INTEREST FLOODING ATTACK MITIGATION IN A VEHICULAR NAMED DATA NETWORK

MUHAMMAD ABDULLAH | IMRAN RAZA | TANVEER ZIA | SYED ASAD HUSSAIN

1 Communication Networks Research Group, Department of Computer Science, COMSATS University, Lahore Campus, Islamabad, Pakistan
2 School of Computing and Mathematics, Charles Sturt University, Australia

Correspondence
Syed Asad Hussain, Communication Networks Research Group, Department of Computer Science, COMSATS University Islamabad, Lahore Campus, Pakistan.
Email: asadhussain@cuilahore.edu.pk

Abstract
Vehicular named data network (VNDN) is the next-generation network architecture for intelligent transportation system. Contrary to the conventional transmission control protocol/internet protocol (TCP/IP) communication model, VNDN follows a data-centric approach where the user is interested in ‘WHAT’ instead of ‘WHERE’. Interest flooding attack (IFA) is one of the prominent security concerns in VNDNs. In IFA, attackers request for non-existent content to exhaust network resources and cause Interest packet flooding across the network. A novel attack mitigation scheme to counter IFA in VNDN has been proposed in this study. The proposed priority-based per-flow Interest rate monitoring (PP-FIRM) scheme determines the suspicious flow of malicious incoming Interest packets in attacked vehicles. A priority flag is assigned to the incoming flow of Interest packets that detects the occurrence of an attack. The priority of incoming Interest packet flow is calculated using a collaborative or neighbour-assisted approach. A comparison with another attack mitigation scheme validates that the proposed scheme performs better in terms of an improved cache hit ratio and Interest satisfaction ratio during the attack window. Besides this, pending Interest table utilisation, packet collisions rate, Interest packets retransmission count, end-to-end delay, and the ratio of timed out Interest packets have also been reduced. Furthermore, the scalability of the proposed research strategy is also evaluated by changing the density of attackers in real time. Moreover, in the proposed attack mitigation model, the rate of incoming legitimate Interest packets increases by reducing the drop rate of valid Interest packets.

INTRODUCTION

Intelligent transportation system (ITS) [1] has proposed to cater to the need for traffic security and management in autonomous driving system [2]. Vehicular ad hoc network (VANET) [3, 4] is considered a part of ITS as it delivers valuable services. In VANET, vehicles are responsible to send, receive and relay information. Vehicles are equipped with on-board unit, radio transmitter, collision avoidance sensors, and wireless transmitters for sending and receiving data [5]. A VANET provides information services including multimedia data, which cannot tolerate massive delays. It is reported in the Cisco Visual Networking Index that Internet traffic will reach up to 396 exabytes per month by 2022 [6]. The use of a conventional TCP/IP model in VANET for the dissemination of bulky data is not feasible in such situations. Moreover, security alarms and beacon messages that need to be communicated timely require latency-free mechanism, and TCP/IP paradigm does not provide the appropriate solution for message dissemination in autonomous vehicles [7]. Furthermore, rapid content delivery, vehicular mobility management, robust traffic management system, and adaptive routing makes TCP/IP framework infeasible and complex to deal with the quality of service requirements of different applications [8]. Other challenges include intermittent connectivity between nodes due to dynamically changing network topology and network instability. Due to the high mobility of vehicles in a TCP/IP-based VANET, it is hard to sustain dedicated paths between source and destination nodes. Named Data Network (NDN) [9] enabled VANET is known as Vehicular NDN (VNDN), Which comes out as a promising solution for
Interest flooding attack (IFA) is one of the DDoS attacks in VNDN where the attacker sends numerous fake requests and blocks the valid requests from legitimate vehicles. The motivation behind this research work is to mitigate the IFA that leads packet broadcast storm of uncontrolled and unsolicited traffic across VNDN.

Various IFA mitigation schemes have been proposed for NDN scenario, that is, per-face Interest rate monitoring techniques [13–16], statistical modelling-based approaches [17–19], adaptive in-network caching [20–25] and packet routing algorithms [26–32]. However, the drawback of these schemes is that along with malicious Interest packets, a high volume of legitimate Interest packets is dropped as well. Low Interest satisfaction ratio (ISR) results in flooding of the unsolicited flow of malicious Interest packets that leads to packet broadcast storm.

Moreover, existing IFA mitigation schemes are resource extensive, which is not a feasible option for the VNDN environment. Furthermore, in previous IFA mitigation schemes, multipath routing has been merely highlighted. Therefore, in this research work, we have proposed a novel priority-based per-flow Interest rate monitoring (PP-FIRM) strategy that efficiently detects the suspicious flow of Interest packets and triggers attack recovery mechanism to reduce the effect of IFA. Furthermore, attack prevention at intermediate nodes has also been considered in the proposed attack mitigation model. The attack prevention phase is viable in reducing the scale of IFA in a VNDN scenario. The main contributions of this research work are as follows:

1. A novel PP-FIRM is proposed to effectively mitigate IFA in a VNDN environment implementing priority-based attack detection and a collaborative approach to avoid overreaction.
2. The proposed scheme calculates the priority of incoming Interests and only forwards Interests with high priority as opposed to the per-face Interests rate monitoring schemes [13–16], which only reduce the rate of incoming Interests. As a result, the proposed scheme prevents a large number of legitimate Interests with unbound delays, and the Interests drop rate is reduced as well.
3. Unlike other existing Interest rate monitoring scheme [16], the proposed scheme is resilient to flooding of unsolicited Interests.
4. Several simulations have been performed to evaluate the efficiency of PP-FIRM and congestion-based IFA mitigation [16]. The simulation results show that the proposed scheme can effectively mitigate IFA and reduce unnecessary broadcast of malicious Interest packets.

The rest of this study is organised as follows. Section 2 presents the VNDN overview and its packet forwarding daemon. Section 3 exhibits related work. The proposed PP-FIRM is described in Section 4. Experimentation and results are elaborated in Section 5. Section 6 concludes the study.

2. **VEHICULAR NAMED DATA NETWORK: AN OVERVIEW**

NDN-enabled VANET is known as Vehicular Named Data Network (VNDN). VNDN is an extension of wired NDN architecture with certain modifications due to vehicle mobility and network scalability. Another similar architecture named data vehicular network [33] has been proposed as a conceptual model that claims to support the multicast Interest forwarding model. VNDN provides better support for vehicular environments in terms of reliable and quick message propagation. Also, VNDN decouples the underlying communication plane from location and content distribution services. Moreover, support for data dissemination through multiple radio interfaces increases reliability and data acquisition.

2.1 **VNDN architecture and forwarding daemon**

Data in VNDN is delivered in a pull-based fashion; hence, this scheme is also known as a data-driven approach. The data requesting node is called consumer or subscriber, and the destination node is called publisher or data/content producer. Intermediate nodes support the rapid content delivery process and perform the job of relaying vehicle and content producer. In VNDN, a vehicular node has to maintain three data structures of pending Interest table (PIT), content store (CS), and forwarding information base (FIB). PIT is a table containing a list of unsatisfied pending Interest packets followed by the incoming interface(s) [33]. CS performs the task of in-network caching and contains a chunk of the most frequently used data. FIB maintains name prefixes followed by outgoing faces and performs packet routing and forwarding operations as in the TCP/IP model [34, 35]. Figure 1 depicts all three data structures being maintained in intermediate nodes.

2.2 **Interest flooding attack**

IFA is a type of DoS attack, where the attacker(s) send malicious requests to all neighbouring nodes [36]. These malicious
requests fill up buffer space of vehicular node(s), and as a result, valid requests are discarded. Sometimes these malicious Interest packets collude with the server to attack any victim router (i.e. collusive-IFA) [37]. DoS attack in VNDN is quite different as compared to native TCP/IP architecture. Usually, in a host-centric approach, a DoS attack is generated to target a specific server or network device. The consequences of a DoS attack in VNDN are more severe since the attack not only compromises a specific content source but all the intermediate nodes along its path as shown in Figure 2. The goal of the malicious node is to flood a large number of Interest packets with valid prefix but invalid suffix. These malicious Interest packets are created in the PIT of every intermediate node [38]. Eventually, the PIT of compromised intermediate nodes reaches its capacity and ultimately drop packets.

3 | Related Work

This section reviews some existing attack mitigation solutions designed for named-centric networks. Countermeasures of IFA in named-centric networks comprise two phases, namely, detection and recovery. The detection phase identifies the malicious face or targeted prefix, whereas the recovery phase either limits the ratio of incoming Interest packets at a suspicious face or blocks entire traffic arriving on that suspicious face(s). Initially, per-face rate monitoring, statistical and hypothetical testing-based approaches have been adapted to limit the rate of malicious Interest packets.

ISR is one of the detection mechanisms used to cope with IFA. ISR is the ratio of data packets sent and the number of incoming Interest packets received. Upon detection of an attack, the routing node limits Interest arrival rate on the suspicious interface. Authors in [13] have developed an IFA mitigation scheme based upon the PIT utilisation rate. However, there is no standard to set the threshold value for ISR. PIT size monitoring needs distributed content nodes for computation. This causes dependency and if any of the content router malfunctions, the technique under execution cannot produce any fruitful results. Authors in [14] have used Theil-based countermeasure to mitigate IFA. Theil index is calculated based upon the uneven distribution of incoming Interest packets through the interface(s). Intra- and inter-group are formed for incoming Interest packets. When an attacker generates IFA, the frequency of forged names increases immensely. The purpose behind grouping is to evaluate the distribution of incoming Interest packets and the contribution of group differences. When an attacker launches an attack, it sends a large number of malicious Interest packets that ultimately disturbs the distribution of Interest packets. As a result, Thiel’s entropy value will go beyond the pre-determined normal range, which signifies that the system is under attack. Similarly, in [15], authors have used entropy value along with ISR and PIT utilisation ratio that reflects variation caused by an attack. An attack detector is deployed as a classifier to predict suspicious behaviour of the network using collected parameters. Additionally, support vector machine (SVM) has been used to learn network anomalies. SVM is a supervised learning model used to train systems for classification and regression analysis. Another IFA mitigation method based on incoming Interest packet flow and PIT consumption rate has been proposed in [16]. The authors have introduced the congestion parameter to ensure the valid detection of the attack. ISR and the congestion value of each interface are considered to detect IFA. Whenever specified values of the node’s incoming face exceed a threshold value, intermediate nodes consider that flow as suspicious and eventually limit the rate of incoming traffic.

The statistical approach is reactive and relies on network values based upon PIT expiration rate and PIT occupancy rate to identify any abnormal traffic pattern. In [17], the authors used node’s reputation value (RV) as a metric that is calculated by each intermediate node to either accept or reject the incoming Interest packet. RV calculated using a collaborative approach is shared between neighbours. The authors have used a statistical-based hypothetical testing theory with Neyman–Pearson dual-criteria methodology. This approach does not depend on the router’s calculated statistical values and provides a consistent solution for IFA mitigation, though in the composite hypothesis approach, scalability issues are present. In [18], the authors proposed the IFA detection and prevention mechanism based upon a centralised controller. In this network topology, nodes are directly connected with access routers, which detect the abnormal behaviour of incoming packets passing through radio interfaces of the node(s). The authors have classified their attack mitigation scheme as local and global IFA detection. Whenever an access router finds any unusual traffic flow at a certain face(s) of a node, it immediately notifies the central controller about any possible attack. Finally, access routers block the malicious traffic as directed by the access router. This mechanism does not guarantee that legitimate Interest packets will never be discarded. Likewise, in [19], a threshold value is set for many suspicious \( Y' \) and timed out Interests \( Y_0 \). Access routers intimate the central controller as \( Y' \) exceeds \( Y_0 \). Statistical-based solutions are effective; however, they require high computational resources that are scarce in a VNDN scenario. Table 1 depicts various statistical and per-face Interest rate monitoring schemes for IFA mitigation in NDN.
In-network caching is supported in NDN to enable instant content delivery and to avoid packet redundancy. Primarily, the Interest packet is only flooded when the requested content is unavailable in the CS, so there is a requirement to deploy an effective and adaptive caching policy in mobile nodes. In a VNDN, the mobility of vehicles reduces the efficiency of the caching mechanism. In [20], the authors proposed cooperative caching with mobility prediction, which undergoes the clustering of vehicles having similar mobility patterns. In [21], the authors proposed neighbourhood selective caching (NSC) based on distributed proactive caching. The idea behind NSC is to cache content one hop away from the content source. In [22], opportunistic caching has been adopted for caching popular data at intermediate nodes. Each intermediate node maintains its content popularity statistics that help to increase the cache hit ratio (CHR). The aim is to enhance content delivery services. In [23], authors have proposed a machine learning-based solution called deep-cache framework. In this method, long-term memory encoder-decoder is implemented to determine the rate of the requested content. The authors in [24] have proposed ‘mobility aware edge caching’ by incorporating an age threshold scheme to cache the right content at the right time, otherwise the essence of in-network caching becomes useless. In [25], the authors introduced a probabilistic caching approach based upon cache occupancy and link stability between the sender and receiver. Cache occupancy defines the probability of requested content, whereas relative movements decide link stability between communicating vehicles. Moreover, cached content is distributed relative to the application type of requested data. Caching schemes are essential to limit the flooding of malicious Interest packets. A comparison of various in-network caching approaches is presented in Table 2.

To reduce the scale of IFA and packet broadcast storming, efficient packet forwarding is required. NDN deploys separate routing and forwarding plane for efficient dissemination of Interest and data packets. Ad hoc networks can encounter various packet relaying challenges that invoke IFA and ultimately affect the propagation of packets [26]. Several packet forwarding techniques have been proposed to handle the flooding of unsolicited packets. In [27], the authors have optimised multi-path packet forwarding to support seamless packet transmission. The proposed scheme consumes low bandwidth using a global optimisation problem. In [28], the authors proposed a distance-based IFA mitigation scheme known as intersection-based forward selection (IBFS) that is more effective than an individual level mitigation strategy. In IBFS, trajectory information of each vehicle is shared with its neighbours across the radio range. By doing this, the location of the potential data producer or consumer is determined. A relay or forwarding node is selected to avoid flooding of Interest and data packets. Distributed interest forwarder selection [29], is one of the packet forwarder selection mechanisms where two forwarding nodes are selected. This is done to cover a large transmission area and less propagation delay. The selection of two forwarders also alleviates hop-by-hop transmission. In [30], the authors proposed a novel statistical approach based on collaborative mitigation algorithms for the detection of IFA. The proposed mechanism relies on a charging and rewarding mechanism. Virtual money has been assigned to every intermediate or forwarding node. The charging mechanism deals with charging users

### Table 1: Comparison of various per-face and statistical-based Interest flooding attack (IFA) mitigation schemes

| Classification | Literature | IFA mitigation model | Collaboration scope |
|---------------|------------|----------------------|---------------------|
|               |            | Prevention | Detection | Recovery | Individual | Collaborative |
| Per-Face Interest packet rate monitoring | [13] | ✓✓✓ | ✓ | ✓ | ✓ | ✓ |
| | [14] | ✓✓ | ✓ | ✓ | ✓ | ✓ |
| | [15] | ✓✓ | ✓ | ✓ | ✓ | ✓ |
| | [16] | ✓✓ | ✓ | ✓ | ✓ | ✓ |
| Statistical and hypothetical testing based approaches | [17] | ✓✓ | ✓ | ✓ | ✓ | ✓ |
| | [18, 19] | ✓✓ | ✓ | ✓ | ✓ | ✓ |

### Table 2: Comparison of in-network caching approaches

| Architecture | Literature | Caching policy | Proactive | AI-based | Collaborative | Infrastructure-assisted |
|--------------|------------|----------------|-----------|----------|---------------|------------------------|
| COMP         | [20]       |                | ✓         | ✓        |               |                        |
| Neighbourhood selective caching | [21] | ✓ | ✓ | ✓ | ✓ | ✓ |
| Opportunistic caching | [22] | ✓ | ✓ | ✓ | ✓ | ✓ |
| Deep caching framework | [23] | ✓ | ✓ | ✓ | ✓ | ✓ |
| Probabilistic caching | [24] | ✓ | ✓ | ✓ | ✓ | ✓ |
TABLE 3  Comparison of various packet forwarding schemes in named data network (NDN)

| Classification                      | Literature | Packet type | Communication type | Mobility area |
|--------------------------------------|------------|-------------|--------------------|---------------|
|                                      |            | Interest    | data               | Urban         | Rural         |
| Distance based forwarding            | [27]       | ✓           | Multicast          |               | ✓            |
|                                      | [28]       | ✓           | Multi-hop          |               | ✓            |
| Collaborative and relay node selection | [29]     | ✓           | Unicast            |               | ✓            |
|                                      | [30]       | ✓           | Multi-hop          |               | ✓            |
| Geographical-based                   | [31]       | ✓           | Multi-hop          |               | ✓            |
|                                      | [32]       | ✓           | Unicast            |               | ✓            |

upon packet forwarding service. A node gets a reward if it is legal. Hidden Markov model [31] is applied to observe the behaviour of the node. This model helps in the identification of attacks by observing the hidden behaviour of the suspicious node. To control flooding of unsolicited packets, control of useless Interest flooding (CUIF) [32] restricts useless propagation of Interest and data packets. In CUIF, retransmission of Interest packets entirely depends on the location of consumer vehicles. When the Interest packet arrives at an intermediate node, it matches its location with the sender’s location. If there is a difference between a location, the Interest packet is not retransmitted and eventually discarded.

Distinct from the aforementioned countermeasures, the proposed IFA mitigation method known as a PP-FIRM efficiently identifies suspicious flow of Interest packets and triggers attack recovery mechanism to reduce the effect of IFA. Each flow of incoming Interest packets has been assigned priority according to the cumulative network statistics. The interface(s) with low priority has been declared as suspicious. Furthermore, attack prevention at intermediate nodes has also been considered in the proposed attack mitigation model. Table 3 shows various packet forwarding schemes in NDN for IFA prevention.

4   PP-FIRM SCHEME

The drawback of per-face limiting schemes is that along with malicious Interest packets, legitimate Interest packets are also dropped, which compromises the ISR of the network. We have implemented a novel (PP-FIRM strategy that efficiently identifies the suspicious flow of Interest packets in multipath routing scenarios. It then triggers the attack recovery mechanism to reduce the effect of IFA. Each flow of incoming Interest packets has been assigned priority according to the cumulative network statistics. The interface(s) with low priority has been declared as suspicious. Furthermore, attack prevention at intermediate nodes has also been considered in the proposed attack mitigation model. Table 3 shows various packet forwarding schemes in NDN for IFA prevention.

This section presents the proposed PP-FIRM scheme to mitigate IFA in NDN-enabled vehicular environment. The basic idea of the proposed strategy is to reduce the flow of malicious Interest packets. The priority of an incoming Interest packet proves to be an effective parameter and is considered to determine the correct detection of an attack.

4.1   Architecture of the proposed scheme

The primary module of the proposed scheme is an Interest packet flow monitor. This module considers the flow of Interest packets as a single object. Primarily, Interests flow is monitored via a radio interface to make sure to which flow it belongs. Two fields, that is, priority flag and hop count have been appended in the Interest packet. Priority flag is used to avoid transmission of malicious Interest packets, whereas hop count value is helpful to limit further dissemination across the network. A per-flow monitoring module is introduced that encapsulates the basic PIT structure as shown in Figure 3. As the normal flow of the Interest packet is determined, the packet flow is passed to this flow monitoring module, which is responsible for collecting the per-flow state of Interest packets. The flow monitoring module handles the transmission of incoming Interest packets from each face of the vehicular node. This flow of incoming Interest packets arriving from different faces is taken as a single flow object, to differentiate previously known and unknown flow.

Flow monitoring module keeps track of departures and drops of Interest packets, collected count of Interest packet and byte arrivals. The per-flow monitor has four components, that is,
prefix analyser, priority checker, suspicious list, and scheduler as shown in Figure 4.

### 4.1.1 Prefix analyser

IFA can be launched with an invalid name prefix that does not follow the standard NDN naming scheme. To alleviate the propagation of Interest packets with an invalid naming scheme, the prefix analyser is designed. The purpose is to add additional support to the NDN Interest forwarding daemon for the identification of spam incoming Interest packets. Moreover, invalid Interest packets are not picked up by the wired NDN framework. To avoid invalid Interest packets, there must be some mechanism to detect the flow of malicious Interest packets. Hence, this component is designed to validate the flow of incoming Interest packets. This is useful to protect the NONCE list from getting polluted.

### 4.1.2 Priority checker

The priority checker serves as an essential parameter to predict the system under attack. Whenever the unknown flow of Interest packets enters through the radio face, priority is assigned to each flow. After a few iterations, the Interest packet flow that has the lowest priority level is suspended and moved to a suspicious list. It is worth mentioning here that ISR, packet drop rate, cache hit/miss ratio, and hop count values are considered to avoid the probability of false alarms during the attack detection process. Values of ISR, CHR, the number of hops traversed, delay, and the number of legitimate Interest packets have been used for assigning priority to incoming Interest packet flow.

### 4.1.3 Suspicious list

This component has been introduced to discard the flow of incoming Interest packets before the PIT lockstep process. Suspicious prefixes list helps in the early detection of IFA, and thus reduces the PIT utilisation ratio. False detection of IFA and discarding of legitimate Interest packets alongside malicious ones results in low ISR value. A suspicious list contains a set of incoming Interest packets that are declared as suspicious during the IFA detection phase. The proposed system uses a collaborative approach to validate the suspicious flow of incoming Interest packets. For this reason, the proposed system undergoes multiple iterations to correctly determine the suspicious flow of incoming Interest packets. We have set the threshold value for Interest packet flow as 0.5 to determine suspicious transmission. After several simulations, it is found that a threshold value greater than 0.5 allows more malicious Interest packets to reside in PIT that ultimately reduces ISR.

### 4.1.4 Prefix scheduler

As the name suggests, this module is responsible to sort the flow of incoming Interest packet(s) prefixes according to the assigned priority. This increases the probability of a legitimate flow of Interest packets. Moreover, least chance is given to the malicious flow of Interest packets that ultimately reduces ISR and increases Interest retransmission count.

### 4.2 Detection phase algorithm

The overall procedure of attack detection is illustrated in Algorithm 1. Whenever a vehicle receives Interest packet(s), it executes the following checks

**ALGORITHM 1 IFA detection procedure**

**Input:** Received Interest packet flow \([\text{Name, Selector(s), NONCE, H, P: Priority of incoming Interest packet flow } F(\alpha)]\)

**Output:** Prioritised flow of incoming Interest packets: \(F(\alpha)\)

1. for each Interest packets flow \(i \in F(\alpha)\) do
2. If \(P = \text{NULL}\) then assign \(P = \text{MAX}\),
3. Calculate \(P_i = \text{ISR} \times \text{CHR} + \text{NL} (P_i \geq 0)\),
4. Scan for suspected prefix list (PL),
5. If entry found in PL then DECREMENT P,
6. If \(P \leq 0.5\) then Drop packet,
7. Update neighbouring nodes,
8. //System under IFA
9. Else if
10. PIT operations,
11. CS lookup,
12. end
13. Return \((F(\alpha))\)
14. end
(i) First, the flow monitor object identifies the type of incoming Interest packet flow \( F(\alpha) \), that is, known or unknown (lines 1–4). For known flow, a collection of metrics is processed to calculate its legitimacy. Otherwise, the initial priority is assigned to the new incoming flow of Interest packets. To return the prioritised flow of Interests \( F(\alpha) \), priority \( P_i \) is calculated with the help of ISR, Interest satisfaction delay (ISD), hop count, and CHR. Equation (1) shows the ratio of cache hits when incoming Interests arrive at PIT of the intermediate node.

\[
CHR = \frac{\text{Presence of Requested Content}}{\text{Total Incoming Interests}} \times 100 \quad (1)
\]

Second, the prefix is analysed to validate the prefix format of incoming Interest packet(s). This is done to protect the NONCE list from storing invalid Interest prefix.

(ii) After that, the metrics collection process is initiated that completes in five cycles. In the beginning, priority \( P_i \) is checked for a previously known flow. If priority is found below 0.5, that flow is declared as suspicious and moved to a suspicious PL. \( P_i \) is decremented and neighbours get intimation of attack (lines 5–10).

(iii) Before transmitting Interest packets to PIT lookup, scheduling is performed to forward high-priority Interest packets.

(iv) Then, a suspicious list check is processed to instantly discard the prioritised incoming flow of Interest packets if the threshold value is found below 0.5 (line 11). Finally, the flow of Interest packets having a threshold count of priority more than 0.5 is allowed to start the PIT and CS lookup process (lines 16–17).

For the priority assignment at each victim and normal node(s), the following calculations are needed to be performed to avoid false detection of IFA.

\[
\text{Interest Satisfaction Ratio}_i = \frac{\sum_{j=0}^{i} \text{Number of Data packets Received}_j}{\text{Number of Interest Packets Sent}_i} \quad (2)
\]

Here, Equation (2) calculates the aggregated ISR value of each face of the intermediate vehicle.

\[
\text{trans Updated Avg}_{\alpha} = \sum_{i=0}^{i=n} (1 - \vartheta) \times \text{PrevAvg}_{\alpha} + \vartheta \times \text{inr}_i \quad (3)
\]

Likewise, in Equation (3), the aggregate value of the average incoming Interest packet rate is calculated at each interface \( i \).

Here, \( \text{trans Updated Avg}_{\alpha} \) is the value of the updated rate of incoming Interest packets at \( n \) interfaces. \( \text{PrevAvg}_{\alpha} \) represents the newly calculated current average rate of incoming Interest packets at the \( \alpha \)th interface, while \( \text{inr}_i \) represents the incoming rate of Interest packets at the \( \alpha \)th node to time.

A skew factor \( \vartheta \) is needed that represents the upper bound and lower bound values of the average incoming rate of Interest packet(s) at each face of the intermediate vehicle. Usually, \( \vartheta \) is calculated to reduce the fading effect during transmission.

\[
\vartheta = \{0.1 \text{ as upper bound, as lower bound}\}
\]

To model the effect of IFA, \( N_w \) is considered as the number of malicious Interest packets that have been sent in a unit of time.

In Equation (4), \( N_L \) denotes the number of legitimate Interest packets besides malicious ones under IFA. Hence, the rate of incoming Interest packets has the following effect on IFA.

\[
N_L = N_L + N_w \quad (4)
\]

\[
\text{ISR} = \frac{\text{Delay} \times \text{Link Bandwidth} \left[ \frac{\text{B/s}}{\text{s}} \right]}{\text{Size of Data chunk} \left[ \text{B} \right]} \quad (5)
\]

The delay parameter is used to calculate the estimated arrival time of the data packet. Moreover, the link capacity for the flow of the Interest packet is calculated to reduce uncontrolled flooding of malicious Interest packets. Equation (5) shows the calculation of ISD, that is, link capacity for a flow of Interest packets. The rate of Interest packet flow through each link is set as 400 ms to maximise the probability of content delivery. In VNDN, 400 ms is an optimal average time for the Interest packet to reach the nearest relay node. Ten simulations are performed to get this average value of Interest packet flow via each link.

For calculation of hop traverse (HT) value by Interest packet at an intermediate node, the following equation has been used:

\[
\text{HT} = h_j + B \times \text{where} (B > 0) \quad (6)
\]

In Equation (6), \( h_j \) is hop count at current node and \( B \) denotes marginal count to get data chunk. To prevent flooding of uncontrolled malicious Interest packets across the network, the maximum threshold value of HT is set to 5. With repeated simulations, it is observed that end-to-end delay increases if the value of HT is set above 5.

Priority value at \( \alpha \)th node \( P_i \) is calculated using Equation (7):

\[
P_i = \frac{\text{ISR} \times CH}{\text{HT} \times \text{ND}} + N_L \quad (7)
\]

where the lower bound of \( P_i \) is greater than 0, while the upper bound is set dynamically.
**Algorithm 2** IFA recovery method

Input: Received suspected Interest packet flow [Name, Selector(s), NONCE, H, P: Priority of incoming Interest packet flow $F(\mathfrak{d})$]

Output: Suspicious node $N(\mathfrak{d})$

1. for each incoming face(s), $f_i \in F(\mathfrak{d})$
2. Maintain fairness queue for $F(\mathfrak{d})$
3. DECREMENT $P_i$
4. DECREMENT Interest lifetime,
5. Update neighbouring nodes,
6. Scan suspected vehicles, $V(\mathfrak{d}) \times N(\mathfrak{d})$
7. Apply Interest trace-back
8. Block traffic from $V(\mathfrak{d})$
9. end
10. Return (attacker’s node)
11. end

5 Malicious Interest packet processing in Recovery Phase

The recovery phase is triggered when the suspicious flow of Interest packets is discarded. For the detection of malicious sources, the Interest push back mechanism is highly preferable. The proposed scheme has implemented a priority-based Interest push back algorithm, where the backtracking process is executed based on the priority of radio interface(s). Algorithm 2 specifies the attack recovery mechanism of the proposed IFA mitigation model. Upon receiving a suspicious flow of Interest packets $F(\mathfrak{d})$, the following counter steps are performed (lines 1–10):

(i) Upon receiving a discarded flow of Interest Packets $F(\mathfrak{d})$, the respective interface has been declared suspicious and priority is decremented.

(ii) After that, fairness queues have been maintained for each face. This is done to establish fairness among radio faces.

(iii) The suspicious face $f_i$ is allocated low fairness to limit the suspicious flow of incoming Interest packets. Priority ($P_i$) and Interest lifetime of $F(\mathfrak{d})$ are also reduced to avoid PIT overflow (lines 2–3).

(iv) Neighbouring vehicles get intimated about the suspicious flow of Interest packets $N(\mathfrak{d})$ (line 4).

(v) Finally, the backtracking process is executed to identify attacking vehicles $V(\mathfrak{d})$ (lines 6–9).

In both algorithms, the time complexity is linear and calculated as $O(n)$, where $n$ is the flow of incoming Interests. For congestion calculation in [16], the authors take two parameters negative acknowledgment (NACK) and timed out Interests. The values of these parameters are compared to check whether the network is congested or not. The time complexity of the existing approach is $O(n^2)$.

6 EXPERIMENTATION AND RESULTS

6.1 Simulation setup

For implementation, analysis, and testing of the proposed research methodology, NDN simulator (ndnSIM) [39] has been used. The ndnSIM is an emulator for NS-3 [40]. The simulation scenario is based upon a built-in waypoint mobility model [41], that is, a random waypoint mobility model, where the velocity of moving vehicles changes randomly, though bounded by the network topology. Ubuntu 18.04 LTS version is used as a base operating system. Eclipse IDE version-4.12.0 is used for programming purposes. R-Studio version-1.2 and WPS Spreadsheet (designed for Linux) have been used for mapping acquired simulation results to the graphical layout.

Moreover, IEEE 802.11p is used for V2V communication as shown in Table 4. This research work aims to compare the aforementioned attack mitigation methods in VNDN to quantify the rate of satisfied Interest packets for the legitimate intermediate vehicle(s) when they are under attack. The minimum and maximum range of Interest satisfaction rates for valid users under the IFA window are plotted as well.

6.2 Results and discussion

The proposed IFA mitigation scheme, that is, PP-FIRM, is compared with the existing scheme(s), namely, a per-face rate-limiting scheme known as a congestion-based Interest rate-limiting scheme [16]. An attacking window has been considered to evaluate the performance of IFA mitigation schemes under normal and abnormal circumstances. The existing scheme in a...
TABLE 4  Simulation parameters

| Parameter                        | Value                      |
|----------------------------------|-----------------------------|
| Communication model              | MAC, 802.11p (10 MHz)       |
| Connection type                  | NDN                         |
| Antenna type                     | Omnidirectional             |
| Simulation time                  | 0–150 s                     |
| Attacking time                   | 50–100 s                    |
| Interest lifetime                | 2 s                         |
| Pending interest table (PIT) size| As per Interest lifetime    |
| Content store (CS) size          | 100 (MAX)                   |
| CS policy                        | Least recently used         |
| Mobility model                   | Random way point            |
| Transmission range               | ~300 m                      |
| Forwarding strategy              | Priority-based best route    |
| Legitimate Interest packets rate  | 50% of total incoming Interests packets |
| Malicious Interest packets rate   | 50% of total incoming Interests packets |
| Malicious Interest names         | 100 random suffixes         |
| Malicious nodes                  | 1–5                         |

6.2.1 ISR

Interest Satisfaction Ratio or ISR specifies the network throughput. Figure 5 shows the ISR of the proposed IFA mitigation scheme for incoming Interest packets. During attacking window 4–11, IFA mitigation methods start countermeasures to protect PIT from malicious Interest packets. It is done to prevent PIT to reach its bottleneck. It can be seen in Figure 5 that PP-FIRM works efficiently under the attacking window. The proposed scheme is compared with the exiting attack mitigation solution to measure effectiveness and improvement concerning ISR. When the transmission of Interests leaves the attacking window (4–11), IFA mitigation schemes show nearly similar performance as attacking nodes stops injecting malicious Interests. During IFA, the proposed countermeasure has produced better results, that is, 21% more ISR as compared to other attack mitigation methods.

6.2.2 Interest retransmission count

During IFA, the number of unsatisfied Interest packets increases, which causes packet retransmissions, until Interest packet lifetime expires (i.e. 4 s) in PIT. Primarily, the proposed attack mitigation method aims to reduce the rate of Interest packet retransmissions by assigning low priority to those outgoing interfaces that undergo more retransmissions. The proposed PP-FIRM scheme experiences 28.6% less Interest retransmissions during the attacking window (4–11) as shown in Figure 6. The reason is the implementation of the IFA prevention method. It modifies the native NDN best route Interest forwarding scheme to assign priority according to retransmission count on the outgoing face(s). This eventually blocks malicious Interest retransmission from the suspicious outgoing face.

6.2.3 PIT utilisation ratio

PIT utilisation ratio, which is also known as the PIT consumption rate, specifies the number of stored malicious Interest prefixes over the total number of Interest prefixes in PIT of an intermediate node. When there is an attack in a VNDN scenario, the PIT utilisation ratio of an intermediate node increases as the attacker keeps on sending malicious Interest packets towards the neighbouring nodes. Eventually, the PIT memory of the attacked node gets exhausted and legitimate Interest packets get discarded. In Figure 7, when no attack mitigation scheme is applied, the PIT utilisation ratio begins to increase as malicious incoming Interest packets are received at an intermediate vehicle during the attacking window (4–11). The variation in the PIT utilisation ratio of the proposed scheme specifies the high mobility of vehicular nodes. Moreover, when a vehicle goes out of sight, it receives less amount of incoming Interest packets, thus, sustaining the rate of PIT consumption. For the PP-FIRM scheme, there are 57% less malicious Interest packets in PIT during an attack as compared to a congestion based per-face rate-limiting scheme.
CHR is defined by the number of cache hits over the total number of incoming Interest packets. The phenomenon where Interest packets that find requested content chunk in the cache of an intermediate node is considered as a cache hit. During IFA, the CHR gets reduced, as Interest packets arrive with non-existent content prefixes. The proposed scheme has used the least recently used (LRU) cache eviction policy that contains the most frequently requested content and discards unpopular cached content. In Figure 8, it can be seen that the CHR is higher during the attacking window (4–11). The proposed research solution has generated a 21.4% more CHR as compared to a per-face attack limiting scheme.

6.2.4 | Interest packet collision rate

When many Interest packets cannot get the requested chunk of data, they are forwarded towards other potential content provider(s), and this causes collisions. As a result, legitimate Interest packets face congestion and long delays. The proposed novel attack mitigation scheme reduces the propagation of an abundant number of malicious packets. Consequently, forwarded Interest packets suffer from fewer packet collisions. In Figure 9, the proposed PP-FIRM scheme has reduced the Interest packet collision rate to 60% during the attacking window (4–11) as compared to the congestion based per-face Interest rate-limiting scheme.

6.2.5 | Timed out Interest packets ratio

In NFD, when a new Interest packet arrives at an intermediate node, it waits in PIT until it gets the requested chunk of cached data. After 4 s, the entry of the waiting Interest packet is removed from PIT. The ratio of timed out Interest packets with incoming Interest packet specifies the number of unsatisfied Interest packets that face timeout in PIT. In Figure 10, it can be seen that during the attacking window (4–11), the number of timed out Interest packets is huge in the absence of an attack mitigation scheme. However, when an attack mitigation strategy is applied, the ratio is quite reduced. It has been found that the proposed attack mitigation model experience 60% less timed out Interest packets as compared to the per-face congestion-based rate-limiting scheme.

6.2.6 | Random attackers

In real-time attack scenarios, the number of malicious nodes is randomly distributed, and attackers collaboratively launch a DDoS attack. Similarly, in the VNDN environment, the number of attackers changes at different time slots of the attacking window. In Figure 11, the density of attackers changes over time. The number of attacking vehicles increases incoming malicious Interest packet transmission across the intermediate node. This results in increased congestion and longer delays.
nodes. This reduces ISR and increases the packet collision ratio. Upon implementation, it has been observed that the proposed attack mitigation model gives 23.6% more ISR as compared to the per-face congestion-based Interest rate-limiting scheme. Moreover, the results show that the proposed attack mitigation scheme is robust and maintains relatively high ISR when multiple attackers disseminate malicious Interest packets.

6.2.7 End-to-end delay

The time taken during transmission of an Interest packet between the source node (sender) and content provider (receiver) is calculated as an end-to-end delay. End-to-end delay between the consumer and the data producer during the attack has been depicted in Figure 12. It can be seen that end-to-end delay increases between the sender and receiver when the number of vehicular nodes increases. The proposed novel attack mitigation scheme reduces the propagation of an abundant number of malicious packets. Consequently, forwarded Interest packets suffer from fewer packet collisions and network congestion. The proposed PP-FIRM scheme has reduced end-to-end delay to 53.4% as compared to the congestion based per-face Interest rate-limiting scheme.

The IFA mitigation is comprised of attack detection and recovery. The attack detection phase monitors the abnormalities in the network’s behaviour, while the attack recovery phase is concerned with the identification of a suspicious node. In this research work, we have proposed the PP-FIRM scheme to enhance the IFA mitigation strategy in VNDN. Moreover, the proposed strategy focuses on the prime metrics, such as ISR, Interest retransmission ratio, PIT utilisation ratio, CHR, timed out Interest packets, and packet collision ratio. These metrics are essential to evaluate the performance of IFA mitigation in VNDN as shown in Table 5. For the comparison, we have selected the most appropriate per-face Interest rate monitoring scheme based strategy, that is, congestion-aware IFA mitigation scheme [16]. According to the achieved statistics based on selected metrics, the proposed PP-FIRM performed better than the existing IFA mitigation scheme in terms of:

1. Higher ISR
2. Reduced Interest retransmission ratio
3. Reduced PIT utilisation ratio
4. Enhanced CHR
5. Less timed out Interest packets
6. Low packet collision ratio.

From Figures 5–12, we can say the PP-FIRM performed better during the attacking window as compared to the existing IFA mitigation solution [16]. The reason is that the proposed scheme efficiently detects abnormal behaviour of the network and block the suspicious flow of incoming Interests. Moreover, overreaction has been avoided through an appropriate threshold count for suspicious Interest flows. The proposed scheme has reduced flooding of malicious Interests, PIT utilisation, and packet collision ratio. Consequently, the ISR of VNDN increases.

7 CONCLUSION

This study has presented a novel attack mitigation scheme named PP-FIRM to counter IFA in VNDN. The proposed IFA mitigation strategy efficiently identifies the suspicious flow of Interest packets and triggers attack recovery mechanism to reduce the flow of malicious Interests. It is observed that the
existing IFA mitigation scheme is unable to prevent the unso-
licted flooding of malicious Interests. The aim of PP-FIRM is
not only the detection of malicious Interests but also the
prevention of flooding of malicious Interests. Hence, we have
also included the IFA prevention phase for reducing the suspi-
cious flow of Interests. We have simulated both the congestion-
based IFA mitigation scheme and the proposed scheme to eval-
uate their performance. The results show that the proposed
PP-FIRM strategy performs better than the existing per-face
congestion-based method in terms of ISR, Interest retransmis-
sion count, CHR, packet collision ratio, timed out Interest pack-
ets ratio, PIT utilisation ratio, end-to-end delay, and network scalabil-

**ORCID**

Syed Asad Hussain 🐧 https://orcid.org/0000-0002-8264-7857

**REFERENCES**

1. Skricketi, V., Šabanović, E., Žuraulis, V.: Autonomous road vehicles: Recent
   issues and expectations. IET Intel. Transport Syst. 14(6), 471–479 (2020)
2. Yurtsever, E.: A survey of autonomous driving: Common practices and
   emerging technologies. IEEE Access 8, 58443–58469 (2020)
3. Nazakat, I., Khurshid, K.: Intrusion detection system for in-vehicular commu-
   nication. In: Proceedings of 15th International Conference on Emerging
   Technologies (ICET), Peshawar, Pakistan, pp. 1–6 (2019)
4. Khan, F., Njuguna, S.K.: Location-based data delivery between vehicles and
   infrastructure. IET Intel. Transport Syst. 14(5), pp. 288–296 (2020)
5. Khelifi, H., et al.: Security and privacy issues in vehicular named data nets-
   works: An overview. Mobile Inf. Syst. 18, 1–11 (2018)
6. Barnett, Jr., T.: Cisco Annual Internet Report (2017–2022). (2018).
   https://newsroom.cisco.com/press-release-content?articleId=1555935
7. Martínez-Díaz, M., Sotong, E., Pérez, L.: Autonomous driving: A bird’s eye
   view. IET Intel. Transport Syst. 13(4), 563–579 (2019)
8. Tang, L., Duan, Z., Zhu, Y.: Data dissemination in service discovery for
   vehicular ad hoc networks: A survey. IET Intel. Transport Syst. 12(10),
   1189–1200 (2018)
9. Wang, A., et al.: NDNVIC: Named data networking for vehicle infrastruc-
   ture cooperation. IEEE Access 7, 62231–62239 (2019)
10. Yang, N., Chen, K., Liu, Y.: Towards efficient NDN framework for con-
    nected vehicle applications. IEEE Access 8, 60850–60866 (2020)
11. Kumar, S., Mann, K.S.: Prevention of DoS attacks by detection of multiple
    malicious nodes in VANETs. In: Proceedings of International Conference
    on Automation, Computational and Technology Management (ICACTM),
    London, United Kingdom, pp. 89–94 (2019)
12. Wu, W., et al.: A Survey of intrusion detection for in-vehicle networks.
    IEEE Trans. Intell. Transp. Syst. 21(3), 919–933 (2020)
13. Nguyen, T., et al.: Reliable detection of interest flooding attack in real
    deployment of named data networking. IEEE Trans. Inf. Forensics Secur.
    14(9), 2470–2485 (2019)
14. Hou, R., et al.: Theil-based countermeasure against interest flooding
    attacks for named data networks. IEEE Network 33(3), 116–121 (2019)
15. Zhi, T., et al.: Resist Interest flooding attacks via entropy–SVM and
    Jensen–Shannon divergence in information-centric networking. IEEE Syst.
    J. 14(2), 1776–1787 (2020)
16. Benouassa, A., et al.: A novel congestion-aware interest flooding attacks
detection mechanism in named data networking. In: Proceedings of IEEE
   28th International Conference on Computer Communication and Net-
   works (ICCCN), Valencia, Spain, pp. 1–6 (2019)
17. Nguyen, T., Cogranne, R., Doyen, G.: An optimal statistical test for
    robust detection against Interest flooding attacks in CCN. In: Proceedings
    of IEEE International Symposium on Integrated Network Management
    (IM), Ottawa, Canada, pp. 252–260 (2015)
18. Yin, G., et al.: Controller based detection scheme of interest flooding attack
    in named data networking. In: Proceedings of IEEE 5th International
    Conference on Computer and Communications (ICCC), Chengdu, China,
    pp. 1628–1633 (2019)
19. Cheng, G., et al.: Detecting and mitigating a sophisticated interest flooding
    attack in NDN from the network-wide view. In: Proceedings of IEEE
    First International Workshop on Network Meets Intelligent Computations
    (NMIC), Dallas, TX, USA, pp. 7–12 (2019)
20. Huang, W., et al.: Cluster-based cooperative caching with mobility predic-
    tion in vehicular named data networking. IEEE Access 7, 23442–23458
    (2019)
21. Zhu, X., et al.: A popularity-based collaborative caching algorithm for
    content-centric networking. J. Commun. 11(10), 886–895 (2016)
22. Meng, Y.: EHCIFP. An efficient hybrid content placement strategy in named
data network caching. IEEE Access 7, 155601–155611 (2019)
23. Narayanan, A., et al.: DeepCache: A deep learning based framework for
    content caching. In: NetAT18: ACM SIGCOMM 2018 Workshop on Net-
    work Meets AI & ML, Budapest, Hungary (2018)
24. Zhang, Y., et al.: A mobility-aware vehicular caching scheme in content
    centric networks: Model and optimization. IEEE Trans. Veh. Technol.
    68(4), 3100–3112 (2019)
25. Van, D.D., et al.: Efficient caching strategy in content-centric networking
    for vehicular ad-hoc network applications. IET Intel. Transport Syst. 12(7),
    703–711 (2018)
26. Tariq, A., Rehman, R.A., Kim, B.: Forwarding strategies in NDN-based
    wireless networks: A survey. IEEE Commun. Surv. Tutorials 22(1), 68–95
    (2020)
27. Zhang, Y., et al.: Concurrent multipath routing optimization in named data
    networks. IEEE Internet Things J. 7(2), 1451–1463 (2020)
28. Maryam, H., Wahid, A., Shah, M.A.: Mitigating broadcast storm in inter-
    est/data packet forwarding in vehicular content centric networking. In:
    Proceedings of International Conference on Communication Technolo-
    nies (ComTech), Rawalpindi, Pakistan, pp. 162–167 (2017)
29. Ahmed, S.H., Yaqub, M.A., Song, H.: DIFS: Distributed interest forwarder
    selection in vehicular named data networks. IEEE Trans. Intell. Transp.
    Syst. 19(9), 3076–3080 (2018)
30. Zhang, X., Li, R.: An ARI-HMM based interest flooding attack counter-
    measure in NDN. In: Proceedings of IEEE 23rd International Conference
    on Computer Supported Cooperative Work in Design (CSCWD), Porto,
    Portugal, pp. 10–15 (2019)
31. Zhang, X., Li, R.: A charging/rewarding mechanism-based interest flood-
    ing attack mitigation strategy in NDN. In: Proceedings of IFIP/IEEE
    Symposium on Integrated Network and Service Management (IM), Arling-
    ton, VA, USA, pp. 402–407 (2019)
32. Tahir, M.U., Rehman, R.A.: CUIF: Control of useless interest packets
    flooding in vehicular named data networks. In Proceedings of IEEE
    International Conference on Frontiers of Information Technology (FIT),
    Islamabad, Pakistan (2018)
33. Khelifi, H., et al.: Named data networking in vehicular ad hoc networks:
    State-of-the-art and challenges. IEEE Commun. Surv. Tutorials 22(1),
    320–351 (2020)
34. Wang, R.: V2V-based method for the detection of road traffic congestion.
    IET Intel. Transport Syst. 13(5), 880–885 (2019)
35. Tourani, R., et al.: Security, privacy, and access control in information-
    centric networking: A survey. IEEE Commun. Surv. Tutorials 20(1), 566–
    600 (2018)
36. Fang, C., et al.: A survey of mobile information-centric networking: Research
    issues and challenges. IEEE Commun. Surv. Tutorials 20(3), 2353–2371
    (2018)
37. Liu, L., et al.: The detection method of collusive interest flooding attacks
    based on prediction error in NDN. IEEE Access 8, 128005–128017
    (2020)
38. Signorelli, S., et al.: Advanced Interest flooding attacks in named-data
    networking. In: Proceedings of IEEE 16th International Symposium on
    Network Computing and Applications (NCA), Cambridge, MA, pp. 1–10
    (2017)
39. Introduction-ndnSIM. https://ndnsim.net/current/intro.html (2019). Accessed 28 Dec 2019
40. Documentation-NS-3 https://www.nsnam.org/ (2019). Accessed 28 Dec 2019
41. Waypoint Mobility Model-NS-3. https://www.nsnam.org/doxygen/classns3_1_1_waypoint_mobility_model.html (2019). Accessed 28 Dec 2019

How to cite this article: Abdullah M, Raza I, Zia T, Hussain SA. Interest flooding attack mitigation in a vehicular named data network. IET Intell Transp Syst. 2021;15:525–537. https://doi.org/10.1049/itr2.12042