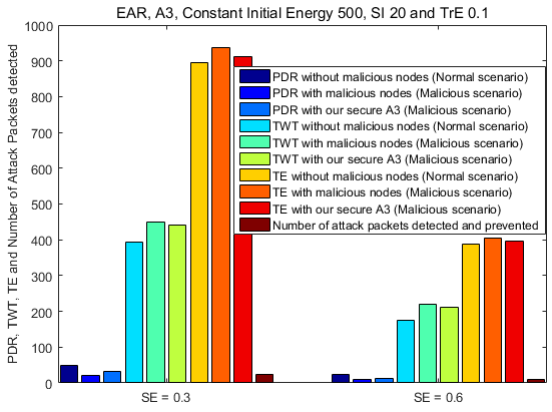
(e) BC with simulation time (test5)



(f) BC with various mobility model (test6)



(g) BC with different deployment of nodes in scenario (test7)



(h) PDR, TWT, TE and attacks detection with SE (test1)

FIGURE 7. Simulation results.

RTOC, IFAM simulation results). AL of SprayAndWait is a little bit improved in our A3, this is because SprayAndWait spray packets then wait some time, our algorithm stop malicious nodes, drops ratios decreased which enhanced AL.

Fig. 7(c) shows simulation results of ABT. Results show that proposed A3 enhanced ABT because A3 stops malicious nodes which launches flood attacks. When malicious nodes launch attacks buffer becomes full of malicious

packets, so it will increase drops ratios (nodes are not available which decreased ABT). A3 prevent malicious nodes which enhanced buffer capacity, so packets spend more time in the buffer which further enhanced PDR. Fig. 7(d) shows the simulation results of TWT. Simulation results show that when malicious nodes launch flood attacks so TWT becomes very high. It is clear form simulation that our A3 prevent malicious attacks, which ultimately enhanced TWT. Fig. 7(e), Fig. 7(f) and Fig. 7(g) shows simulation results of BC with various simulation time, various mobility model and various deployment of nodes in scenarios respectively. It is clear from simulation results that our proposed A3 prevent malicious nodes, which consumed less buffer like RTOC and IFAM. Which ultimately improved PDR and PLR due to less BC.

This article also deduct from simulation results when malicious nodes are dynamically deployed and normal nodes are static, so it consumed high amount of buffer relative to others scenarios. Because malicious nodes move which consumed buffer of almost every innocent nodes. It is also clear from simulation when both malicious and normal nodes are static it consumed less buffer relative to others scenarios. Because when nodes are static so there is the probability that malicious nodes consumed buffer of very less number of nodes. When malicious nodes are static and normal are dynamic so the probability of BC are less relative to first scenario (in which malicious are dynamic).

Corollary From Experiment 9: From simulation results, this article concluded that PDR of the epidemic is mostly effected relative to other protocols when malicious nodes launch attacks. Epidemic also consumed more resources (buffer, TWT and energy) relative to other protocols. PDR of SprayAndWait is higher than other protocols because it consumed less buffer which enhanced PDR. It is also clear from simulation results that AL of FirstContact is high relative to other protocols because it forwards packets to first contacted nodes, which takes a long time reached to destination. AL of the epidemic is high relative to SprayAndWait because epidemic consumed buffer, which causes low PDR and high PLR. That is why AL of the epidemic is high due to high PLR. From simulation results, this article concluded that TWT of the epidemic are higher than other protocols and TWT of SprayAndWait are less relative to other protocols.

2) EXPERIMENT 10

As mentioned already in this article that malicious nodes waste energy resources which cause low PDR and high PLR. In experiment 10 this article give initial energy 500 and various SE, SI, TrE (mentioned in the top of every graph) to test how much energy resources are consumed. In experiment 10 this article calculated PDR, TWT, TE, and the number-of-attack packets with various tests. In test1, test2, test3, test4 this article calculated previously mentioned parameters with SE, SI, TrE and various nodes deployment scenarios respectively. Fig. 7(h) shows simulation results of PDR, TWT, TE and number-of-attack packets with SE. Simulation

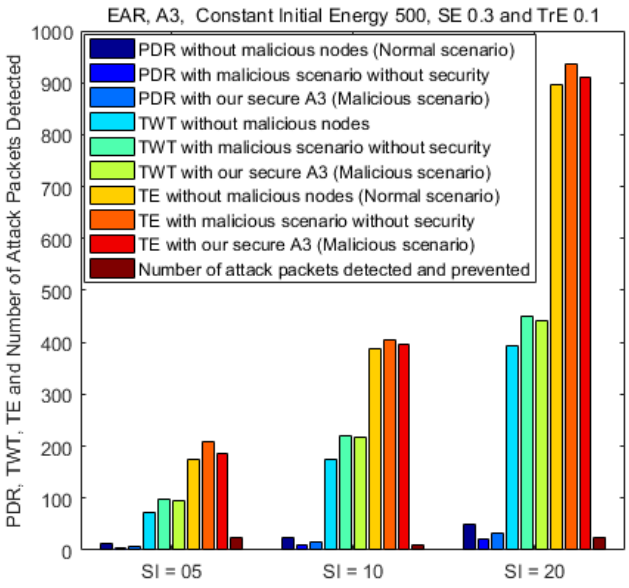


FIGURE 8. PDR, TWT, TE, attacks-packets with SI (test2).

results show that all mentioned parameters are improved in our A3, because A3 prevent malicious nodes which enhanced PDR, TWT (A3 consumed fewer energy that is why PDR and TWT are improved). It is also clear from simulation results that TE with A3 is less relative to malicious scenario (a scenario in which malicious nodes launch attacks), which proves A3 stops some certain malicious nodes and its malicious packets. Fig. 8 shows simulation results with SI. Simulation results show that all parameters are improved with our A3 like test1. Fig. 9 and Fig. 10 shows simulation results of previously mentioned parameters with TrE and various nodes deployment scenarios respectively. Simulation results show PDR, TWT, and TE are improved with our proposed A3 like test1 and test2 (reasons are already mentioned that our A3 consumed less energy, which improved nodes lifetime). Simulation results of test3 imply that PDR is decreased with TrE, However after some time, it increased (when TrE increased from 0.1 to 0.2 it decreased PDR, but when TrE increased from 0.2 to 0.3 PDR increased). This is because of the facts when nodes consumed more TrE (especially malicious nodes) so malicious nodes become down, that is why after some time PDR is increased (maintain stable graph). It is also clear from a simulation of test4 when malicious nodes are static and normal is dynamic so TWT is high. Because when normal is dynamic and malicious are static, so malicious nodes affect less number of legitimate nodes, legitimate nodes forwards packets, that is why TWT are high. When malicious nodes are dynamic and normal nodes are static, so TWT are low. Because malicious nodes consumed buffer of every node, so innocent nodes quickly become down. That is why benign nodes forward less number of packets, so TWT are less in this case. When both malicious and benign nodes are static so it consumed more bandwidth because nodes forward large number of packets (Nodes lifetime are improved, the probability of nodes, lifetime improved due to less probability of

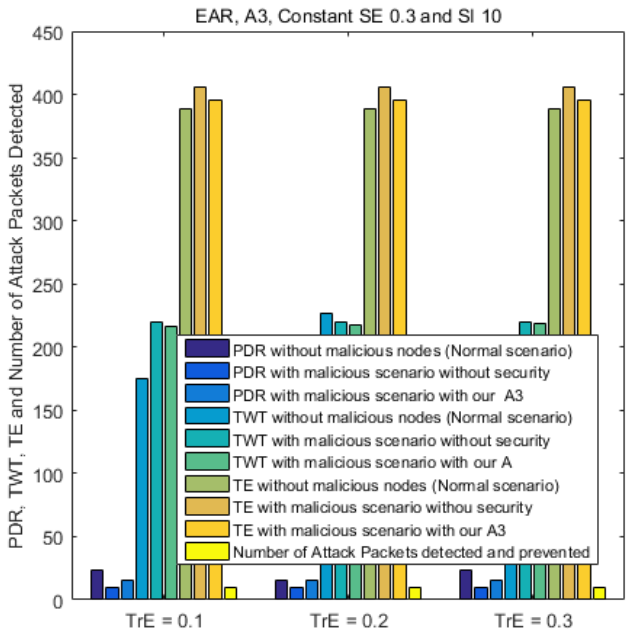


FIGURE 9. PDR, TWT, TE, attack-packets with TrE (test3).

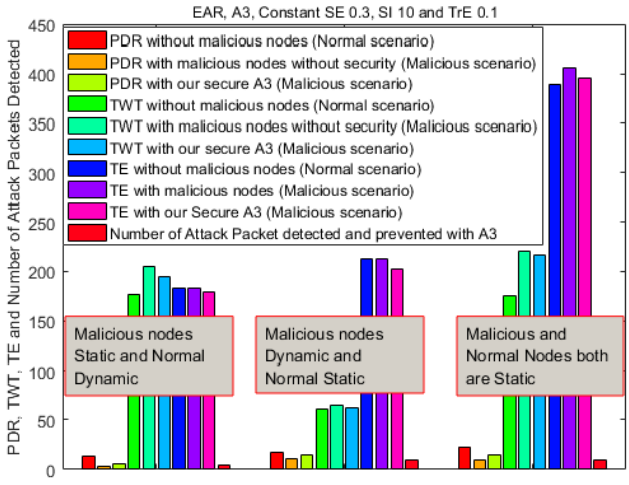


FIGURE 10. PDR, TWT, TE, attack-packets with nodes deployment (test4).

attacks on every benign node (attacks are successful in few numbers of nodes)).

Corollary From Experiment 10: This article concluded from experiment 10 that SE is inversely related to PDR, TWT and TE. When nodes consumed more energy so nodes quickly become dead which decreased PDR, TWT, and TE (nodes died due to EC so the number of transmitted packets becomes less which decreased TWT and TE). It is also cleared from simulation results that SI is directly related to PDR, TWT, and TE (nodes scan after long time so energy is less consumed). When SI is high so it consumed less energy, which implies that nodes forward more packets which improved PDR. Also when nodes forward more packets due to less EC (long lifetime) so TWT and TE will be increased.

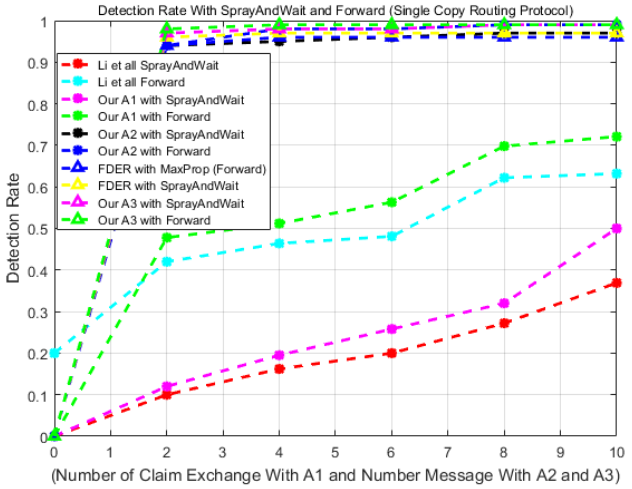


FIGURE 11. Flood attack in two sites/city scenario.

VI. COMPARISON

A. DETECTION RATE/DETECTION ACCURACY

This article compared the simulation results (Detection Rate) of RTOC, IFAM, and HFAM with article [36] (Li article) and article [48] (FDER). Fig. 11 shows simulation results of Detection Rate. Simulation results show that Detection Rate is linearly increased when the number of claims (In case of RTOC) and the number of messages (In case of IFAM and HFAM) are increased. Simulation results of Detection Rate show that Detection Rate is high with Forward routing protocol as compare to SprayAndWait. This is because SprayAndWait take some time after spray phase (due to disconnection probability of detection are decreased) and forward algorithm forwards packets to those nodes which have high probability with destination, so obviously, forward routing protocol increased Detection Rate.

Simulation results shows that the Detection Rate of our proposed RTOC is a little bit enhanced as compared to Li algorithms. This is just because of the facts that RTOC compress packets, which take more time in buffer (ABT are high already proved in the simulation section, because BC is less, drops probability becomes less). Detection Rate of Li [36] is low because it waste buffer actually drops probability are high, so most of the time claims packets are drops (due to buffer overloading) without malicious nodes detection. Simulation results shows that our proposed A2 and A3 enhanced Detection Rate (IDS directly blacklist those malicious nodes which violate Rate limit) as compared to Li algorithm and FDER. This is because our proposed algorithms do not send extra information (Claims in Li algorithm and Encounter history in FDER) along with packets and does not cross-check packets claims and encounter history. Obviously claims verification and encounter history sharing took a long time so Detection Rate is not high. Detection accuracy does not hundred percent in A2 this is just because of intermittent connectivity. Detection Rate of A3 is a little bit higher than A2, this is because, A2 some time forwards packets to ordinary nodes, in-contrast A3 only forwards to

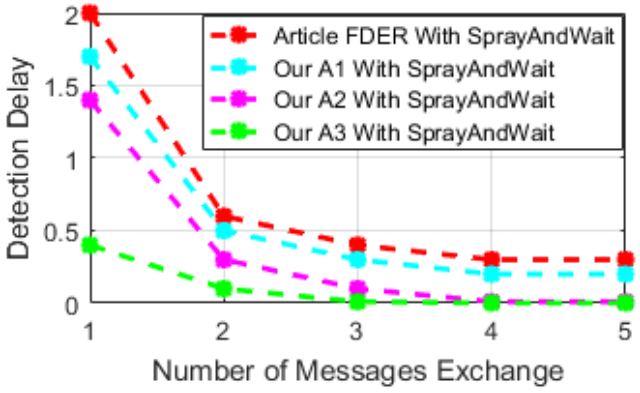


FIGURE 12. Flood attack in two sites/city scenario.

IDS based nodes, which directly blacklist malicious nodes. Nonetheless, A2 and A3 have the ability to detect colluding attacks (In which the malicious nodes collaborate to launch flood attacks) but it took some time.

B. DETECTION DELAY

This article compared the simulation results of RTOC, IFAM, and HFAM with FDER algorithm. Fig. 12 shows the results of Detection Delay. Simulation results show that RTOC, IFAM, and HFAM enhanced Detection Delay. Actually, FDER forwards encounters history to others nodes, then cross check encounter history. However, due to the disruption, it took a long time to verify encounter history and also encounter history waste buffer, so packet drops ratios are high (Most of the time encounter history packets are drops without attacks detection due to buffer overloading). In contrast, RTOC compress packets which consumed less buffer relative to FDER, so drops ratios are less in RTOC. That is why RTOC little bit improved Detection Delay.

A2 and A3 do not cross-check claims and share encounter history, However, when nodes violate rate limit, IDS directly black-list malicious nodes. So Detection Delay of A2 and A3 are improved relative to RTOC and FDER. Detection Delay of A3 is improved more relative to A2, because A2 forwards packets to both ordinary nodes and IDS based nodes, so detection takes some more time when nodes forward packets to ordinary nodes. In contrast A3 only forwards packets to IDS based nodes, which quickly detects malicious nodes.

C. MISCELLANEOUS PARAMETERS

This article simulates various parameters in the simulation section, which are already mentioned. Simulation results shows that our proposed RTOC, IFAM and HFAM enhanced resources consumption (BC, EC, and BWC this is because of Huff-man coding in RTOC, IFAM and HFAM do not send extra-information along with packets that are claims and encounter history) which ultimately improved PDR, PLR, ABT, TWT, BC and OH. Simulation results show that AL is dis-improved. PDR, PLR, ABT, TWS, BC, EC and OH etc are not shown in the article [48] (FDER) and [36] (Li) that is why this article does not compare the above mentioned parameters. However, this is already proved in analysis and simulation section that our proposed algorithms enhanced the above-mentioned parameters.

D. COST ANALYSIS

Cost is very important parameters for security. For every security attacks detection, cost is required, without cost, security is impossible. This section analytically analyzed that how much cost is required to detect malicious nodes which launches flood attacks. Consider a rate limit based algorithms [36], encounter-based [48] and our proposed RTOC, IFAM and HFAM. All algorithms detect malicious nodes with some cost. Generically there are three types of cost which are followed as, Communication Cost (CC), Computational Cost (CMC) and Storage Cost (SC)

$$\text{Cost} = \text{CC} + \text{CMC} + \text{SC} \tag{27}$$

1) COMMUNICATION COST

Some of the proposed algorithms forwards some extra information (mentioned already in this article) along with packets to detect malicious nodes. Which consumed some extra communication resources (Communication Cost). The amount of extra communication cost required for detection of malicious nodes is called communication cost. In sender side, rate limit based and RTOC forwards P-Claim with new packets and T-Claim with every packet. In receiver side, receiver nodes cross check packets claims. So in rate limit based and RTOC, CC is equal to the sum of the communication of packets claims and claims verification. If the number of new packets is (NNP), the number of intermediate relayed packets is (NRP) and Claim Verification cost is (CVC), then CS of rate limit based and RTOC will be calculated with the following formula.

$$\text{CC} = \text{NNP} * \text{P-Claim} + \text{NRP} * \text{T-Claim} + \text{RLC} + \text{CVC} \tag{28}$$

Encounter-based algorithm (FDER) share sender encounter history and receiver nodes verify encounter history. If number of encounter-history cost is (NEHC) and verification of encounter-history is (VEHC) Therefore CS of the encounter-based algorithm (FDER) will be calculated with the following formula.

$$\text{CC} = (\text{NEHC}) + \text{RLC} + (\text{VEHC}) \tag{29}$$

A2 only send rate limit certificate along with packets. So CC of A2 will be calculated with the following formula.

$$\text{CC} = (\text{NNP})* \text{RLC} + (\text{NRP})* \text{RLC} \tag{30}$$

A3 forwards rate limit certificate and MAC along with packets. However, the Mac is very small relative to packet claims and encounter history. According to the analytical analysis of this article, the CC of A3 will be calculated with a following formula.

$$\text{CC} = (\text{NNP}) * (\text{RLC} + \text{MAC}) + (\text{NRP}) * (\text{RLC} + \text{MAC}) \tag{31}$$

Above all equations clearly shows that CS of A2 is minimum because it only sends RLC with packets. CS of encounter based algorithms are maximum because it sends encounter history and verify encounter history, rate limit based and RTOC send P-Claim and T-Claim but claims packets are very small so the cost of that is lower than encounter history. Also, CS of RTOC is lower than original rate limit based (Li scheme) because RTOC forwards compress packets. CC of HFAM is a little bit high than RTOC because it forwards MAC along with packets, which consumed more communication resources than RTOC.

2) COMPUTATION COST

The amount of cost required for extra works before sending of packets is called CMC. CMC of all algorithms is different. Consider a rate-limit-based algorithm (Li scheme) which create P-Claim, T-Claim, create a signature and verify the signature. If Claims Creation Cost is (CLC), Claims Verification Cost is (CLV), Signature Creation Cost is (SCC) and Signature Verification Cost is (SVC) then cost will be calculated with a following formula.

$$\mathrm{CMC} = \mathrm{CLC} + \mathrm{SCC} + \mathrm{SVC} \tag{32}$$

If packet compression cost is (PCC) then CMC of RTOC will be calculated with the following formula.

$$\mathrm{CMC} = \mathrm{PCC} + \mathrm{CLC} + \mathrm{SCC} + \mathrm{SVC} \tag{33}$$

Encounter-based algorithm only create signature and verify signature so CMC will be calculated as follow as.

$$\mathrm{CMC} = \mathrm{SCC} + \mathrm{SVC} \tag{34}$$

If MAC creation cost is MCC and MAC verification Cost is MVC then CMC of A3 will be followed as.

$$\mathrm{CMC} = \mathrm{MCC} + \mathrm{SCC} + \mathrm{SVC} + \mathrm{MVC} \tag{35}$$

A2 only sign packets so CMC of A2 is almost negligible, CMC of RTOC is maximum due to compression, claims, and signature creation/verification. CMC of A3 will be a little bit high than IFAM (RTOC need PCC and HFAM need MCC and MVC).

3) STORAGE COST

The time average extra information store along with packets are called storage Cost. Rate limit based (Li scheme) only stores packets claims along with packets. RTOC stores packets claims along with packets, but its storage cost is less than Li because it consumed minimum buffer due to compression. Encounter-based algorithm (FDER) stores encounter history information, which consumed a slightly greater amount of buffer than rate limit and RTOC. HFAM forwards MAC along with packets which consumed some buffer (BC are very less relative to others schemes). The SC of IFAM is minimum relative to all because it does not store any other information that is why it improved PDR and PLR (already proved in analysis and simulation section).

VII. CONCLUSION AND RECOMMENDATIONS

Flood attack is serious and very challenging threat in DTNs security. Being a serious threat, flood mitigation is very important to tackle limited resources of DTNs. This article analyse flood attacks with various parameters rigorously, which enable us to modify one existing rate-limit-based algorithm which slightly improved PDR, detection rate and detection time. This article also proposed two distributed resources efficient algorithms, which are suitable for DTNs to mitigate misbehaving nodes. Simulation results shows that proposed algorithms mitigates misbehaving nodes, save scarce resources which improved PDR and PLR, detection time and detection rate. Simulation results clearly shows that our A1 improved PDR almost 18, 2 and 3-11 percent with Epidemic, DirectlyDelivery and DD1 respectively with test 1. Simulation results shows 14-25, 2-5 and 6-13 percent improvement with Epidemic, DirectDelivery and DD1 respectively with test 2. Simulation results also clearly shows that our A2 and A3 improved PDR 30, 22, 25, and 20 percent with SprayAndWait, FirstContact, Epidemic and DirectDelivery respectively.

From simulation results, this article concluded that PDR is directly related to SI and inversely related to SE. This is because when SI is high so nodes consume less energy which increase PDR. Also if SE is high so PDR is decreased because nodes waste maximum energy. This decreased nodes lifetime consequently, which ultimately causes low PDR. It is clear from simulation results that encounter is inversely proportional to SE when we increase SE so TE is decreased, which decrease PDR. From simulation results, this article conclude that PDR is inversely related to BC. It is very clear from simulation results that detection probability is high when malicious nodes are randomly deployed. It is also clear from simulation results that PDR of the CMM model are high and RWM is low that is why number of encounters are high in CMM due to less transmission area. Simulation results also show that epidemic consume more resources (bandwidth, buffer, and energy) relative to other protocols. Resources consumption of direct delivery protocol is minimum as compared to other protocols.

This article analyse that researcher's proposed some traditional methods (Not suitable in DTNs) to detect malicious nodes which launch flood attacks. This article recommends IDS based detection algorithms because IDS based methods are cheapest, suitable to DTNs. According to analysis, flood mitigation is a very tough task, so this article proposes, why the researchers do not use preventive-based-algorithms. According to the analysis of this article, why the researchers do not detect malicious packets rather than malicious nodes. This article recommends detection of malicious packets rather than malicious nodes. According to the analysis of this article machine-learning-based algorithms are very powerful to detect malicious packets. This article recommended, if researchers propose machine-learning-based algorithms, it will be a cheapest and suitable solution (which will enhance detection time and detection accuracy) in DTNs.

This article proposed RTOC which enhance resources consumption, PDR and detection time. However, RTOC detects malicious nodes with cross-checking strategies (traditional approach), which obviously takes time. DTNs require algorithms which quickly detect malicious nodes and save scarce resources. This article proposed IFAM which improved detection time, detection accuracy, resources consumption, and PDR. However, IFAM is applicable to a specific scenario. This article proposed HFAM for a generic scenario which according to analysis and simulation results, is not a bad solution. However, it verify packets with same key. If researchers propose algorithms which can verify packets with a different key, or propose some other methods for packets verification, so it will be the better solution.

Hopefully, this article will further motivate researchers interest in this particular security research area and accordingly highlight the following directions for investigation.

1) Algorithms which verify packets in the destination without the same key used in HFAM.
2) Relationship of parameters and constants used in the analysis.
3) Distributed algorithms to mitigate flood attacks, enhance resources consumption, detection accuracy, detection time and PDR.
4) Preventive based algorithms to thwart flood causing malicious nodes.
5) Machine learning based algorithms which detect malicious packets rather than malicious nodes, which enhance detection accuracy and overcomes false positive and false negative ratios.

REFERENCES

[1] K. Fall, K. L. Scott, S. C. Burleigh, L. Torgerson, A. J. Hooke, H. S. Weiss, R. C. Durst, and V. Cerf, *Delay-Tolerant Networking Architecture*, document 4338, 2007.

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

[3] 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.

[4] 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.

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

[6] 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, 2007.

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

[8] K. L. Scott and S. Burleigh, *Bundle Protocol Specification*, document 5050, 2007.

[9] W. Narongkhachavana, T. Choksatid, and S. Prabhavat, "An efficient message flooding scheme in delay-tolerant networks," in *Proc. IEEE 7th Int. Conf. Inf. Technol. Electr. Eng. (ICITEE)*, Oct. 2015, pp. 295–299.

[10] L. Wood, W. M. Eddy, and P. Holliday, "A bundle of problems," in *Proc. IEEE Aerosp. Conf.*, Mar. 2009, pp. 1–17.

[11] K. Fall and S. Farrell, "DTN: An architectural retrospective," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 5, pp. 828–836, Jun. 2008.

[12] S. Raut, "A survey based on secure data retrieval in disruption tolerant network," *Int. J. Res. Comput. Eng. Electron.*, vol. 4, no. 6, pp. 32–45, 2016.

[13] D. Tang and J. Ren, "A novel delay-aware and privacy-preserving data-forwarding scheme for urban sensing network," *IEEE Trans. Veh. Technol.*, vol. 65, no. 4, pp. 2578–2588, Apr. 2016.

[14] G. Rajan and G. Cho, "Applying a security architecture with key management framework to the delay/disruption tolerant networks," *Int. J. Secur. Appl.*, vol. 9, no. 4, pp. 327–336, 2015.

[15] 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, 2015.

[16] 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.

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

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

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

[20] 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.*, May 2017, pp. 1–6.

[21] 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.

[22] M. Alajeely, R. Doss, and V. Mak-Hau, "Catabolism attack and anabolism defense: A novel attack and traceback mechanism in opportunistic networks," *Comput. Commun.*, vol. 71, pp. 111–118, Nov. 2015.

[23] M. 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.

[24] M. Arshad, Z. Ullah, M. Khalid, N. Ahmad, M. 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, 2018.

[25] M. Aloqaily, S. Otoum, I. Al Ridhawi, and Y. Jararweh, "An intrusion detection system for connected vehicles in smart cities," *Ad Hoc Netw.*, vol. 90, Jul. 2019, Art. no. 101842.

[26] S. Khan, D. Paul, P. Momtahan, and M. Aloqaily, "Artificial intelligence framework for smart city microgrids: State of the art, challenges, and opportunities," in *Proc. IEEE 3rd Int. Conf. Fog Mobile Edge Comput. (FMEC)*, Apr. 2018, pp. 283–288.

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

[28] M. Khalid, Y. Cao, N. Ahmad, M. 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, 2018.

[29] M. Khalid, Y. Cao, M. Arshad, M. 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.

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

[31] D. Turgut and L. Boloni, "Value of information and cost of privacy in the Internet of Things," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 62–66, Sep. 2017.

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

[33] M. Khalid, Z. Ullah, N. Ahmad, A. Adnan, W. Khalid, and A. Ashfaq, "Comparison of localization free routing protocols in underwater wireless sensor networks," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 3, pp. 408–414, 2017.

[34] S. Otoum, B. Kantarci, and H. T. Mouftah, "On the feasibility of deep learning in sensor network intrusion detection," *IEEE Netw. Lett.*, vol. 1, no. 2, pp. 68–71, Jun. 2019.

[35] S. Otoum, B. Kantarci, and H. T. Mouftah, "Detection of known and unknown intrusive sensor behavior in critical applications," *IEEE Sensors Lett.*, vol. 1, no. 5, Oct. 2017, Art. no. 7500804.
[36] Q. Li, W. Gao, S. Zhu, and G. Cao, "To lie or to comply: Defending against flood attacks in disruption tolerant networks," *IEEE Trans. Dependable Secure Comput.*, vol. 10, no. 3, pp. 168–182, May/Jun. 2013.
[37] F. C. Lee, W. Goh, and C. K. Yeo, "A queuing mechanism to alleviate flooding attacks in probabilistic delay tolerant networks," in *Proc. IEEE 6th Adv. Int. Conf. Telecommun. (AICT)*, May 2010, pp. 329–334.
[38] P. T. N. Diep and C. K. Yeo, "Detecting flooding attack in delay tolerant networks by piggybacking encounter records," in *Proc. IEEE 2nd Int. Conf. Inf. Sci. Secur. (ICISS)*, Dec. 2015, pp. 1–4.
[39] D. Kuriakose and D. Daniel, "Effective defending against flood attack using stream-check method in tolerant network," in *Proc. IEEE Int. Conf. Green Comput. Commun. Elect. Eng. (ICGCCEE)*, Mar. 2014, pp. 1–4.
[40] 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, 2003.
[41] V. Natarajan, Y. Yang, and S. Zhu, "Resource-misuse attack detection in delay-tolerant networks," in *Proc. IEEE 30th Int. Perform. Comput. Commun. Conf. (IPCCC)*, Nov. 2011, pp. 1–8.
[42] D. S. D. Hepsiba and S. Prabhu, "Enhanced techniques to strengthening DTN against flood attacks," in *Proc. IEEE Int. Conf. Inf. Commun. Embedded Syst. (ICICES)*, Feb. 2014, pp. 1–4.
[43] P. Nagrath, S. Aneja, and G. N. Purohit, "Defending flooding attack in delay tolerant networks," in *Proc. IEEE Int. Conf. Inf. Netw. (ICOIN)*, Jan. 2015, pp. 40–45.
[44] 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. 2017.
[45] S. Rashid and Q. Ayub, "Integrated sized-based buffer management policy for resource-constrained delay tolerant network," *Wireless Pers. Commun.*, vol. 103, no. 2, pp. 1421–1441, 2018.
[46] Q. Ayub and S. Rashid, "Resource refrain quota based routing protocol for delay tolerant network," *Wireless Netw.*, vol. 12, pp. 1–10, May 2018.
[47] A. Keränen, J. Ott, and T. Kärkkäinen, "The ONE simulator for DTN protocol evaluation," in *Proc. 2nd Int. Conf. Simul. Tools Techn.*, 2009, p. 55.
[48] 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.