Survivability Analysis of MANET Routing Protocols under DOS Attacks

Sohail Abbas[1*], **Muhammad Haqdad**[2], **Muhammad Zahid Khan**[2], **Haseeb Ur Rehman**[2], **Ajab Khan**[2], **Atta ur Rehman Khan**[3]

[1] Department of Computer Science, College of Computing and Informatics, University of Sharjah,
Sharjah, UAE
[e-mail: sabbas@sharjah.ac.ae]

[2] Department of Computer Science and I.T, University of Malakand,
Dir Lower, KPK, Pakistan
[e-mail: haqdad5050@gmail.com,{mzahidkhan, haseeburrahman, ajabkhan}@uom.edu.pk]

[3] College of Engineering and Information Technology, Ajman University
Ajman, UAE
[e-mail: dr@attaurrehman.com]

*Corresponding author: Sohail Abbas

*Received December 19, 2019; revised March 24, 2020; accepted April 29, 2020;
published September 30, 2020*

Abstract

The network capability to accomplish its functions in a timely fashion under failures and attacks is known as survivability. Ad hoc routing protocols have been studied and extended to various domains, such as Intelligent Transport Systems (ITSs), Unmanned Aerial Vehicles (UAVs), underwater acoustic networks, and Internet of Things (IoT) focusing on different aspects, such as security, QoS, energy. The existing solutions proposed in this domain incur substantial overhead and eventually become burden on the network, especially when there are fewer attacks or no attack at all. There is a need that the effectiveness of these routing protocols be analyzed in the presence of Denial of Service (DoS) attacks without any intrusion detection or prevention system. This will enable us to establish and identify the inherently stable routing protocols that are capable to survive longer in the presence of these attacks. This work presents a DoS attack case study to perform theoretical analysis of survivability on node and network level in the presence of DoS attacks. We evaluate the performance of reactive and proactive routing protocols and analyse their survivability. For experimentation, we use NS-2 simulator without detection or prevention capabilities. Results show that proactive protocols perform better in terms of throughput, overhead and packet drop.

Keywords: Ad hoc routing protocols, selfish node, black hole, denial of service, survivability.

http://doi.org/10.3837/tiis.2020.09.004 **ISSN : 1976-7277**

1. Introduction

Mobile Ad hoc Network (MANET) is temporarily constructed in a fully self-organized fashion. The network is not dependent on any predefined centralized architecture where a source to destination communication is performed in multi-hopping via intermediate nodes. Some of the important applications of these networks are wireless sensor networks, vehicular ad hoc networks, robot networks, unmanned aerial vehicles [1], underwater networks [2], Internet of Things (IoT) [3] and so on.

Due to special characteristics of these networks, such as their open nature (i.e. nodes may join and leave at any time), mobile and resource constraint devices, they need specially designed routing protocols. For example, the routing protocols need to tolerate the changes incurred by the topology due to mobility. Since, battery is a scarce resource in these networks; the routing protocols should be made lightweight in order to consume fewer resources. In MANET, routing generally is classified into reactive and proactive protocols. Destination-Sequenced Distance-Vector Routing Protocol (DSDV) [4], Optimized Link State Routing Protocol (OLSR) [5], Ad hoc On-Demand Distance Vector (AODV) [6] and Dynamic Source Routing (DSR) [7] are the popular and extensively cited proactive and reactive routing protocols. The former two are proactive while the latter two are reactive protocols. Routing is cooperative in ad hoc networks: each mobile node besides being a host, operates as a router as well, providing communication services to its neighboring nodes. However, the malicious nodes may not follow the routing procedure. For example, some nodes may not allow their resources to be used by others and hence, pose reluctance to this cooperative routing, i.e. they drop other nodes' packets causing service holes in the network.

In this paper, we categorize the packet dropping behavior into two classes, i.e. active and passive. In the former type of attack, an attacker advertises fake shortest paths to the destinations intending to attract network traffic. The attacker then drops all or selective packets which is called black hole and grey hole attack respectively. This malicious activity is also called active Denial of Service (DoS) attack. The black hole attack can also be launched against a victim node. In that case, the malicious node broadcasts fabricated best routes on behalf of the victim node. As a result, all the traffic is diverted towards the victim node thereby depleting its resources uselessly. In this paper, we will consider the first version of this attack. The passive version of this attack happens when an attacker drops all or selective packets received for forwarding purpose. This form of attack is different than the previous one because in the passive form the attacker does not maliciously attract network traffic. This is also called passive DoS attack.

The above mentioned reactive and proactive routing protocols play an important role because they have recently been modified and extended into different emerging domains, such as Unmanned Aerial Vehicles (UAVs) [1], Intelligent Transport Systems (ITSs) [8-10], Bio-inspired applications [11], underwater networks [12], and Internet of Things (IoT) [3]. Researchers focus their efforts on improving different aspects of these protocols, for example, security [13-16], energy [17], and mobility [18-20]. However, in the presence of the above mentioned attacks, the routing protocols are needed to be evaluated and compared in order to establish the inherent strength of these protocols for network survivability and fault tolerance. According to M. N. Lima *et al.* [21], "survivability is the ability of a system to fulfil its mission in a timely manner, in the presence of attacks, failures or incidents". Protocols that provide services in the presence of attacks and failures are called survivable protocols.

Based on our knowledge, no such work has been done on the survivability analysis of ad hoc routing dealing with both of the above mentioned DoS attacks. Similarly, no comprehensive simulation based evaluation has been done in order to find the effect of these attacks on the proactive and the reactive protocols. It is worth mentioning to note that in the literature various solutions have been proposed, for instance [22, 23] for passive and [24] for active DoS attacks. But since these solutions incur substantial overhead and eventually become burden on the network, especially when there is fewer attacks or no attack at all, as pointed out by [25]. Apart from survivability analysis, the paper also analyses the effectiveness of the routing protocols in the presence of DoS attacks without any intrusion detection or prevention system. This will enable us to establish and identify the inherently stable routing protocol that will survive longer in tolerating these attacks. To answer these questions, in this paper, we make the following contributions.

- We analytically evaluate the adverse effect of the DoS attackers on the data forwarding service of the ad hoc routing protocols.
- We theoretically analyse survivability on the node and the network level.
- We assess the performance of the ad hoc routing protocols through NS2 network simulator using various evaluation metrics. Results obtained demonstrate that proactive protocols perform better in terms of throughput, overhead and packet drop.

This article is organized into various sections. In Section 2, we describe MANET routing protocols in brief and the related work while highlighting the problem in the existing literature. Section 3 is about the theoretical analysis of the adverse effects of DoS attacks on the routing. In Section 4, we analytically analyse survivability of the network accompanied with attacks. Section 5 describes the performance evaluation of reactive and proactive routing protocols. In Section 6, the results and discussion are presented where we analyse the survivability of the routing protocols and suggest future improvements. The conclusion is outlined in Section 7.

2. Related Work

Due to the dynamic nature and infrastructure-less configurations of MANETs, route establishment and exchange of information is different from other networks. Routing protocols for MANETs can broadly be classified into *Flat*, *Hierarchical* and *Geographical* protocols. In this paper, we focus on flat routing protocols for comparison and analysis. The flat routing protocols may be classified into *Proactive* and *Reactive* protocols. Since, in proactive protocols each node maintains a routing table to all destinations, therefore, they are also called table-driven protocols. The routing information in these tables is updated periodically due to the changes induced in topology because of mobility of nodes. But the frequent route updates yield a higher overhead cost; however, due to the route frequent maintenance, latency is significantly reduced. Some of the most famous and widely cited proactive routing protocols are: DSDV [4] and OLSR [15].

On the other hand, the reactive protocols are commonly known as o*n-demand* routing protocols, because in these protocols the route to the destination is established when required, hence it reduces the periodic generation of control overhead. Basically, for route discovery, a source node initially broadcasts a Route Request (RReq) message in the network, and then it only maintains the effective routes while relinquishing all outdated routes after an active timeout threshold. Given that, these protocols incur comparatively less overhead, due to the fact that routes are only established on demand. Yet, on-demand routing protocols have higher latencies as new routes are being discovered. DSR [7] and AODV [6] are the two most widely known and used on-demand routing protocols in MANET. In the next sub-sections, we explain these protocols in brief. The detail discussion and explanation of these protocols can be found in [26].

2.1 Dynamic Source Routing (DSR) Protocol

In the DSR protocol [7], every node holds a route cache, and upon the discovery of new routes, the route cache is updated accordingly. DSR protocol has two phases i.e. *Route Discovery* and *Route Maintenance.* Any node that wants to communicate to destination, first checks its route cache. If the route to the specified destination exists, then the route will be used for data transfer. However, if there is no route found in the route cache then the existing route discovery process starts in order to establish the route. In the route discovery process, the node broadcasts a RReq control packet within its transmission range. The RReq contains the unique request ID, and the initiator and the destination of the route discovery. In addition, RReq have record of addresses of intermediate forwarder nodes via which the RReq propagates. Once a node receives this RReq packet - and the destination or intermediate node having unexpired route to the destination - then a Route Reply (RREP) message is piggybacked to the initiator node. When a route reply message is received by an initiator node, it stores this route in the routing cache for any future data transfers. In the route maintenance phase, when a node along the path transmits packets to the next hop node, the transmitter waits for a stipulated time in order to receive the passive acknowledgement for the packet. After the timeout, the transmitter retransmits the packet till the threshold reaches. Upon this, the transmitter broadcasts a special control packet called Route Error (RERR) ending with the source node, which initiates another route discovery.

2.2 Ad Hoc on-Demand Distance Vector Routing (AODV)

AODV [6] is a widely used o*n-demand* routing protocol, where route is maintained on every hop. Like DSR, route establishment in AODV occurs in two phases i.e. route discovery and route maintenance. Primarily, all nodes in the network transmit Hello messages as well as capture Hello messages broadcasted by the neighbors. This way a node gets connected to its neighbors, while for route discovery to a particular destination, a RReq message is sent by the source node to its neighbors. But if the path to the destination is not available, then the process is repeated till the destination is found. A node having path information when receives this message sends route reply message back to the sender. Further, the forwarding nodes to the route reply message also save the route information. Besides, the initiator node assigns a unique identifier (ID) to every RReq message. Once a node receives this message, it inspects this identifier. The identifier is discarded if already processed in order to avoid duplication of messages and routing loops. Hence, by applying the reverse path the RReq message is forwarded to the source node and the source node then starts transferring data once receives the RReq message. However, if link failure occurs, a new RReq is sent to all sources using this route in order to inform them of a link failure.

2.3 Destination-Sequenced Distance-Vector Routing Protocol (DSDV)

DSDV [4] is a famous proactive table-driven routing protocol, where a routing table is maintained by each node in the network for all likely destination and also storing other information like number of hops and an end-node generated sequence number. The sequence numbers are employed for the avoidance of routing loops. In addition, the sequence number is increased if the nodes' neighbours change. Once the route is updated, the stale route is changed with a route having a higher sequence number to maintain fresh and updated routes in the table. Hence for routing, the highest sequence number route is selected.

2.4. Optimized Link State Routing Protocol (OLSR)

Another popular proactive protocols is the OLSR [5]. Like DSDV, OLSR provides routes to the requester immediately when demanded. The OLSR is the modified version of the link state routing protocol that reduces control traffic overhead incurred by flooding. OLSR do not allow every node to flood rather only selected nodes will be allowed to flood data in the network; those nodes are called Multi Point Relays (MPRs). In order to determine shortest paths, OLSR needs the partial link state to flood. MPR nodes establish links to their MPR selector nodes. They are then required to forward the control messages further. One of the strengths of OLSR is that it quickly reacts to the topological changes by minimizing the time intervals for periodic control messages transmission. In addition, MPR yields better bandwidth utilization and reduces overhead by using two techniques: first, only MPR selectors are advertised with short messages; second, only MPR forwards broadcast packets.

In the last two decades, various authors have evaluated the ad hoc network routing protocols through several performance metrics. Some have considered existence of attacks while some merely compared the performance, ignoring security attacks. Some authors, on the other hand, did not approach the problem comprehensively, i.e. they either consider the reactive or the proactive routing protocols. So, the three main factors based on which we can categorize these schemes are the number of routing protocols, performance metrics, and the attacks. **Table 1** summaries the existing work with their limitations.

Previous work evaluated the performance using limited number of routing protocols, notably [24, 27] and the author did not consider partial droppers in the evaluation and some even did not consider these attacks in the evaluation at all, for example [28, 29]. The work in [30] examines the impact of packet dropping behavior on three routing protocols DSDV [4], DSR [7], and AODV [6] using metrics, i.e. normalized throughput, routing overhead, normalized routing load and average packet delay.

The research work in [31] focused on the evaluation of OLSR [5] and AODV [6] only; although the author considered black hole attacks. The performance metrics used can also be seen from **Table 1**. Similarly, the work done in [32] concentrated on Temporally ordered routing algorithm (TORA), OLSR, DSR, and AODV which is complete in terms of routing protocols' selection; however, they consider only the black hole attack. The AODV has been investigated in [27] but they considered only the black hole attacks. While considering nodes` mobility, throughput, and delay-based performance metrics were used. Moreover, in [33], the black hole effects were analyzed on routing protocols, such as AODV, DYMO [34] and DSR. The above mentioned studies dealt with the performance evaluation in the presence of attacks but with fewer routing protocols.

The author in [35], investigated the effect of two link state routing protocols, i.e. OLSR and Trust Level Routing Protocol (TLR) on the network survivability and reliability. The main focus was put on network energy without considering any kind of attacks. Black hole attacks are comprehensively analyzed in [24] on top of AODV protocol and new detection mechanisms have been proposed; however, it has not been shown that which routing protocol is inherently more stable than that of AODV during black hole attacks. The work of [36] is closely related to ours, in which ad hoc routing protocols are examined for network survivability in the presence of different Byzantine attacks, including black hole attacks.

Table 1. Comparison of Different Approaches

Approaches	Protocols	Attack Types	Metrics	Simulators	Limitations
[28]	OLSR, ZRP, AODV	No	Throughput, network load, retransmission, data dropped and delay	OPNET	Requires selfish nodes analysis.
[29]	AODV, DSR	No	Throughput, Delay, PDR	NS2	Requires selfish nodes analysis.
[24]	AODV	Black hole	PDR, percentage of routes won	NS3	Evaluate AODV only for black hole attacks.
[30]	AODV, DSR, DSDV	Full packet dropper	Throughput, packet drop, routing overhead, NRL	NS2	Requires investigating more proactive protocols nature and partial packet dropper
[31]	AODV, OLSR	Black hole	End-to-end delay, retransmission attempts, network load, throughput	OMNET++	Need broad comparison of more protocols.
[32, 37, 38]	AODV, DSR, TORA and OLSR	Black hole	PDR, end-to-end delay, packet drop, network throughput	OPNET	Need to investigate partial packet dropper
[27, 38]	AODV	Black hole	Throughput, PDR, end-to-end delay	NS2	Need broad evaluation of more protocols to find the more resistant protocol.
[33]	AODV, DSR, DYMO	Black hole	Throughput, PDF, end-to-end delay, probability of reach ability	QualNet	Only reactive protocols evaluated.
[36]	AODV and ODSBR	byzantine attacks, black holes	PDR and overhead in different settings	NS2	Comprehensive analysis required
[39]	AODV	Black hole and grey	Normalized routing load, overhead & total	NS2	Proactive routing protocols

		hole	dropped packets		performance evaluation is required
[40]	DSR	Packet dropper	Throughput and delay	NS2	Requires performance evaluation of proactive protocol.
[35]	OLSR and TLR	None (energy considerations)	remaining energy of network and reliability	NS2	No attack model considered.
[41]	AODV	Black hole and selfish nodes	Normalized Goodput, end-to-end delay, average hop count, network survivability (analytical)	NS2	Topological survivability was analyzed via simulation and analytically; however, only AODV was used as a case study.

The AODV protocol is used as a case study; however, the author then proposed an improved version of it, i.e. On-Demand Source Based Routing (ODSBR) protocol without comparing the routing protocols for survivability as compared to our approach. Another closely related work to ours is [41]. The author examined the effects of selfish packet droppers and node failures on both network performance and survivability. Again, the author focuses on AODV protocol and that of establishing the effects of node misbehaviors and failures on survivability. A comprehensive analysis of reactive and proactive routing protocols is needed in the presence of both DoS attacks using broad range of evaluation metrics. In order to establish which routing protocols are inherently stable to survive and to be able to provide services in the presence of failures and attacks.

3. Adverse Effect of DoS Attacks

In this section, we analytically show the adverse effect of DoS attacks in the network. For simplicity concerns we consider Passive version of DoS Attacks (PDA). In the lower level, the PDA nodes are involved in the routing paths and start different kinds of malign activities. Irrespective of their behaviour, we want to show the probability of routes being contaminated by the PDA nodes. We define a malicious route as the one having at least one PDA node along the routing path.

3.1 System model

Let us suppose a network is composed of N number of nodes that are randomly distributed over an area of size $X \times Y$. The location of each node is independent of the locations of all the other nodes. The source and the destination nodes are randomly selected in order to establish traffic flows that construct routing paths in the network. The intermediate nodes along the route are chosen as PDA nodes independently with a probability that is denoted by p_s. In our analysis, we examine an arbitrary route having average number of hops, *h*. In any route, intuitively, there will be $h-1$ packet forwarding nodes (routers) along the path from the source to the destination. Each of these intermediate nodes can act maliciously with probability p_s. Now the probability of the path having at least one PDA node is given as

$$p_{sp} = 1-(1-p_s)^{h-1} \tag{1}$$

In order to evaluate Eq. (1) and to determine p_{sp}, the average number of hops *h* of a routing path must be known. We follow a simple approach to estimate the *h*, i.e. first, we estimate the average progress along each hop in the network, *k*. Second, we then approximate the average distance between the source and the destination, *d*. finally, we then can calculate *h* as follows.

$$h = d/k \tag{2}$$

We can further estimate the average 1-hop progress, *k*, as the average maximum distance between the transmitter and each of the neighbours (preferably the farthest one) within its transmission circle. For the sake of simplicity, we assume that the farthest node will be in the direction towards the destination node. The average number of nodes falling in the radio range may be given as

$$\rho = \frac{N}{X \times Y}\left(\pi R^2\right) \tag{3}$$

Where *R* is the transmission range of each node and assuming that to be homogenous across all the network nodes.

The probability of all ρ nodes falling within distance $r_0$from the center of the radio range (assuming location independence and randomness of nodes) may be given as

$$\begin{aligned} F(r_0) &= P(All\ \rho\ nodes\ falling\ within\ a\ circle\ of\ radius\ r_0) \\ &= [P(a\ node\ resides\ with\ r_0)]^{\rho} \\ &= \left[\frac{\pi r_0{}^2}{\pi R^2}\right]^{\rho} \\ &= \frac{r_0{}^{2\rho}}{R^{2\rho}} \end{aligned}$$

By definition, the probability density function $f(r_0)$ of progress r_0 from the source is given by the derivative of $F(r_0)$:

$$f(r_0) = \frac{d}{dr}F(r_0) = \frac{2\rho \times r_0{}^{2\rho-1}}{R^{2\rho}}$$

The average progress *k* can then be calculated as the expected value of *r* w.r.t the $f(r_0)$,

$$k = \int_0^R r_0 f(r_0)dr_0 = \frac{2\rho\ R}{2\rho+1} \tag{4}$$

In Eq. (4), when $\rho = 0$, there can be no progress made, hence, $k = 0$. And, when $\rho = 1$, the progress will become the expected value of the distance on which the only node is located from the center, i.e. $k = \frac{2}{3}R$. Furthermore, when ρ is large the progress ultimately approaches *R*, i.e. $k \to R$. For uniformly distributed nodes in a network of size $X \times Y$ (assuming the squared area: $X = Y$), the expected distance between two random nodes (i.e. source and destination) is given as

$$d = 0.5214054L \tag{5}$$

The *d* in Eq. (5) is the Euclidean distance between a random source and a random destination deployed in a squared area of side *L* [42].

The expected number of hops using Eq. (4) and (5) can be estimated as follows.

$$h \approx \frac{d}{k} \approx \frac{(2\rho+1)\times d}{2\rho\ R} \tag{6}$$

putting the value of *h* in Eq. (1), we get

$$p_{sp} = 1 - (1 - p_s)^{\frac{(2\rho+1)\times d}{2\rho . R} - 1} \tag{7}$$

Table 2. P_s vs. node density

P_s = 0.1			
Nodes	50	100	200
P_{ps}	0.06	0.07	0.08

P_s = 0.2			
Nodes	50	100	200
P_{ps}	0.23	0.25	0.26

P_s = 0.3			
Nodes	50	100	200
P_{ps}	0.43	0.45	0.46

P_s = 0.4			
Nodes	50	100	200
P_{ps}	0.65	0.67	0.67

We use Eq. (7) in order to compare the probability of malicious routes when the network area of size 1000x1000 and 250m radio range for different number of nodes, the numerical results are depicted in Table 2. It is evident from the results that the probability of malicious routes increases with the increase in PDA nodes ratios. The number of nodes also affects the value of P_{ps}, which may be due to more routes created and hence polluted by PDA nodes in the network. Furthermore, the adverse effect of PDA nodes in the network can also be observed from the table. For instance, when the PDA nodes ratio is 30% in the network, around 50% of the routes contain at least one PDA node in the path. This high probability would definitely lead the network into severe throughput performance degradation.

4. Survivability Analysis

We categorize nodes as follows to analyse wireless ad hoc networks survivability:

- *Cooperative nodes*: these nodes provide packet forwarding service to their neighbours and they are non-malicious.
- *Selfish nodes (passive DoS launchers)*: these nodes do not provide packet forwarding service to their neighbours and due to their selfish nature, they don't want to share their resources in the network; however, they consume network services.
- *Black holers (active DoS launchers)*: these are the malicious nodes carrying out active DoS attacks.
- *Faulty nodes*: these are the nodes that cannot take part in the communication due to flat batteries or having some hardware or software faults.

Normally in MANETs, a node is isolated and disconnected from the network when it goes out of range from network nodes due to mobility. It usually happens to the boundary nodes of the network. Another scenario is that when neighbours of a node become faulty or dead due to battery outage and no active neighbour left for communication, the node is deemed to be disconnected. In this paper, we discuss two scenarios in which nodes are virtually disconnected. For example, there are situations in which neighbours of a node do exit physically but they do not cooperate in packet forwarding; as a result, the node is virtually disconnected from the network.

As shown in Fig 1(a), node *S* is surrounded by selfish neighbours which prevents *S* from communicating beyond its 1-hop neighbours. For instance, a path from a source node *S* to a destination node *D* exists via a neighboring node *E*; however, node *E* being selfish makes node *S* to be disconnected and isolated. Similarly, in the second case, shown by Fig 1(b), node *S* is surrounded by both cooperative and malicious nodes, i.e. black hole. In order to communicate with destination *D*, node *S* finds a path to *D* via a cooperative node *E* but the black hole node *B* advertises a false shortest (i.e. 1-hop) path to *D*; as a result, node *S* forwards packets towards *B* (instead of *E*) which makes *S* virtually disconnected. The interesting point to note in this case is that nodes will be deemed as disconnected even if all their neighbours are cooperative except one black hole attacker. This is due to the fact that the black hole attacker will attract all the traffic towards itself by broadcasting falsified shortest routes. We can conclude from Fig 1(b), that the presence of even a single black hole node can disconnect node *S* and hinder it to communicate beyond its 1-hop neighbors, even in the presence of its *n*-1 neighbours.

In the following section, we formally analyse the above scenarios using probability and graph theory, we use the notation given in **Table 3**.

Table 3. Notations

NOTATION	DESCRIPTION
N	mobile ad hoc network
N_c	network of cooperative nodes
$C(N_c)$	connectivity of the cooperative nodes
$S_k(\mathrm{N})$	survivability of network *N*
$P_c(v)$	the number of cooperative node-disjoint (outgoing) paths of a node *v*
P_{co}	probability of a node being cooperative
P_{BH}	probability of a node being a black hole
d	Degree of a node
n_{co}	number of cooperative neighbors
n_{BH}	number of black hole neighbors
n_F	number of faulty neighbors
$\zeta(N)$	minimum node degree of *N*
$\psi(N)$	the minimum cooperative degree of all the nodes in *N*

Definition 1: A wireless ad hoc network *N* is considered to be *k*-connected (for $k \geq 2$), if there exist at least *k* mutually independent routes for each node pair, i.e. *k* node-disjoint routes, connecting them. For this *k*-connected network *N*, the maximum value of *k* is defined to be the connectivity of *N*, which is denoted by $C(N)$.

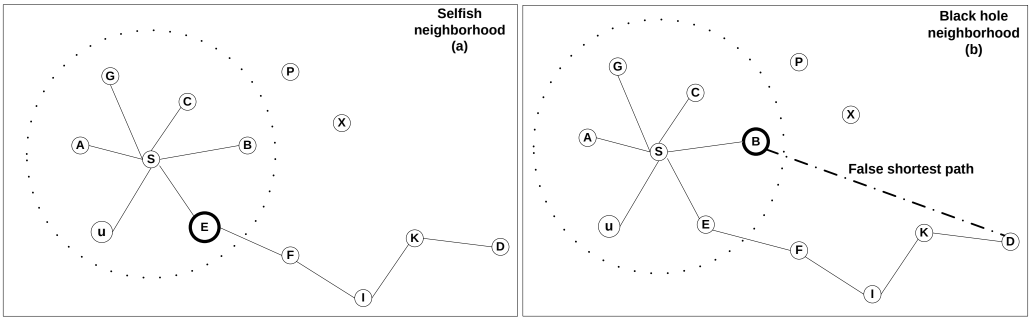


Fig. 1. Neighbourhood analysis of a node: presence of (a) a selfish node and (b) a black hole attacker

The above definition implies that all the network nodes are cooperative (in terms of packet forwarding) and non-malicious. For $k \geq 2$, the network survivability can be analysed as each pair of nodes has at least one alternative backup path available in order to cope with any unpleasant situation, such as path breakups, etc. However, in reality, not all nodes are cooperative. Nodes may be faulty, selfish, or malicious attackers. In that case for connectivity and survivability, we use $C(N_c)$ which denotes the connectivity among cooperative nodes. In order to reflect nodes' behaviour in the network connectivity, Definition 1 will be modified as follows.

Definition 2: Let $C(N_c)$ is the cooperative nodes' connectivity in network *N*, the survivability of *N* denoted by $S_k(\mathrm{N})$, may be defined as the probability that all cooperative (non-malicious) nodes are *k*-connected, i.e.

$$S_k(N) = P_r(C(N_c) = k \mid N_c) \tag{8}$$

Equation (8) demonstrates the probability of cooperative nodes to be k-connected (i.e. at least *k* mutually independent routes containing cooperative nodes for each node pair is there). In order to analyse the network connectivity in the presence of active and passive DoS attackers, first we analyse the connectivity of an individual node and then extend it to the overall network connectivity.

5.1 Probability of a node being disconnected

A node *v* will be disconnected from the network if $P_c(v) = 0$, where $P_c(v)$ are the number of cooperative node-disjoint (outgoing) paths of the node *v*. It is due to the fact that node *v* may communicate in the network only through its cooperative neighbors. Node *v* will be isolated from the network if it's all neighbors are selfish nodes or it has at least one black hole neighbour. More formally, we can formulate this fact as follows. Given a node *v* with degree *d*, if $n_{BH}(v) \geq 1$ or $n_{SL}(v) + n_F(v) = d$, then node *v* has no cooperative neighbour, i.e. $P_c(v) = 0$. So, the probability of a node being disconnected may be given as follows.

$$Pr(P_c = 0|D = d) = 1 - (1 - P_{BH})^d + (1 - P_{co} - P_{BH})^d \tag{9}$$

where, *D* is the degree of a node, P_{co} and P_{BH} are the probabilities of a node being cooperative and a node being black hole, respectively. According to (9), neighbors of a node must not contain any black hole node and must contain at least one cooperative node in order to keep it connected with the network.

5.2 Nodes Probability for being k-connected

The above analysis indicates an individual node being disconnected in a network. Now we need to extend it to *k*-connectivity of a node. A node is said to be *k*-connected if its cooperative neighbours are *k*, i.e. $P_c(v) = k$. And the probability of a node being *k*-connected is given as

$$Pr(P_c = k|D = d) = Pr(n_{co} = k, n_{BH} = 0, n_{SL} + n_F = d - k) \tag{10}$$

Where n_{co} is number of cooperative neighbors, n_{BH} represents black holes, n_{SL} is number of selfish neighbours, faulty neighbours are shown by n_F. Eq. (10) implies that a node *v* has *k* node-disjoint outgoing connections or paths if and only if *v* does not have black hole neighbor and at least *k* cooperative neighbors. Since, the actions and events of these nodes are mutually independent; hence by using the *multinomial probability*, (10) may be written as follows.

$$Pr(P_c = k|D = d) = \frac{d!}{k!(d-k)!} (P_{co})^k (1 - P_{co} - P_{BH})^{d-k}, k \geq 1 \tag{11}$$

After formulating the *k*-connectivity of individual nodes, it is important that we generalize it and extend it to network level. It has been shown in [43] that for a random graph *G* having *N* vertices, the probability that the graph *G* is *k*-connected is approximately equal to the probability of every vertex in *G* has at least *k* neighbours, i.e.

$$Pr(C(G) = k) \cong Pr(\zeta(G) \geq k) \tag{12}$$

Provided that *N* is large enough and $Pr(\zeta(G) \geq k)$ to be almost one, where $\zeta(G)$ is the minimum degree (or vertex degree) of graph *G*. Moreover, [43] has further shown that even if *N* is in the order of 50 and $Pr(\zeta(G) \geq k)$ is not close to one, $Pr(\zeta(G) \geq k)$ still provides a good estimation for $Pr(C(G) = k)$. It is worth mentioning that the above work does not consider DoS attackers. As we discussed above, these attackers do not provide any effective outgoing paths. So, the condition for a network to be *k*-connected would be that every node must have at least *k* benign or cooperative neighbours.

Let $\psi(N)$ be the *minimum cooperative degree* of all the nodes in network *N*, then the above point is formulated by the following theorem.

Theorem 1: Given wireless ad hoc network *N* consisted of *v* nodes (not less than 50 including the attackers), if *N* attains at least *k* cooperative neighbours, then *N* is asymptotically *k*-connected, i.e.

$$Pr(C(N) = k) \cong Pr(\psi(N) \geq k) \tag{13}$$

Proof: let $D(v)$ and $D_c(v)$ are the degree and the cooperative degree of a node *v*, respectively. Intuitively, $D_c(v) \leq D(v) \forall v \in N$ holds then $\psi(N) \leq \zeta(N)$ implies that $\Pr(\psi(N) \geq k) \leq \Pr(\zeta(N) \geq k)$. Similarly, as connectivity cannot be greater than that of the minimum cooperative degree, i.e. $\mathrm{C}(N) \leq \psi(N)$; hence, $C(N) \leq \psi(N) \leq \zeta(N)$. Thus, in general, $\Pr(C(N) = k) \leq \Pr(C(N) \geq k) \leq \Pr(\psi(N) \geq k)$ holds.

Revisiting the definition of survivability in Eq. (8) and theorem 1, the survivability of a network *N* is the probability that all nodes must have at least *k* cooperative neighbours (degree), i.e.

$$S_k(N) \cong \Pr(\psi(N_c) \geq k) \tag{14}$$

Where N_c is a sub-network of *N* formed by all active nodes. In other words, for a *k*-connected network *N* to be survivable is actually the network formed from cooperative nodes N_c because the cooperative nodes are the ones that provide services and connectivity to the network.

5. Performance Evaluation

5.1 Setup Details

This investigation aims to determine the impact of DoS invaders (where they drop selective or all packets) on ad hoc routing protocols under different performance metrics, given below. We designed all our MANETs scenarios in NS-2 with the help of the simulation factors shown in **Table 4**. Some of the parameters given in the table will be explained in the coming subsection. NS-2 is a consummate discrete event simulator used for MANET in research community. Traffic antecedents and descends are randomly selected through the use of Constant Bit Rate (CBR) agents for traffic generation. We practice random way point mobility model that befits the random movement pattern of MANETs. For the simulation work, we simulated 30 random scenarios in each case and then the mean of these 30 simulations is taken.

Table 4. Simulation Parameters

PARAMETER	VALUE
Simulator	NS-2.35
Protocols	DSR, AODV, OLSR, DSDV
Nodes	50
Max. connections	25
Attack type	Packet droppers (partial and full)
Type-1 attackers	0% to 100%
Type-2 attackers	50%
Packet drop rate	0% to 100%
Simulation areas	1000m^2, 2000m^2,3000m^2
Pause time	0, 20, 40, 60, 80, 100
Maximum speed	5, 10, 15, 20, 25, 30 m/sec
Radio range	250m
Traffic type	CBR
Packet size	64 Bytes
Simulation time	900 sec

5.2 Performance Metrics

In Section 2, we have presented the metrics used in the existing work. However, we use almost all of the metrics used in the existing work where these metrics were used in parts. To perform comparison, the efficiency metrics are as under:

- **End-to-end delay:** it is the total time (data) packets utilize to reach their specified destinations divided by the total packets.
- **Packet Drop:** Packet drops due to reasons, such as congestion, attacks, etc. The number of sent packets (at the source) minus the number of received packets (at the destination) computes the packet drop.
- **Packet Delivery Ratio:** it refers to the ratio of total count of received data packets (at application layer) to the count of sent data packets at the same layer.
- **Normalized routing load:** The ratio of the numbers of packets transmitted at the network layer to the number of packets received by the destination at the same layer.

- **Routing overhead:** Routing overhead is the count of forwarded and dispatched events at the network layer.

5.3 Attack Model

Since, the main aim of the active and passive DoS attackers is to drop all or some packets passing through them. We implement two types of attackers, i.e. partial and full packet droppers, irrespective of their mode being active or passive. The full packet dropper is referred to as type-1 and the partial packet dropper as type-2 attackers.

5.4 Result Analysis

In this section, we discuss the results obtained from our simulations as follows.

5.4.1 Type-1 Attackers' Effects

Fig. 2 illustrates the effect of type-1 attacks on the metrics given in Section 6.2 with supplementary simulation parameters given in **Table 5**. With increasing type-1 attackers, proactive protocols provide good PDF performance as compared to reactive protocols, as evident from **Fig. 2(a)**. For networks facing threats of high percentage of type-1 attackers, proactive protocols are a good choice in terms of high PDFs. It is worth mentioning to note that when all the nodes in the network are type-1 attackers, there is still around 10% PDF sustained. The reason for this is that some of the source nodes directly interact with their destination nodes without any intermediate node. This gives rise to increase in the overall PDF (i.e. increase in sent and received events) of the network. Packet drop and routing load increases when attackers increase, as shown in **Fig. 2(b)** and **(c)**; however, proactive protocols perform better, i.e. in packet drop OLSR performs better while in routing load DSDV performs well. In case of delay, all protocols incur high delays at the start (because of fresh route discoveries) and decreased delays afterwards, **Fig. 2(d)**. The DSR protocol suffers more from high delay at the start as compared to others because of determining source to destination routes. AODV performs better because it uses hop-by-hop routing, as opposed to DSR. In **Fig. 2(e)**, the OLSR protocol demonstrates a little bit higher overhead as compared to others; it may be due to the periodic broadcasts for its MPR selections.

5.4.2 Mobility Effect

We also evaluated the protocols for type-1 attackers with varying mobility in the network. **Fig. 3** indicate the outcome for metrics given in Section 6.2 using the supplementary simulation parameters shown in **Table 6**. It is intuitive to note that packet drop and routing load increases with mobility due to frequent link breakages, as shown by **Fig. 3(a)** and **(c)**. However, OLSR exhibits almost persistent behavior pertaining to mobility. Proactive protocols produce high PDFs as compared to reactive protocols, as depicted in **Fig. 3(b)**.

As shown by **Fig. 3(d)**, as usual, the DSR exhibits high latency than all the other protocols which is due to the fact that DSR incurs added latency for its route discoveries. On the other side, initially the proactive protocols expressed lower delays; however, the delay amplifies in reference to mobility because of the optionally varying entries of routing table entries due to mobility. The performance of reactive protocols is almost the same in the case of overhead. The proactive protocols show inconsistent performance. However, they are sturdy against changing mobility, as shown in **Fig. 3(e)**.

5.4.3 Pause Time Effect

In this simulation experiments, **Fig. 4** represents the varying pause times effects on the metrics given in Section 6.2 along with the simulation parameters specified in **Table 7**. In **Fig. 4(a)**, in case of PDF, both reactive and proactive protocols exhibit steadiness for different pause times. The reactive protocols face high packet drops as compared to the proactive protocols, as depicted in **Fig. 4(b)**.

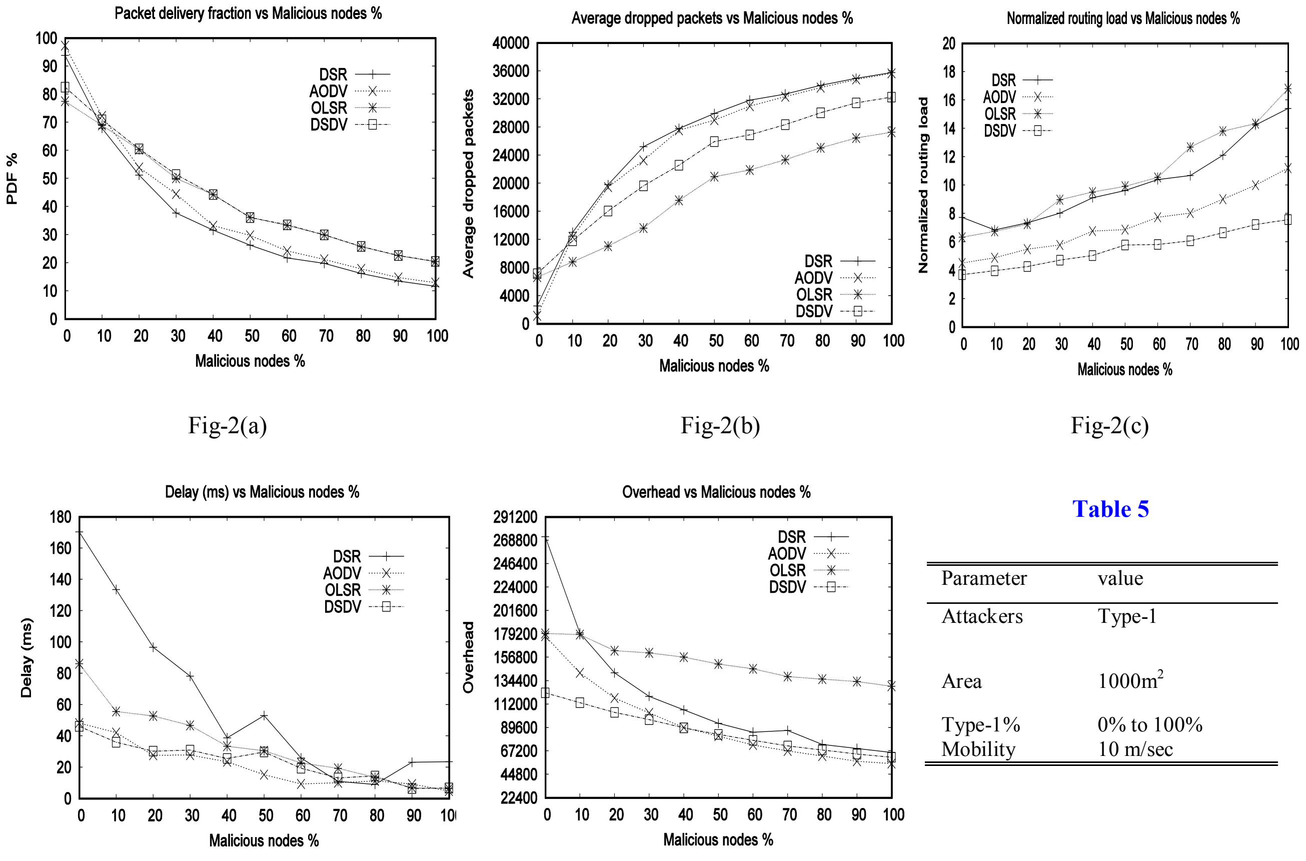


Fig-2(a)

Fig-2(b)

Fig-2(c)

Fig-2(d)

Fig-2(e)

Table 5

Parameter	value
Attackers	Type-1
Area	1000m^2
Type-1%	0% to 100%
Mobility	10 m/sec

Fig. 2. a) PDF vs. type-1 attacks' %, b) Average drop packets vs. type-1 atacker's %, c) Normalized routing load vs. type-1 attackers' %, d) Delay vs type-1 attackers's %, e) overhead vs type-1 attacker's %.

As illustrated in **Fig. 4(c)**, the routing load incurred by DSDV is lower than all others on pause time greater than 20 seconds. The rest of the protocols uphold small increased routing load with respect to pause time increase. The delay incurred by DSDV and AODV is almost the same; however, in OLSR it is almost unpredictable.

The DSR suffers from high delay as usual; see **Fig. 4(d)**. The ensued overhead is depicted in **Fig. 4(e)**. Reactive protocols incur same overhead while the proactive protocols on the other hand do not produce consistent results. For instance, DSDV incurs lowest while OLSR incurs highest overhead.

5.4.4 Terrain Size Effect

In Fig-5, the results for different terrain size using metrics given in the figure are illustrated based on the simulation parameters given in **Table 8**. The network sparseness affects the overall performance of routing protocols. For instance, sparseness increases packet drop rate, as shown in **Fig. 5(a)**. The proactive protocols suffer less because they try to maintain their routing table up-to-date via periodic updates. And fresh alternative paths are easily available to nodes when one route fails due to network sparseness. Same is the case with the routing load, which increases with respect to the sparseness; however, DSDV incurs low load, as shown in **Fig. 5(b)**.

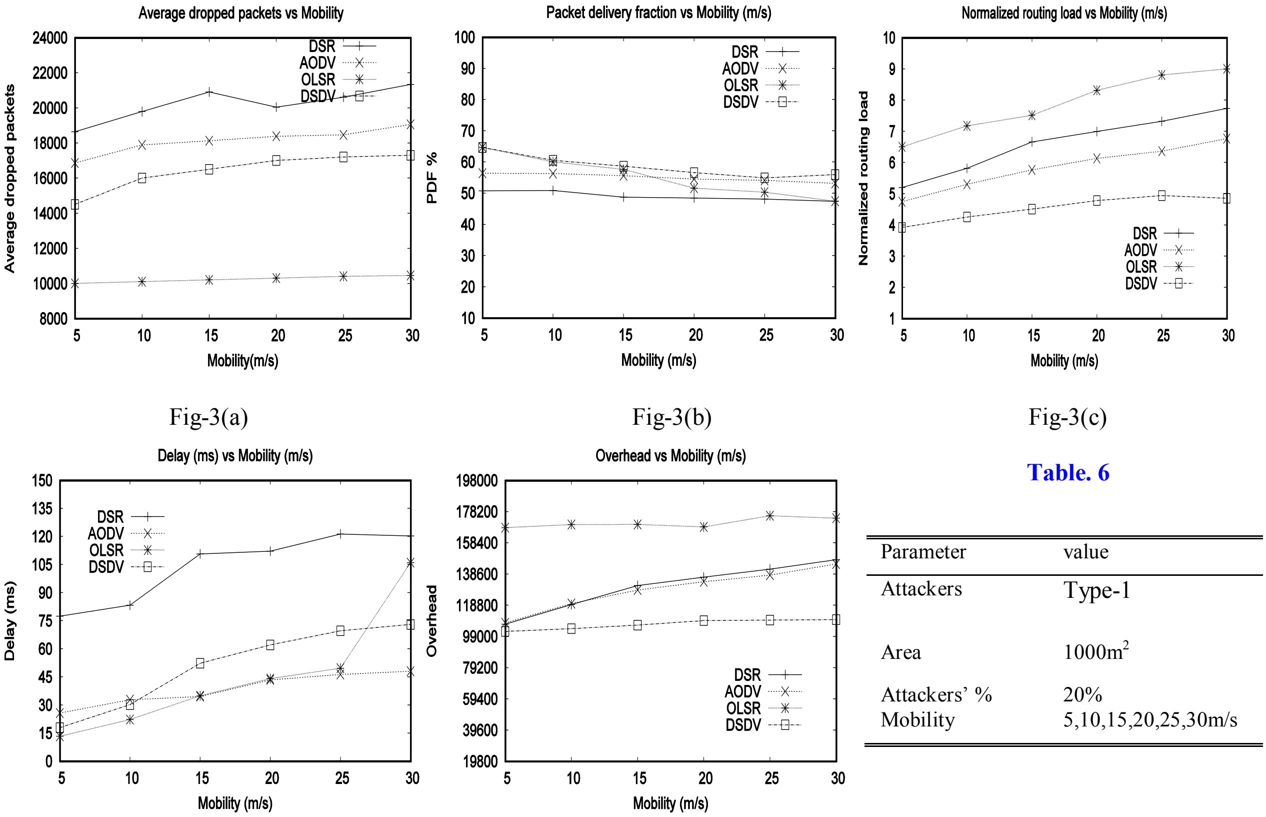


Fig-3(a)

Fig-3(b)

Fig-3(c)

Fig-3(d)

Fig-3(e)

Fig. 3. a) Average packet drop vs. Mobility, b) PDF vs. Mobility, c) Normalized routing load vs. Mobility, d) Delay vs. Mobility, e) Overhead vs. Mobility.

Table. 6

Parameter	value
Attackers	Type-1
Area	1000m^2
Attackers’ %	20%
Mobility	5,10,15,20,25,30m/s

Reactive protocols produce about same performance in terms of routing overhead. However, proactive protocols exhibit incoherent performance, i.e. OLSR‘s has the highest overhead whereas DSDV’s has the lowest, in contrast, as shown in **Fig. 5(c)**. **Fig. 5(d)** represents the proactive protocols delay, which is lower than the reactive protocols. PDFs’ of all protocols increase with the terrain size, depicted in **Fig. 5(e)**.

5.4.5 Type-2 Attackers Effects

Fig. 6 shows the effect on the metrics when type-2 attackers (partial droppers) are in action.

The supplementary simulation parameters can be found in **Table 9**. In this simulation scenario, the type-2 attackers drop rate increases from 0% to 100%, as can be seen on the x-axis in the figure. **Fig. 6(a)** shows the average PDF of partially packet drops percentage. The overall PDR of proactive routing protocols is high on 40% drop rate and higher and almost alike for both DSDV and OLSR. In contrast, when the drop rate is low, on-demand protocols exhibits better performance. In **Fig. 6(b)** the overall comparative results show that the OLSR outperforms other protocols. It is clear from the results that reactive protocols show stable behavior in such attacks. Results in **Fig. 6(c)** represent the increasing drop rate with the normalized routing load for all protocols. Likewise, OLSR produces more loads on the network, while DSDV bears fewer loads, but it is increased with the increase in drop rate.

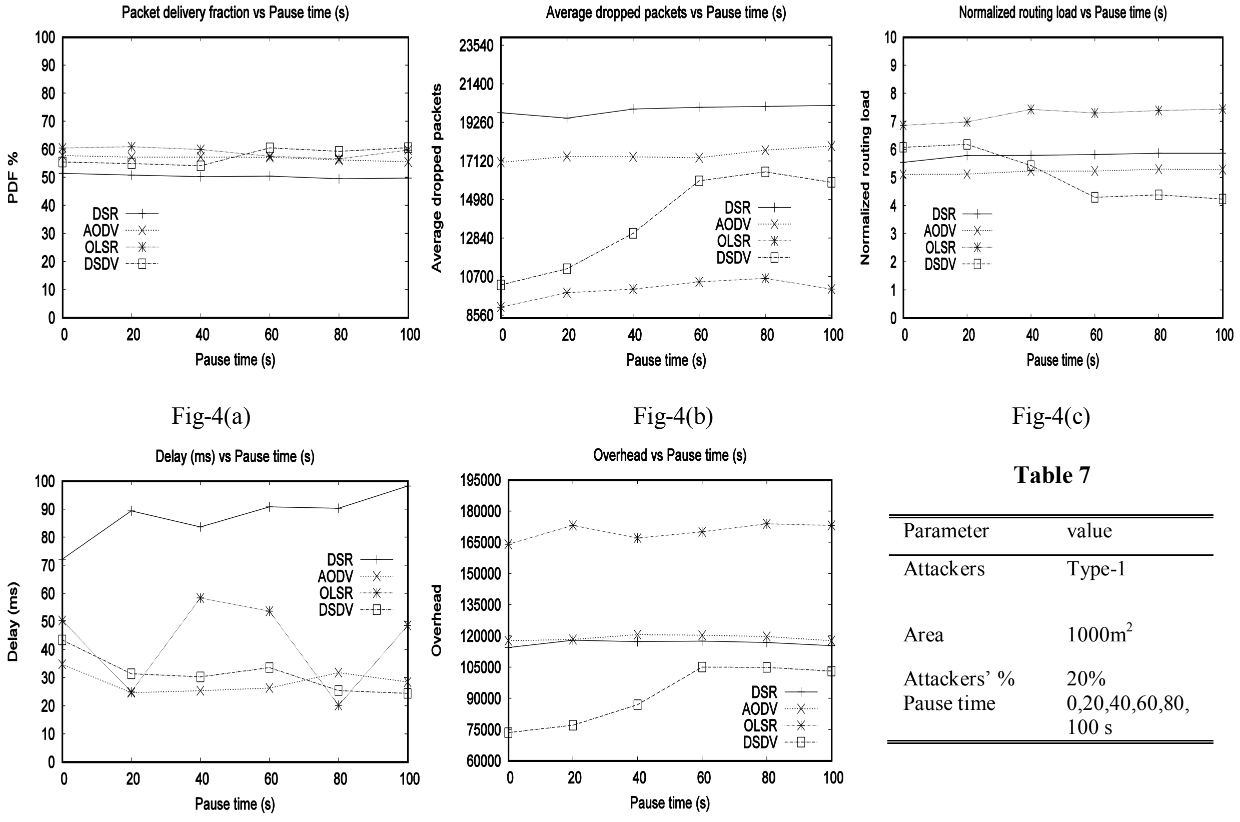


Fig-4(a) Fig-4(b) Fig-4(c)

Fig-4(d) Fig-4(e)

Table 7

Parameter	value
Attackers	Type-1
Area	1000m^2
Attackers' % Pause time	20% 0,20,40,60,80, 100 s

Fig. 4. a) PDF vs. Pause time, b) Average packet drop vs. Pause time, c) Normalized routing load vs. Pause time, d) Delay vs. Pause time, e) Overhead vs Pause time.

Moreover, as shown by **Fig. 6(d)**, the DSR protocol is comparatively more prone to delays than the other protocols when the drop rate rises. OLSR protocol is stable in the long run, i.e. when drop rate increases OLSR overhead decreases, this fact can be seen in **Fig. 6(e)**. Likewise, DSR and AODV also mimic the same behaviour in the long run, i.e. with low drop rate the produce more overhead as compared to their decreased overhead on high drop rates. In the overall picture, DSDV produces low overhead as compared to others.

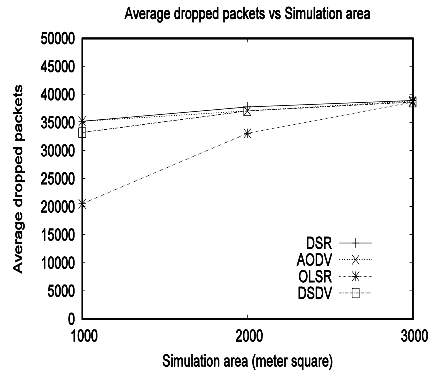


Fig-5(a)

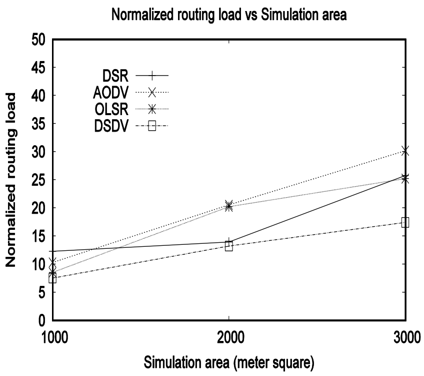


Fig-5(b)

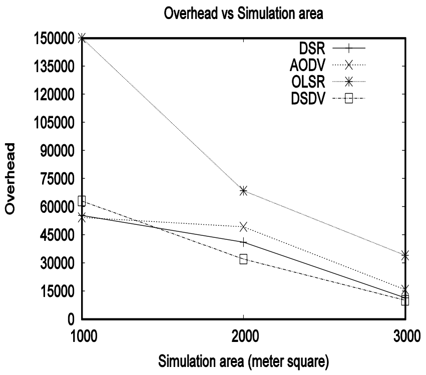
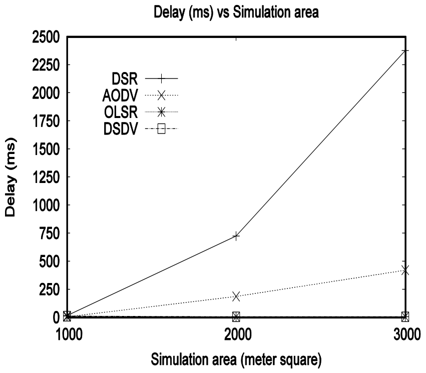


Fig-5(c)



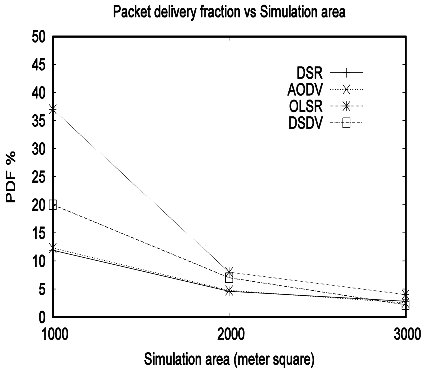


Table 8

Parameter	value
Attackers	Type-1
Area	1000,2000,3000m^2
Attackers' %	50%
Pause time	60 sec

Fig-5(d) Fig-5(e)

Fig. 5. a) Average packet drop vs. Area, b) Normalized routing load vs. Area, c) Overhead vs Area, d) Delay vs. Area, e) PDF vs. Area.

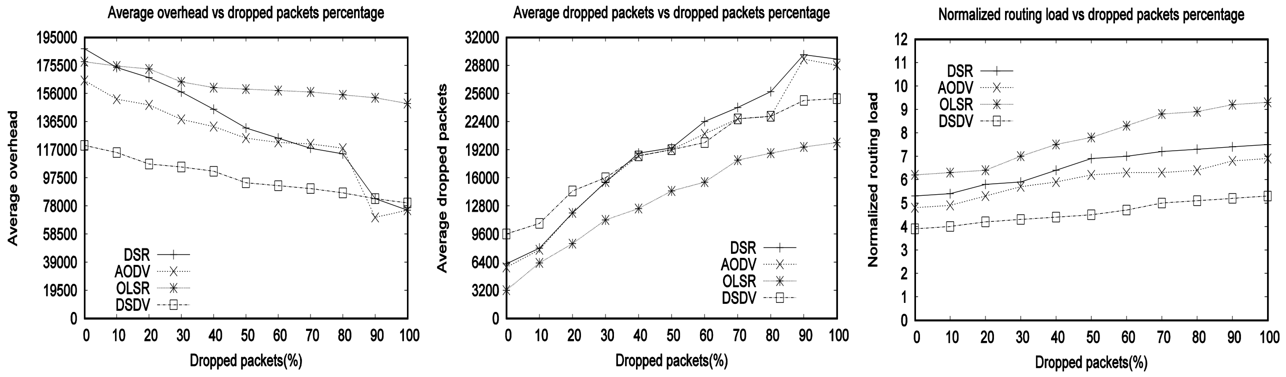


Fig-6(a) Fig-6(b) Fig-6(c)

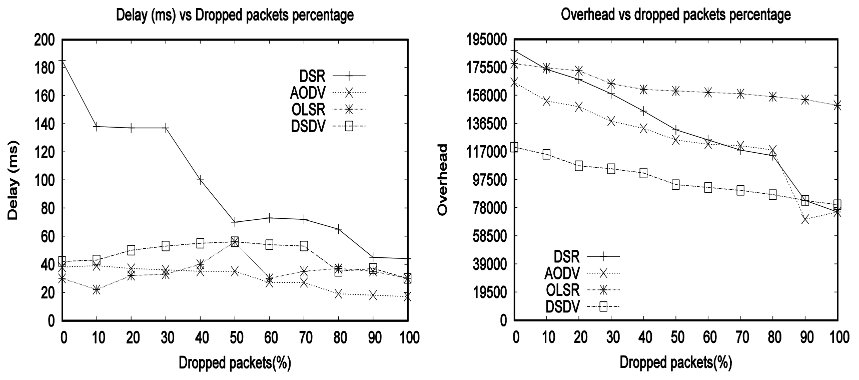


Fig-6(d)

Fig-6(e)

Fig. 6. a) PDF vs. Type-2, b) Average drop packets vs. Type-2,
c) Normalized routing load vs. Type-2, d) Delay vs. Type-2, e) Overhead vs. Type-2.

Table 9

Parameter	value
Attackers	Type-2
Area	1000 m^2
Attackers’ %	0 to 100%
Pause time	60 sec

6. Discussions

Reactive protocols tend to be less survivable. They act as on-demand service. The broken routes may cause service disruption owing to the time required for constructing new routes using fresh route discoveries. This creates a problem, i.e. the delay and overhead incurred in forming new routes towards destination(s). The proactive routing protocols, on the other hand, retain the network up and more survivable. One of the reasons is that each node maintains a table of routes to almost all destinations, at the cost of increased overhead. In case of active or passive DoS attacks, an alternate route is used without causing any delay.

Due to the passive DoS, the attacker drops all or fraction of packets creating service holes in the network. The traffic sources then try to discover alternate routes. However, there is no such mechanism exists in the routing protocols to exclude such nodes in the subsequent route discoveries. As a result, the source nodes uselessly try to reach their destinations with little or no success. This causes bandwidth and network resource wastage. Active DoS attacks are more serious because attackers can target specific victim nodes or even specific regions of the network to disconnect them from the operational part of the network. This is considered as more serious threat to survivability.

These attackers can use other mechanisms to completely cripple any operational network. For example, the attackers can form a group and launch these attacks in groups, called collusion. Similarly, they can strategically target important and sensitive locations of the networks, such as cluster head, base stations, data aggregators, etc. in order to disrupt the functionality or to analyse traffic to compromise privacy.

6.1 Suggested Improvements

***Reputation and trust-based solutions*:** in the literature, reputation and trust based schemes, such as [22, 23, 44], have been proposed for selfish node detection. One of the main concerns regarding using these solutions is the unnecessary incurred overhead, as pointed by [25]. If a lightweight version of these schemes is used properly, this will improve network survivability due to the fact that they isolate packet droppers. This can also help in isolating black hole attackers. Moreover, they encourage nodes to cooperate in order to gain good reputation and trust in the network.

***Adaptive route construction*:** in most of the routing protocols, when the route is broken due to nodes move-out-of-range situations because of mobility or due to DoS attacks, the source node is notified using a control message, such as Route Error (RERR). The source node then starts a fresh route discovery. This new route discovery will become unsuccessful if that route again includes the malicious node(s). To reduce the time required for (unsuccessful) route discoveries, each node should monitor its next hop for packet forwarding. After detecting packet drop threshold, the node preceding the attacker should construct the remaining path adaptively to the destination node thereby diverting the traffic and bypassing the attacker.

***Replicated resources*:** one of the key solutions for promoting survivability and fault tolerance is to increase resource replication. In some situations, it is quite possible to install emergency relay towers or to use existing network infrastructure, such as volunteers' communication devices, such as smart phones, laptops, etc., (ignoring security implications). This will maintain the overall network communication service. Similarly, routing protocols that construct, maintain, and use node-disjoint paths can also improve survivability. Example of those routing protocols is multipath routing protocols.

7. Conclusions

In this work, we evaluated survivability of multiple routing protocols in the presence of DoS attacks. We analysed performance of reactive and proactive protocols for various types of DoS attacks using multiple parameters. Through extensive simulations, it has been established that proactive routing protocols survive longer in the presence of the DoS attacks. One of the reasons for this behaviour is that in proactive routing protocols, each node has pre-established paths that can be used as alternate routes in case of route breakage. In our future work, we intend to propose a lightweight reputation-based mechanism with adaptive route construction strategy for the efficient route discovery and packet drop mitigation in the network.

References

[1] M. Mozaffari, W. Saad, M. Bennis, Y.-H. Nam, and M. Debbah, "A tutorial on UAVs for wireless networks: Applications, challenges, and open problems," *IEEE Communications Surveys and Tutorials*, vol. 21, no. 3, pp.2334-2360, 2019. Article (CrossRef Link)

[2] Y. Zhou, H. Yang, Y.-H. Hu, and S.-Y. Kung, "Cross-Layer Network Lifetime Maximization in Underwater Wireless Sensor Networks," *IEEE Systems Journal (Early Access)*, vol. 14, no. 1, pp. 220-231, 2020. Article (CrossRef Link)

[3] I. Yaqoob, I. A. T. Hashem, A. Ahmed, S. A. Kazmi, and C. S. Hong, "Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges," *Future Generation Computer Systems*, vol. 92, no. 1, pp. 265-275, 2019. Article (CrossRef Link)

[4] C. E. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers," in *Proc. of SIGCOMM '94: Proceedings of the conference on Communications architectures, protocols and applications*, pp. 234-244, 1994. Article (CrossRef Link)

[5] T. Clausen and P. Jacquet, "Optimized link state routing protocol (OLSR)," No. RFC 3626, 2003. Article (CrossRef Link)

[6] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc on-demand distance vector (AODV) routing," No. RFC 3561, 2003. Article (CrossRef Link)

[7] D. B. Johnson, D. A. Maltz, and J. Broch, "DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks," *Ad hoc networking*, vol. 5, pp. 139-172, 2001.

[8] N. O. Alsrehin, A. F. Klaib, and A. Magableh, "Intelligent Transportation and Control Systems Using Data Mining and Machine Learning Techniques: A Comprehensive Study," *IEEE Access*, vol. 7, no. 1, pp. 49830-49857, 2019. Article (CrossRef Link)

[9] M. Abu Talib, S. Abbas, Q. Nasir, and M. F. Mowakeh, "Systematic literature review on Internet-of-Vehicles communication security," *International Journal of Distributed Sensor Networks*, vol. 14, no. 12, p. 1550147718815054, 2018. Article (CrossRef Link)

[10] S. M. Bilal and S. Ali, "Review and performance analysis of position based routing in VANETs," *Wireless Personal Communications*, vol. 94, no. 3, pp. 559-578, 2017. Article (CrossRef Link)

[11] A. A. Mohammed, K. Xiangjie, L. Li, X. Feng, A. Saeid, S. Zohreh, and T. Amr, "BoDMaS: Bio-inspired Selfishness Detection and Mitigation in Data Management for Ad-hoc Social Networks," *Ad Hoc Networks*, vol. 55, pp. 119-131, 2017. Article (CrossRef Link)

[12] T. Liu, Q. Zhao, and L. Zhang, "Modified AODV routing protocol in underwater acoustic networks," in *Proc. of Electronic Information and Communication Technology (ICEICT), IEEE International Conference on*, pp. 191-194, 2016. Article (CrossRef Link)

[13] H. A. Khattak, M. A. Shah, S. Khan, I. Ali, and M. Imran, "Perception layer security in Internet of Things," *Future Generation Computer Systems*, vol. 100, pp. 144-164, 2019. Article (CrossRef Link)

[14] R. Kolandaisamy, R. Md Noor, I. Ahmedy, I. Ahmad, M. Reza Z'aba, M. Imran, and M. Alnuem, "A multivariant stream analysis approach to detect and mitigate DDoS attacks in vehicular ad hoc networks," *Wireless Communications Mobile Computing*, vol. 2018, 2018. Article (CrossRef Link)

[15] A. Derhab, A. Bouras, M. R. Senouci, and M. Imran, "Fortifying intrusion detection systems in dynamic Ad Hoc and wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 10, no. 12, p. 608162, 2014. Article (CrossRef Link)

[16] S. Abbas, M. Faisal, H. U. Rahman, M. Z. Khan, and M. Merabti, "Masquerading attacks detection in mobile ad hoc networks," *IEEE Access*, vol. 6, pp. 55013-55025, 2018. Article (CrossRef Link)

[17] A. R. Khan, A. N. Khan, S. Mustafa, and S. K. u. Zaman, "Impact of mobility on energy and performance of clustering-based power-controlled routing protocols," in *Proc. of 13th International Conference on Frontiers of Information Technology (FIT)*, pp. 252-257, 2015.

[18] M. U. Rahman, A. Alam, and S. Abbas, "Investigating the impacts of entity and group mobility models in MANETs," in *Proc. of International Conference on Computing, Electronic and Electrical Engineering (ICE Cube)*, pp. 181-185, 2016. Article (CrossRef Link)

[19] A. R. Khan, S. Ali, S. Mustafa, and M. Othman, "Impact of mobility models on clustering based routing protocols in mobile WSNs," in *Proc. of 10th International Conference on Frontiers of Information Technology*, pp. 366-370, 2012. Article (CrossRef Link)

[20] F. Khan, S. Abbas, and S. Khan, "An efficient and reliable core-assisted multicast routing protocol in mobile Ad-Hoc network," *International Journal of Advanced Computer Science Applications*, vol. 7, no. 5, pp. 231-242, 2016. Article (CrossRef Link)

[21] M. N. Lima, A. L. D. Santos, and G. Pujolle, "A survey of survivability in mobile ad hoc networks," *IEEE Communications Surveys & Tutorials*, vol. 11, no. 1, pp. 66-77, 2009. Article (CrossRef Link)

[22] S. Djahel, F. Nait-Abdesselam, and Z. L. Zhang, "Mitigating packet dropping problem in mobile ad hoc networks: Proposals and challenges," *IEEE Communications Surveys & Tutorials*, vol. 13, no. 4, pp. 658-672, 2011. Article (CrossRef Link)

[23] S. Abbas, M. Merabti, and D. Llewellyn-Jones, "A Survey of Reputation Based Schemes for MANET," in *Proc. of The 11th Annual Conference on The Convergence of Telecommunications, Networking & Broadcasting, Liverpool, UK*, pp. 21-22, 2010.

[24] C. Panos, C. Ntantogian, S. Malliaros, and C. Xenakis, "Analyzing, quantifying, and detecting the blackhole attack in infrastructure-less networks," *Computer Networks*, vol. 113, pp. 94-110, 2017. Article (CrossRef Link)

[25] S. Abbas, M. Merabti, and D. Llewellyn-Jones, "On the evaluation of reputation and trust based schemes in mobile ad hoc networks," *Security and Communication Networks*, vol. 8, no. 18, pp. 4041-4052, 2015. Article (CrossRef Link)

[26] J. Loo, J. L. Mauri, and J. s. H. Ortiz, *Mobile ad hoc networks: current status and future trends*. CRC Press, 2016.

[27] S. P. Khan and V. Gupta, "A Trusted Vector method for Black hole attack prevention on MANET," *International Journal of Computer Science and Management Research*, 2012.

[28] H. Singh, "To Investigate the Performance of MANET Routing Protocols with Varying Node Densities," *International Journal of Computer Science and Mobile Applications*, vol. 2, no. 10, pp. 01-11, 2014.

[29] A. Muneer, E. A. Fattah, and A. Odeh, "Performance Evaluation of DYMO, AODV and DSR Routing Protocols in MANET," *International Journal of Computer Applications*, vol. 49(11), pp. 29-33, 2012. Article (CrossRef Link)

[30] M. K. Mishra, B. K. Pattanayak, A. K. Jagadev, and M. Nayak, "Measure of Impact of Node Misbehavior in Ad Hoc Routing: A Comparative Approach," *International Journal of Computer Science Issues*, vol. 7, no. 4, 2010.

[31] Pavani,K. et al., "Performance Evaluation of Mobile Ad Hoc Network Routing Protocols under Black Hole Attack," in *Proc. of International Conference on Software Engineering and Mobile Application Modelling and Development (ICSEMA 2012)*, 2012. Article (CrossRef Link)

[32] E. F. Ahmed, R. A. Abouhogail, and A. Yahya, "Performance Evaluation of Blackhole Attack on VANET's Routing Protocols," *International Journal of Software Engineering & Its Applications*, vol. 8, no. 9, 2014.

[33] S. Gupta, B. Bhushan, C. Nagpal, and R. Chawla, "Impact of Malicious Nodes Concentration on MANET performance," *International Journal of Computer Science Applications & Information Technologies*, vol. 1, no. 1, 2013.

[34] R. E. Thorup, "Implementing and evaluating the DYMO routing protocol," *Aarhus Universitet, Datalogisk Institut*, 2007.

[35] E. Taqieddin, A. Miller, and S. Jagannathan, "Survivability and reliability analysis of the trusted link state routing protocol for wireless AD HOC networks," *International Journal of Wireless & Mobile Networks (IJWMN)*, vol. 3, no. 2, pp. 77-89, 2011. Article (CrossRef Link)

[36] B. Awerbuch, R. Curtmola, D. Holmer, H. Rubens, and C. Nita-Rotaru, "On the survivability of routing protocols in ad hoc wireless networks," in *Proc. of First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SecureComm)*, pp. 327-338, 2005. Article (CrossRef Link)

[37] T. Qiu, N. Chen, K. Li, M. Atiquzzaman, and W. Zhao, "How can heterogeneous internet of things build our future: A survey," *IEEE Communications Surveys & Tutorials*, vol.20, no.3, pp.2011-2027, 2018. Article (CrossRef Link)

[38] S. Xu, Y. Li, Y. Gao, Y. Liu, and H. Gacanin, "Opportunistic coexistence of LTE and WiFi for future 5G system: experimental performance evaluation and analysis," *IEEE Access*, vol. 6, pp. 8725-8741, 2017. Article (CrossRef Link)

[39] Usha and Bose, "Comparing The Impact of Blackhole and Grayhole Attacks in Mobile Adhoc Networks," *Journal of Computer Science*, vol. 8, no. 11, pp. 1788-1802, 2012. Article (CrossRef Link)

[40] P. Michiardi and R. Molva., "Simulation-based analysis of security exposures in mobile ad hoc networks," in *Proc. of European Wireless Conference*, pp. 15-17, 2002.

[41] F. Xing and W. Wang, "On the survivability of wireless ad hoc networks with node misbehaviors and failures," *IEEE Transactions on Dependable and Secure Computing*, vol. 7, no. 3, pp. 284-299, 2010. Article (CrossRef Link)

[42] O. Younes and N. Thomas, "Analysis of the expected number of hops in mobile ad hoc networks with random waypoint mobility," *Electronic Notes in Theoretical Computer Science*, vol. 275, pp. 143-158, 2011. Article (CrossRef Link)

[43] X.-Y. Li, P.-J. Wan, Y. Wang, and C.-W. Yi, "Fault tolerant deployment and topology control in wireless ad hoc networks," *Wireless Communications and Mobile Computing*, vol. 4, no. 1, pp. 109-125, 2004. Article (CrossRef Link)

[44] S. Abbas, M. Merabti, K. Kifayat, and T. Baker, "Thwarting Sybil Attackers in Reputation-based Scheme in Mobile Ad hoc Networks," *KSII Transactions on Internet Information Systems*, vol. 13, no. 12, 2019. Article (CrossRef Link)

Sohail Abbas received PhD degree in wireless network security from Liverpool John Moores University, UK in 2011. Currently, he is working as an Assistant Professor in the Department of Computer Science, College of Computing and Informatics, University of Sharjah, UAE. He has been involved in academia and research for more than 14 years. His research interests include security issues, such as intrusion detection, identity-based attacks, and trust in wireless networks, such as mobile ad hoc networks, wireless sensor networks, and the Internet of Things. Dr. Sohail is a member of various technical program committees, including IEEE CCNC, IEEE VTC, IEEE ISCI, IEEE ISWTA, etc. He has been Track Co-chair of 16th ACS/IEEE International Conference AICCSA 2019. He is also serving various prestigious journals as a reviewer, such as Security and Communication Networks, IET Wireless Sensor Systems, Mobile Networks and Applications, International Journal of Electronics and Communications, International Journal of Distributed Sensor Networks.

Muhammad Haqdad is PhD scholar at University of Malakand, KPK, Pakistan. His research interests include security in the Internet of Things and Wireless Networks.

Muhammad Zahid Khan is an Assistant Professor in the Department of Computer and Information Technology at University of Malakand, Pakistan since 2005. He received his BCS (Hons) degree in Computer Science from University of Peshawar, Pakistan in 2003. He received a Ph.D degree from the School of Computing and Mathematical Sciences, Liverpool John Moores University, United Kingdom in 2013. His current research interests are in Wireless Sensor Networks, Mobile Ad-hoc Networks, and the Internet of Things (IoT). He is currently leading a Network Systems & Security Research Group (NSSRG) at the Department of CS & IT, University of Malakand. He is a Higher Education Commission's (HEC) Pakistan approved supervisor.

Haseeb Ur Rahman is working as an Assistant Professor at the Department of Computer Science & IT, University of Malakand, Pakistan. He has received his PhD degree from Liverpool John Moores University, UK in 2013 in P2P networks. Haseeb is also a TPC member of various conferences such as IEEE CCNC etc. His research interests include P2P and Social P2P networks, MANETs, Cloud computing, Sensor networks and IoT. Currently, he is actively involved in research in IoT Smart Farming and Internet of Cultural things.

Ajab Khan is currently working as Director ORIC at Abbottabad University of Science and Technology, KPK, Pakistan. He has received his PhD from University of Leicester, UK. Previously he has been working as Assistant Professor at University of Malakand, Pakistan. Ajab khan research mainly focuses on wireless sensor networks, network security and modelling biological systems.

Dr. Atta ur Rehman Khan is an Associate Professor at College of Engineering and Information Technology, Ajman University, UAE. In the past, he has served as a Postgraduate Program Coordinator at Sohar University, Director of National Cybercrime Forensics Lab Pakistan, and Head of Air University Cybersecurity Center. Currently, he is serving as an Associate Editor of IEEE Access, Elsevier Journal of Network and Computer Applications, Associate Technical Editor of IEEE Communications Magazine, Editor of Springer Journal of Cluster Computing, Oxford Computer Journal, IEEE SDN Newsletter, KSII Transactions on Internet and Information Systems, SpringerOpen Human-centric Computing and Information Sciences, SpringerPlus, and Ad hoc & Sensor Wireless Networks journal. Moreover, he is a Senior Member of IEEE and Steering Committee Member/ Track Chair/ Technical Program Committee (TPC) member of over 70 international conferences. He also serves as a domain expert for multiple international research funding bodies, and has received multiple awards, fellowships, and research grants. His areas of research interest include cybersecurity, mobile cloud computing, ad hoc networks, and IoT. For more updated information, visit his website at www.attaurrehman.com.