Securing Against DoS/DDoS Attacks in Internet of Flying Things using Experience-based Deep Learning Algorithm

Inam Ullah Khan
Isra University
Arsin Abdollahi
University of Kurdistan
Muhammad Asghar Khan
Hamdard University
Irfan Uddin (✉ mirfanud@gmail.com)
Kohat University of Science and Technology https://orcid.org/0000-0002-1355-3881
Insaf Ullah
Hamdard University

Research Article

Keywords: IoFT, Security Attacks, QoS, DoS, Routing Protocols

Posted Date: March 4th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-271920/v1

Securing Against DoS/DDoS Attacks in Internet of Flying Things using Experience-based Deep Learning Algorithm

Inam Ullah Khan[1], Asrin Abdollahi[2], Muhammad Asghar Khan[3], M. Irfan Uddin[4, *], Insaf Ullah[3]

[1]ISRA University, Islamabad 44000, Pakistan. (inamullahkhan05@gmail.com)
[2]University of Kurdistan, Sanandaj, Iran (a.abdollahi@eng.uok.ac.ir)
[3]Hamdard Institute of Engineering & Technology, Islamabad 44000, Pakistan. {(khayyam2302@gmail.com, insafktk @gmail.com)}
[4]Institute of Computing, Kohat University of Science and Technology, Kohat, Pakistan. (irfanuddin@kust.edu.pk)

Abstract

Due to the limited computational resources of small unmanned aerial vehicles (UAVs), the Internet of flying things (IoFT) is vulnerable to cybersecurity attacks, particularly Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. In addition, the transfer of reliable information from source UAV to destination UAV is another big challenge in IoFT networks. Therefore, this article aims to address the security deficiency by proposing an experience-based deep learning algorithm to cater to the DoS, D-DoS and a special kind of threat covering ping-of-death attacks. The proposed scheme uses the notion of the intrusion detection system (IDS). In addition, for reliable communication, a nature-based control routing algorithm AntHocNet is investigated with other contemporary protocols. The proposed approach is implemented in a smart city environment as a case study. The result authenticates the superiority of the proposed schemes in terms of security and QoS requirement from its counterparts.

Keywords: IoFT, Security Attacks, QoS, DoS, Routing Protocols

1. Introduction

Unmanned Aerial Vehicles (UAVs), also known as drones are the aerial devices, which are self-programmed and remotely operated via mobile devices and are connected through certain wireless communication technologies. Their applicability is increasing in a wide range of applications, ranging from civilian, military, logistics, remote monitoring, cinematography, agricultural monitoring, search and rescue, and 3D mapping, due to their ease of deployment, dynamic configuration, low maintenance costs, high mobility and faster response [1]. Connecting UAVs in a group via internet called a new clan of networks called Internet of Flying Things (IoFT). Since UAVs are usually deployed in tough environments and terrain, it is therefore very important to provide a reliable and secure network. In such environments, the intruders may try to attack on the IoFT and can hijack the UAV or also the entire fleet of UAVs. These attacks include denial-off-service (DoS), distributed-denial-of-service (DDoS), spoofing, Sybil. Moreover, UAVs can also be triggered with the false data attack in the surrounding environment which causes very serious destruction [2].

Working on attacks such as ping or DoS, a model scenario is used to detect these attacks, called the intrusion detection method (IDS). For the data-packet length poison probability function, the suggested system for the detection of ping death attacks is used [2]. The cyber-attacks such DoS, DDoS, domain name system, man in the middle, or also some virus-based attacks are discussed in the research study [3]. Detecting any security-attack comes in the category of cybercrime, which can be find-out or traced by using different techniques like hidden-markov model or also some machine learning strategies, which include naïve bayes, k-nearest neighbor, as well as cyber-bullying detection [4-7]. Due to the dynamic behavior of IoFT, working on the security attacks, vulnerabilities between intruder and custodian must be properly explored. The tree-base strategy can easily portray the moves of intruders/attackers, which worked on three basic parameters like occurrence, detection, and severity [8]. This security strategy may give an optimal result in multi-layer approach to defend the IoFT from different attacks [9-12].

Network infrastructure is currently very much extended due to the new trend of flying vehicles as data is disseminated from the UAVs to the base station, therefore data safety and privacy are required to safeguard data from intruders. In addition to the security vulnerabilities, the UAV communication network can also be more reliable and has low delay, and fault tolerance. It is therefore important to establish and select appropriate routing protocols for IoFT in order to make the services and applications more persistent and active in smart city environment. Network performance is an important parameter in terms of throughput and response time, and is dependent on the strength of the algorithm operating within the routing protocol. However, routing is the most challenging job in IoFT due to the unique attributes of UAVs such as high mobility, 3D movement, and rapid topology changes. Figure.1 explains the concept of secure smart cities using protocols in the IoFT. While the main contributions of this study include some important points, which are given below.

- Firstly, an experience-based algorithm is proposed to counter security attacks such as Denial-of-Service (DOS), D-DOS and Ping of death attack in Internet of fling things (IoFT).
- Secondly, a nature-based control routing algorithm AntHocNet is introduced and is investigated with other contemporary routing protocols to improve transmission links performance in futuristic cities.
- Thirdly, state-of-the-art mobility model is utilized in the learning process of IoFT.
- Finally, the simulation results in terms of QoS and security is obtained to test the performance of the proposed schemes.

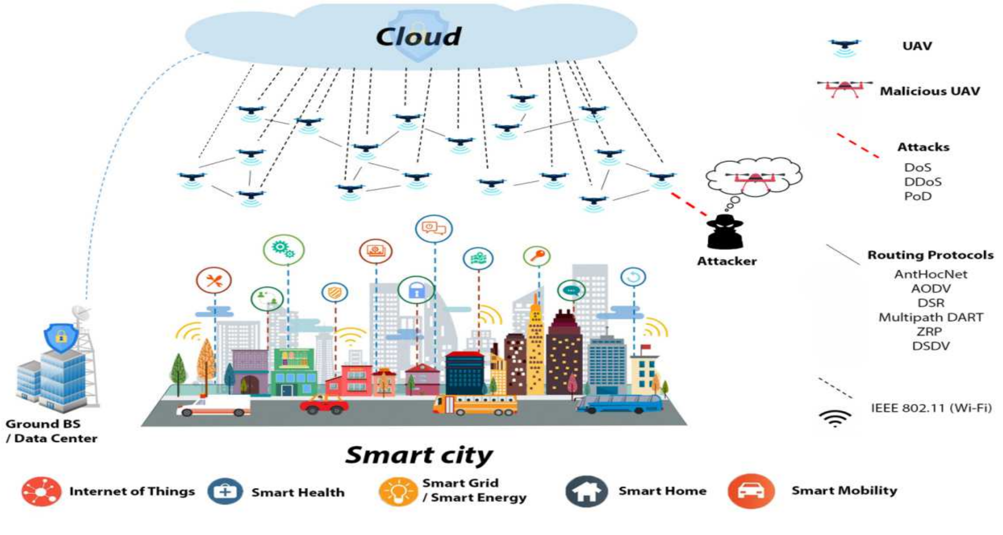


Figure.1 A sample architecture of Internet of Flying Things for smart cities applications.

2. Literature Survey:

To secure the communication in future smart cities, encryption, intrusion detection systems can be used in safeguarding aerial networks from DOS or DDOS attack [13]. In [14], machine learning algorithms are utilized as well as taxonomy-ladder of IoT-based-security systems, which include identification, wireless networking, data collection is briefly studied. In [15], DoS attacks for UAVs are proposed through GPS tracking investigation of data using log files [15]. Wireless vision (Wi-Vi) sensors are put in service for self-controlled flying vehicles, which can be used to rescue or detection of intruders even if there is very thick wall of security [16]. The detection of Sybil attack using mobile nodes is the most difficult task to tackle, received signal strength is the only method to recognize the accurate location also to identify the attack. In [17], the authors suggested that the channel state information can give accurate data about location-coordinates as well as the self-adaptive multiple signal classification set of rules is utilized for passive attack identification. In [18], flying things-based architecture is initiated, which give a solution mechanism for security and privacy to secure aerial-vehicle-to-aerial-drone communication using routing protocols. To secure the link between base station and aerial-vehicle, advanced encryption standard is acquired from electro-encephalogram signals [19]. Zigbee is used as a communication protocol standard also two Xbee modules are utilized in the implementation which easily do on board encryption. Due to this experimentation aerial vehicles can be secured from third-party-attack also this is a very unique way to provide safe communication links. In [20], the authors proposed a practical demonstration of third party-attack by real aerial-robot easily inspects the vulnerabilities of flying-network using three-Denial-off-service tool, which influence IoD. Also, in future this simulation is suggested to be utilized for DDoS. In [21], the flying vehicles and VPN-Sniffing using WIFI-Pineapple are exemplified [21]. Heuristic computational drones-based projects must be having pragmatic results in civil and military fields but keeping in view the issue of collision dodging in aerial vehicles must have been given proper solution to this problem [22]. Furthermore, the classification of DoS/D-DoS security threats are shown in figure.2.

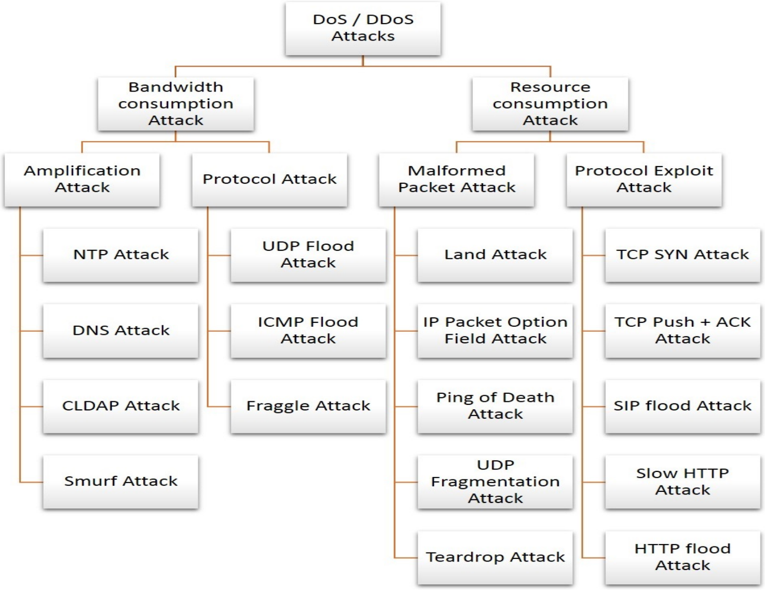


Figure.2 Classification of DoS/D-DoS Security Threats

3. Communication Protocols for IoFT

As we see the quick swift in the pattern of flying things that requires high accuracy of UAV's localization. For this purpose, position-based routing schemes must be incorporated in aerial networks. The scrutiny in the UAV-network design issues comprises physical structure of aerial network, mobility patterns, jitter, link dis-connectivity, collision, flying network architecture and scalability must be addressed [23]. Intelligent autonomous aerial vehicles employ network design which will be either central station or either decentralized whichever encompass single and multi-group swarm ad hoc network. In addition, the end-to-end communication of data needs a reliable protocol to overcome on the instability of flying networks and variation in quality of experience. The area of flying things is still evolving, so in the emergence of UAV-networks base-line routing techniques was used. Later on, researchers found that in drone-assisted-flying-networks rapid mobility pattern changes due to those existing routing schemes must be improved [24]. Further the classifications of routing protocols in aerial vehicles are as under. The hierarchy of routing protocols for internet of flying things is presented in figure.4.

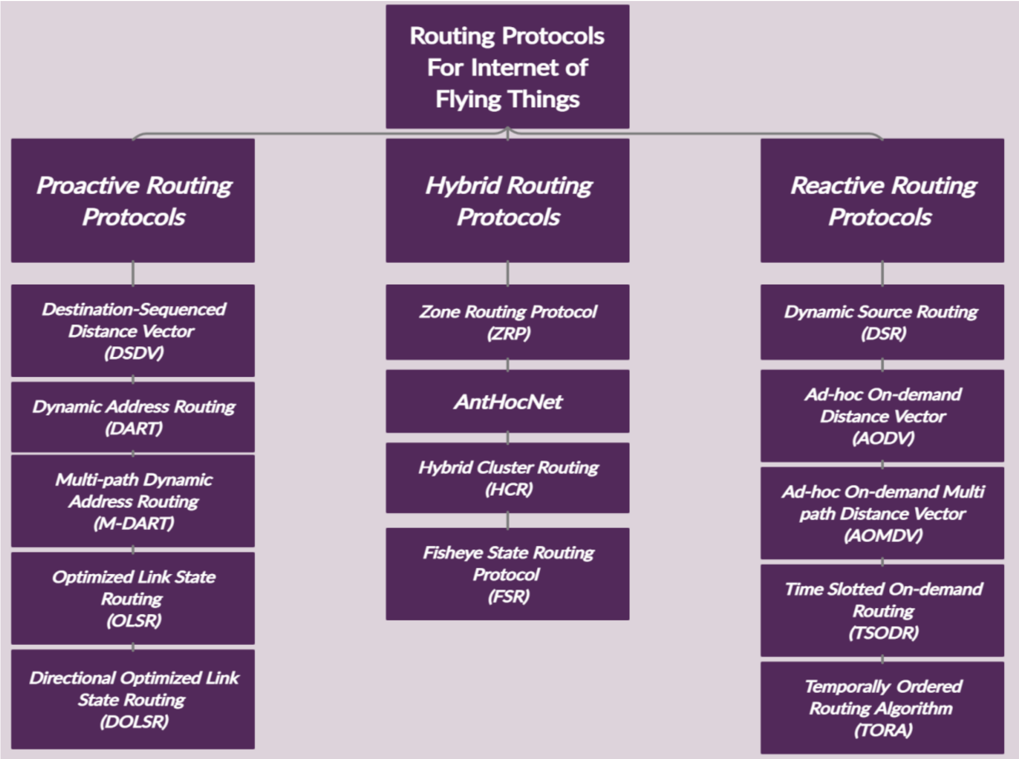

Routing Protocols For Internet of Flying Things
Proactive Routing Protocols
Hybrid Routing Protocols
Reactive Routing Protocols
Destination-Sequenced Distance Vector (DSDV)
Dynamic Address Routing (DART)
Multi-path Dynamic Address Routing (M-DART)
Optimized Link State Routing (OLSR)
Directional Optimized Link State Routing (DOLSR)
Zone Routing Protocol (ZRP)
AntHocNet
Hybrid Cluster Routing (HCR)
Fisheye State Routing Protocol (FSR)
Dynamic Source Routing (DSR)
Ad-hoc On-demand Distance Vector (AODV)
Ad-hoc On-demand Multi path Distance Vector (AOMDV)
Time Slotted On-demand Routing (TSODR)
Temporally Ordered Routing Algorithm (TORA)

Figure.4 Hierarchy of Routing Protocols for Internet of Flying Things

a. Flying-AntHocNet:

The idea of ad-hoc-wireless-multi-hop-networks combines together to make an efficient way of path planning to overcome on different issues faced by routing mechanisms. For searching and maintaining the path-setup process integrate to form anthocnet, which have reactive and proactive nature of behavior. For the first time ant-based algorithm was introduced for wired communication to find the optimal path which was known as ant-based-control. In addition, two newborn strategies include AntNet-FA boost-up the efficiency practices of forward-ants and for the backward behavior estimates the full tour of flying-ant-things from source to destination. Flying-AntHocNet is introduced which works on the similar principles of ant-colony-optimization, which attempt to restore connection failure in drone-assisted-networks [25].

b. UAV-based-AODV:

Flying vehicles make a self-organized internetworking, which settle up the communication link between aerial workstation and the mobile natured framework systems. Due to the changing pattern of topology in flying-UAV, the connection loss occurs sometimes which can be easily fixed using protocol like ad-hoc-on-demand. In addition, for making the links more robust and to increase the life span of a network, novel protocol called energy-improved-AODV, which stabilizes the communication links easily [26].

c. D-S-D-V Routing Mechanism:

Maintaining every route information in the aerial networks is a tough task for this purpose proactive routing method is introduced which regularly update network structural changes and save it in routing table of every node. However, preserve the nearby node bordering data packets in the workstation, this whole process is concluded just because of destination-sequenced distance-vector approach [27].

d. Dynamic Source Routing:

DSR is designed for multi-hop wireless communication networks and exercise reactiveness in nature where a data packet is flooded from source aerial vehicle to target. However, +this routing protocol overcomes on congestion avoidance, link-failure which may lead to disruption in Internet of flying things networks [28].

e. Multi-Path-Dynamic-Address-Routing:

Dynamic address routing is the foundation protocol which is further improved in the form of multi-path-DART, also this algorithm proclaims proactive behavior which maintains the routing tables data packets for the entire aerial network. M-DART implements multi-path strategy utilizing sibling-id, next-hop information, path-cost, network-id and path-log data is extended in the whole mechanism [29].

f. Zone-Routing-Protocol:

Hybrid categorization of routing protocols contains both proactive and reactive attributes in the communication standards. Zone routing technique divides the entire network topology in clusters or zones which reduce aerial data packet overhead issue. The cluster-head (C-H) finds out the geographical location of the flying vehicles which show cognitive-learning from the adaptive environment. Open system interconnection model with the detail architectural design of Z-R-P routing protocol is shown in figure.5 to represent the concept of cluster-based routing algorithm.

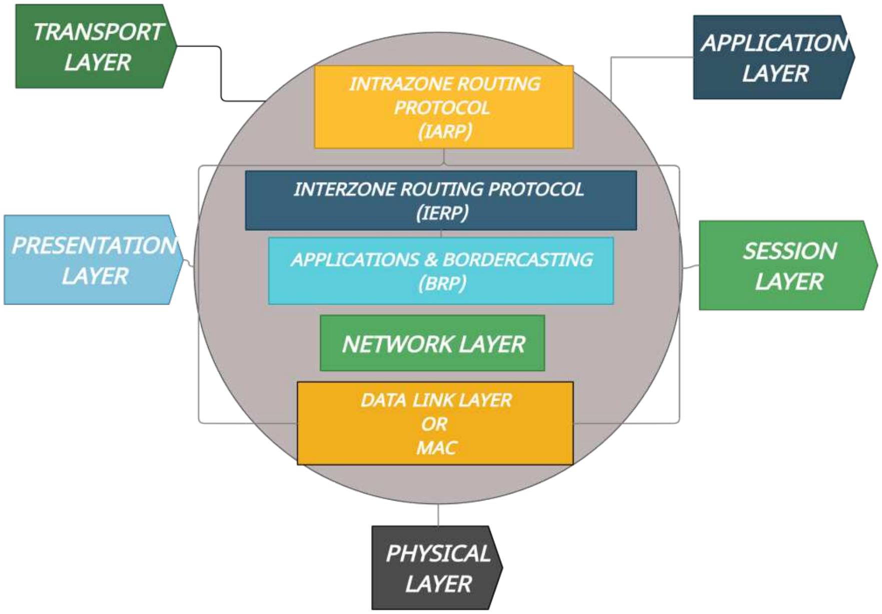
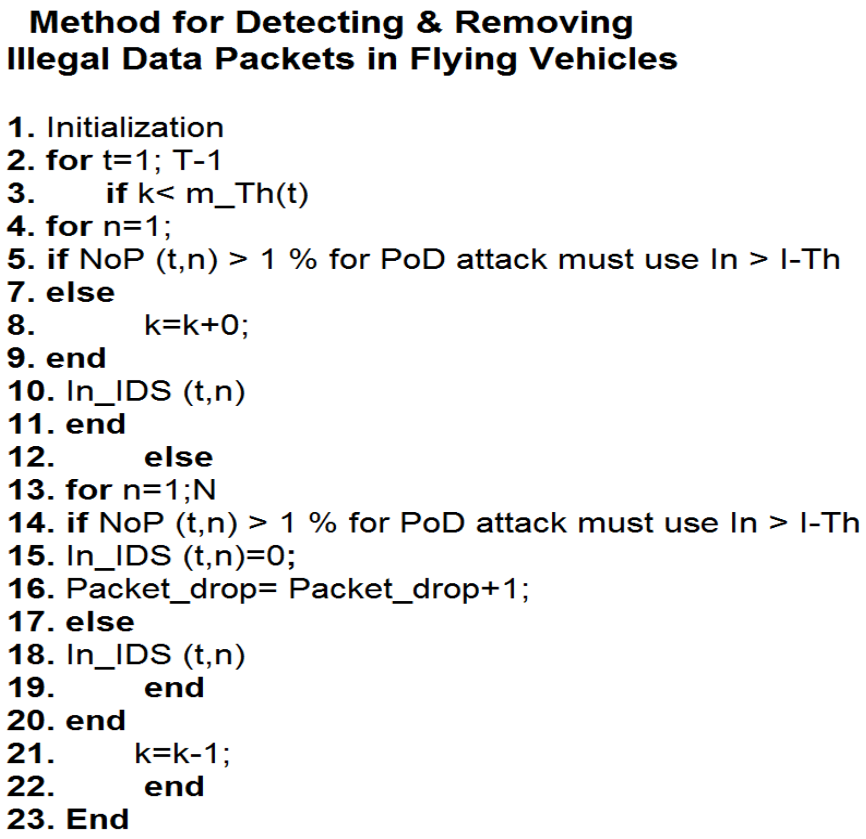


Figure.5 OSI Model with Detailed Architectural Design of ZRP

4. Internet of Flying Things Attack Detection

Ensuring the safety of internet-of-drones the unpredicted data packets in the base-station due to that flying things detection system is introduced. The main focus of flying-things-D-S can easily recognize unauthorized packets to maintain the queue of ground station gateway. Some cyber-security attacks like Ping-of-Death, denial-of-service and distributed-denial-of-service are investigated in the simulation environment. In addition, this system is having the optimal capability to monitor queues also if the data packet is received which can be filtered by this novel detection system to distinguish the abnormal information packets through which decision making will be made possible. Basically, in this research study analysis two algorithms are proposed to secure smart cities. Sampling the data packets in the aerial networks unwanted information must be wiped out, therefore stretching the knowledge more every packet in the stream must have a number through which a threshold will be regulated. Abdollahi et al [2] extend the concept of internet of things detection threshold which give a detailed overview on gateway analysis of security attacks. While keeping an eye on the information like when the ground station is receiving data packets undesired statistical details will be certainly detected at every time slot utilizing figure. 6 algorithms for unwanted detection and removal of information are proposed. In addition, malicious data packets pass through IDS, where hostile information reach at some specific threshold through which proposed sequence delete the misguided data.



Method for Detecting & Removing Illegal Data Packets in Flying Vehicles

```
Initialization
for t=1; T-1
      if k< m_Th(t)
for n=1;
if NoP (t,n) > 1 % for PoD attack must use In > I-Th
else
          k=k+0;
end
In_IDS (t,n)
end
          else
for n=1;N
if NoP (t,n) > 1 % for PoD attack must use In > I-Th
In_IDS (t,n)=0;
Packet_drop= Packet_drop+1;
else
In_IDS (t,n)
          end
end
         k=k-1;
          end
End
```

Figure.6 Algorithm for Detecting & Removing illegal data packets

5. Simulation Environment

The detailed pilot study is conducted using MATLAB for the cyber-security attacks while for experimentation of routing protocols network simulator-2 is employed for making the whole aerial network schema.

6. Network-Topology for IoFT

The network physical structure consists of thirty drones (N=30) and one ground station. The main postulation using internet-of-flying-things will consider time slot for selected UAV’s to send information to land station also every aerial vehicle has the capacity to send data packets per seconds. Two major scenarios are mentioned either “no attack” or “with attack”. Assuming that our internetwork is secure and there is no intruder workstation inside the system. For this purpose, aerial vehicles send legal data packets having average length which is cite as λ_l. Apart from that aerial network modeling can be concluded for generating information of arrival data net which lined-up in the entry to pinpoint land station. Figure.7 shows the physical structure of IDS in land-station where malicious data packets can be removed esily.

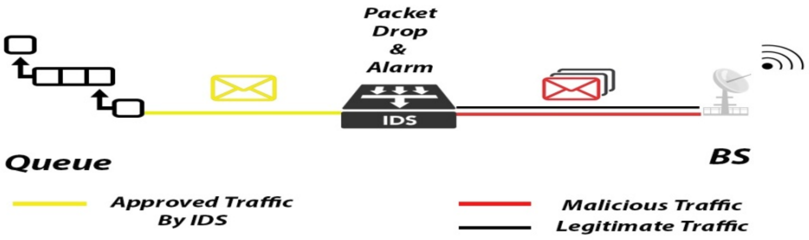


Figure.7 Physical Structure of IDS in land-Station

$$Q(t+1) = \left(Q(t)+\lambda(t)-\mu(t)\right) + \qquad \text{Eq (1)}$$

Q(t) :Queue length

(t) : Arrival time

$\mu(t)$: Out Rate

The above metric values can be either constant or random, so furthermore the randomness can be generated using Poisson distribution. The four probabilistic options are practically demonstrated in the figure.8 as mentioned.

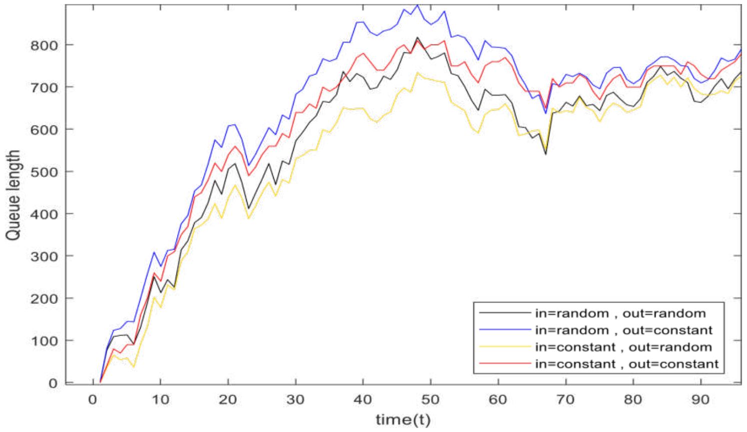


Figure.8 Probabilistic experimentation for generating queue

For t=100 sec, the Poisson random variable with queued length is followed in the below graph.

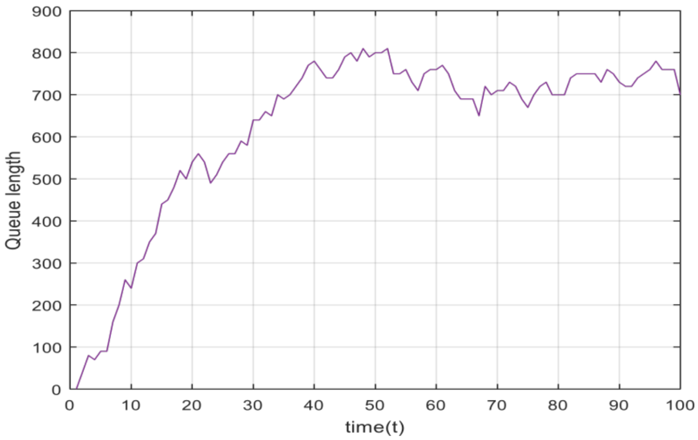


Figure.9 Queue length over time duration without attack

If the number of flying things is increased, so we will see high rise in the length of data packets. However out rate is symbolized by μ through which changes can be done easily in queue length and the entry point is sustained. In the figure. 9. queue length over time duration without attack means when UAV's are safe and packets arrived length in drone-based network show escalation from normal level. Also, sometimes there we find no unauthorized node in the network to attack due to that column of entry point will shoot-up to next level which will exceed reduction in resources. This issue even arises in our network arrangement so for solving this concern the following mechanism is given as.

$$\mu = \frac{N\lambda_l}{2} \qquad \text{Eq (2)}$$

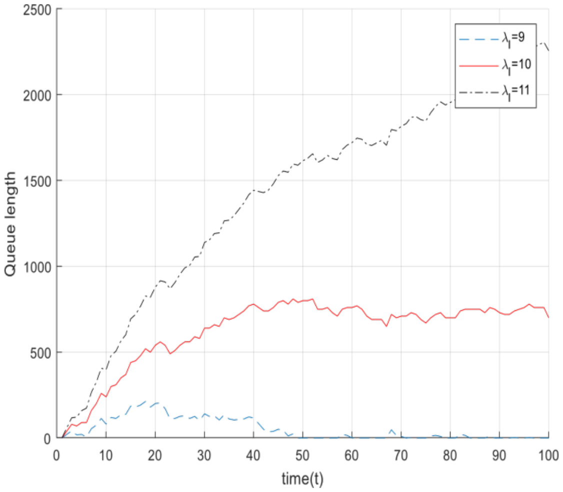


Figure.10 Independent Input rate of queue

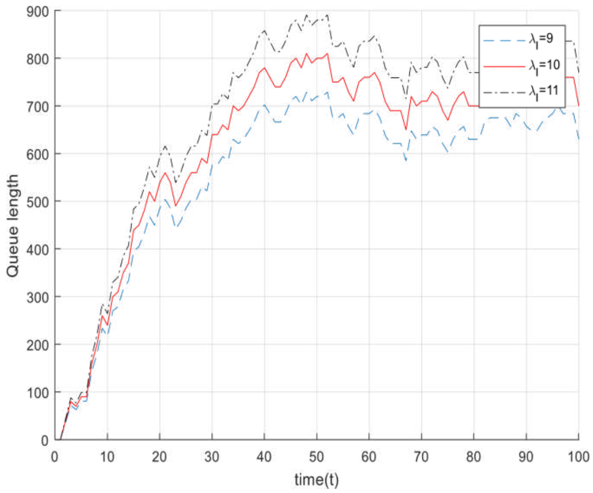


Figure.11 Queue depending on input rate

Considering if the intruder intervenes only broadcasting method is utilized to flood the data packets and make it unavailable to the target node. Normally in DoS and D-DoS cyber security attack try to spoof one or more workstations to give rise to data packets from normal legal length. Ping-of-Death is a type of DoS attack but the differentiation as compared to other customary attack will strike on one UAV which make an effort to modify data lengths with its “pa” probability attack.

7. Markov Chain Distribution

Markov chain is a fundamental part of Markov process in the stochastic processes that use memory distribution in discrete-time steps that recalls discrete-time Markov chain (DTMC). Suppose X={X_t: t=0,1,2,…,T} be the state of Markov chain stochastic process at time ‘t’ with finite state spaces S={1,2} where ‘1’ represent ‘no attack level’ which means normal and ‘2’ stands for the attack level as shown below:

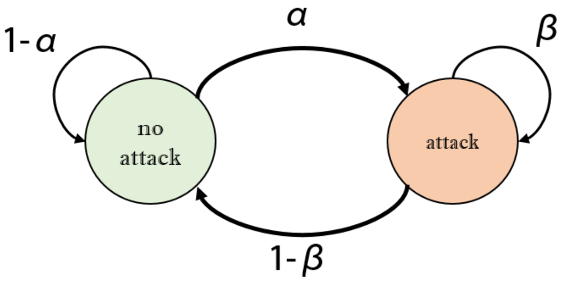


Figure.12 Two-state Markove Process

$$\mathbb{P}(X_t = s_t | X_{t-1} = s_{t-1}. \dots . X_0 = s_0) = \mathbb{P}(X_t = s_t | X_{t-1} = s_{t-1}) \qquad \text{Eq (3)}$$

The above equation (3) shows the formulation of markov chain where for distribution ‘ X_t ‘ having dependency on X_{t-1} . Finding the probability of being in state ‘1’ or ‘2’ at time ‘t’, we need to simulate our security attacks. In Denial-off-Service the attacker injects illegal packets to the network security systems by spoofing one node and attempts to increase numbers of packets by utilizing the ratio $1 + \gamma.p_a$. Apart from that modeling probability ‘ p_a ‘ is being changed in the first scenario where Markov chain with following transition matrix where α and β respectively are ${p_a}_0$ and 1 is proposed in the matrix.

$$(P)_{ij} = (p_{ij}) = \begin{bmatrix} {p_a}_0 & 1 - {p_a}_0 \\ 0 & 1 \end{bmatrix} \qquad \text{Eq (4)}$$

Attack probability of being in state ‘2’ at time ‘t’ is proofed mathematically as

$$\mathbb{P}(X_t = j) = \mathbb{P}(X_t = j. \dots . X_0 = i) \qquad \text{Eq (5)}$$

$$= \textstyle\sum_{k.i\in s} \mathbb{P}(X_t = j | X_{t-1} = k \,.\, X_{t-1} = k. \dots . X_0 = s_1) \times \mathbb{P}(X_{t-1} = k)$$

$$= \textstyle\sum_{k.h.i\in s} \mathbb{P}(X_t = j | X_{t-1} = k) \times \mathbb{P}(X_{t-1} = k | X_{t-2} = h. \dots . X_0 = s_1) \times \mathbb{P}(X_{t-2} = h)$$

$$= \textstyle\sum_{k.h.g.i\in s} \mathbb{P}(X_t = j | X_{t-1} = k) \times \mathbb{P}(X_{t-1} = k | X_{t-2} = h) \times \dots \times \mathbb{P}(X_1 = g | X_0 = i) \times \mathbb{P}(X_0 = i)$$

$$= \textstyle\sum_{i.g.h.k\in s} (\pi_0)_i \times p_{ig} \times \dots \times p_{hk} \times p_{kj}$$

$$= \textstyle\sum_{i\in s} (\pi_0)_i \times (P^t)_{ij}$$

$$= (\boldsymbol{\pi_0}^{\boldsymbol{T}} \boldsymbol{P^t})_{j=2}$$

Whereas,

$$(\pi_0)_i = \mathbb{P}(X_0 = i) = \mathbb{P}(attacker\ choose\ state\ i\ to\ start) = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad \text{Eq (6)}$$

While s_1 , s_2, i and j. However, the attack probability p_a at each time slot will change in sequence using random variables according to DTMC in blocks.

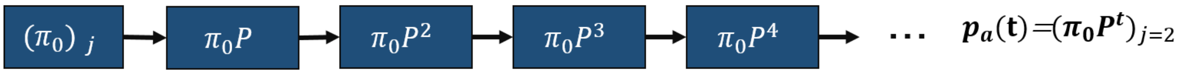

$(\pi_0)\ _j$
$\pi_0 P$
$\pi_0 P^2$
$\pi_0 P^3$
$\pi_0 P^4$
...
$\boldsymbol{p_a}(\mathbf{t}) = (\boldsymbol{\pi_0 P^t})_{j=2}$

Figure.13 Attack Probability at each time slot for desired markov chain

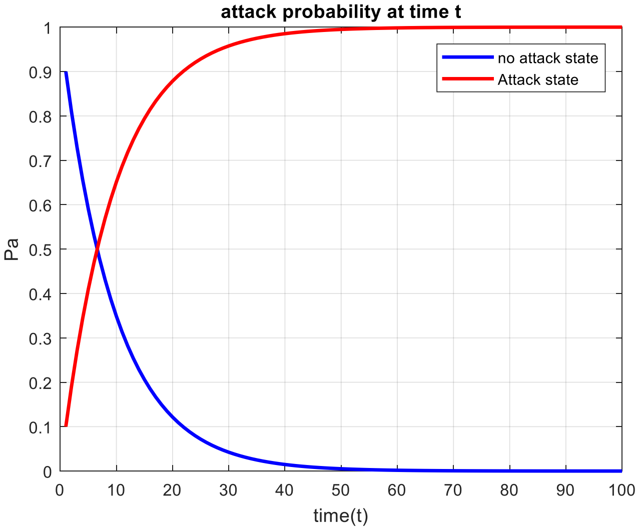


Figure.14 Attack randomness of Markov chain states at time t

Therefore, for enhancing the technique markov binomial distribution where assumption is based on the parameters like α=β=p_{a_0} and X is stationary. Inaddition binomial arrangement is designed for cyber attacks. The transition matrix is equal to:

$$(P)_{ij} = (p_{ij}) = \begin{bmatrix} 1 - p_{a_0} & p_{a_0} \\ 1 - p_{a_0} & p_{a_0} \end{bmatrix} \qquad \text{Eq (7)}$$

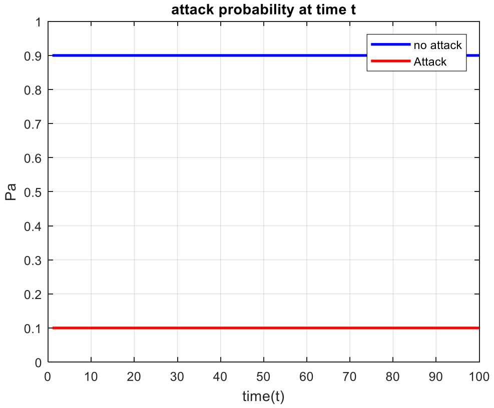


Figure.15 Attack Probability of Markov Binomial Distribution

The binomial distribution is a memory less positioning having probability 'P_a' where each time slot is stationary and equal to $'p_{a_0}$'.

8. Simulation Graphs

Markov:

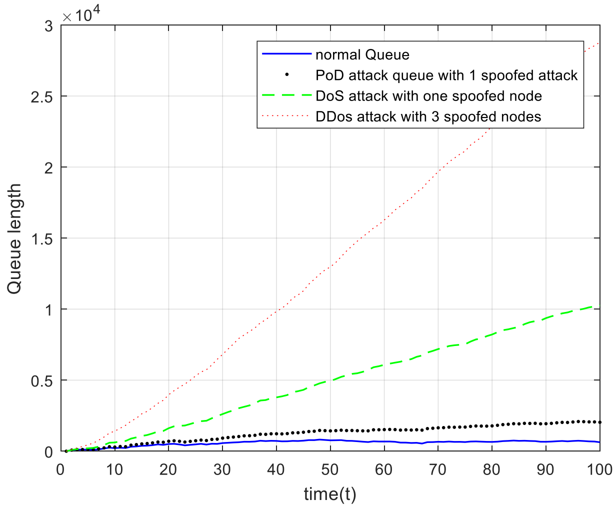


Figure.16 Queue Length generation using Cyber-attacks for Markov Chain

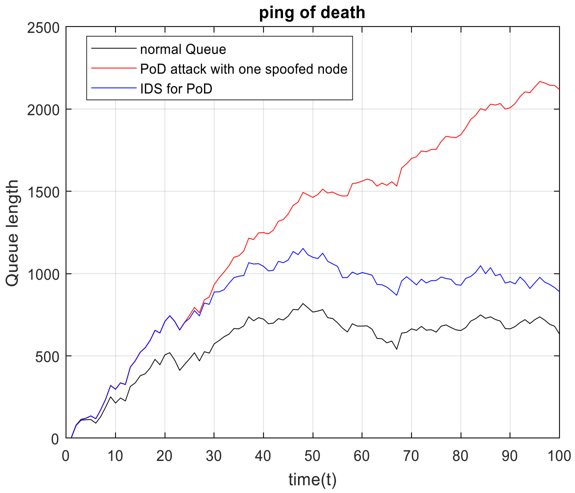


Figure.17 Shrinking queue length using IDS for Ping-of-death using Markov Distribution

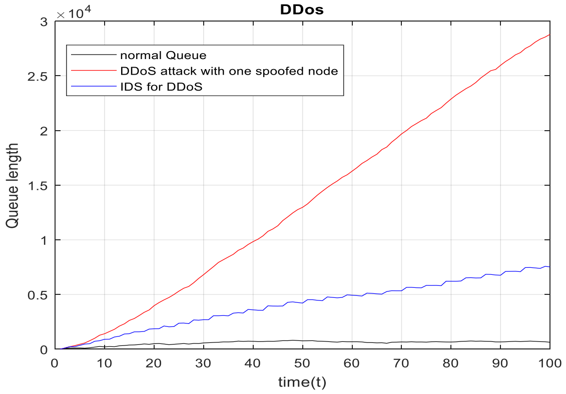


Figure.18 Reducing queue length for D-DoS attack utilizing Markov

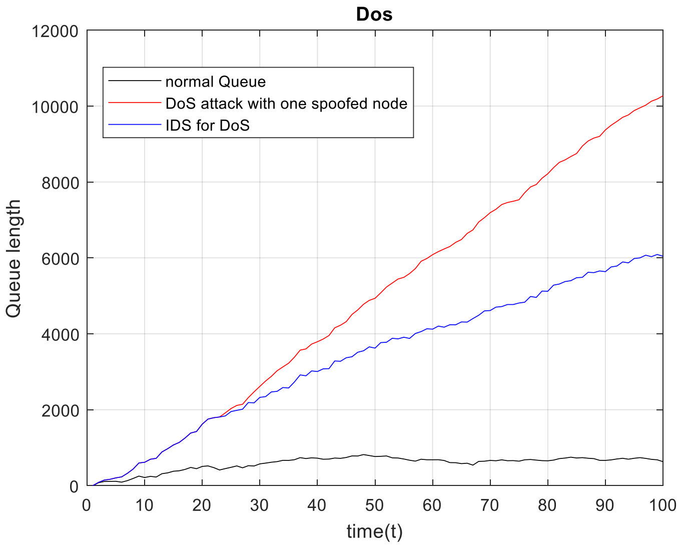


Figure.19 Minimizing queue length for DoS attack using markov chain

Binomial markov:

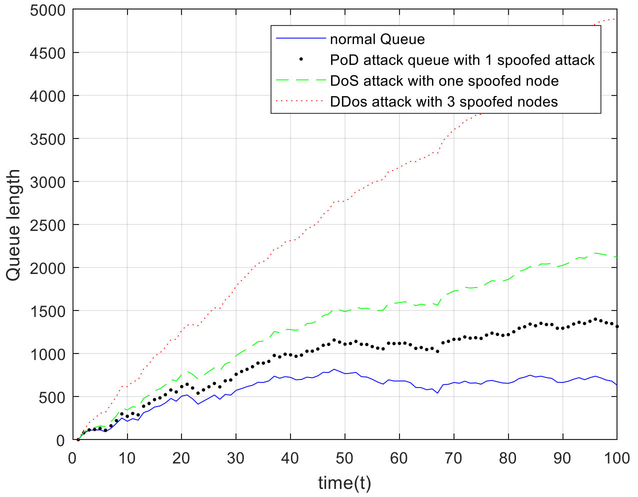


Figure.20 Mitigating queue length for Security threats using markov binomial

Here there is two option, where p_a be constant in binomial distribution or be time variant in Markov chain distribution. The result threshold is shown below:

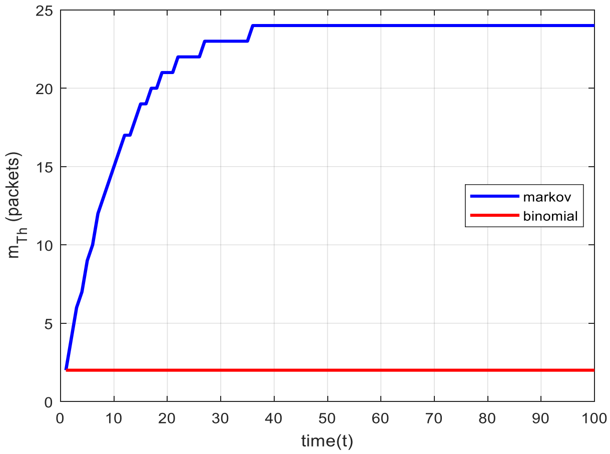


Figure.21 Threshold result of Markov and Binomial distribution

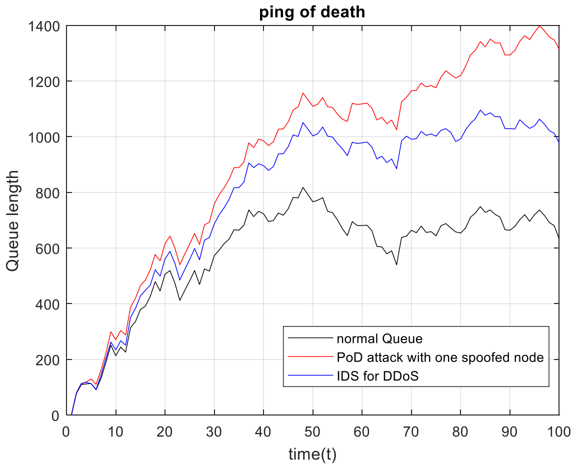


Figure.22 PoD analysis for Queue length making use of Binomial markov

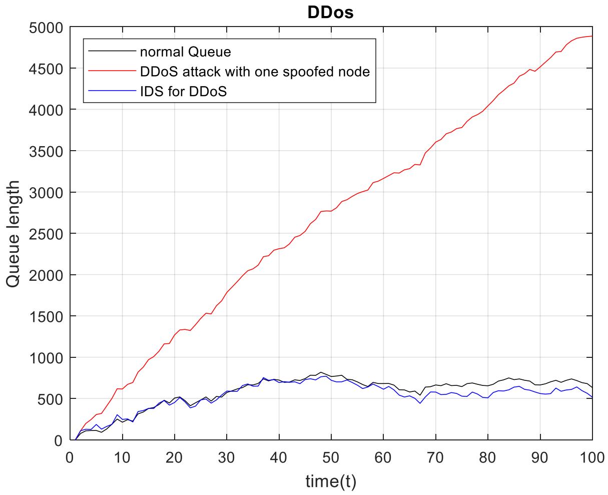


Figure.23 D-Dos study for Queue length employing Binomial markov

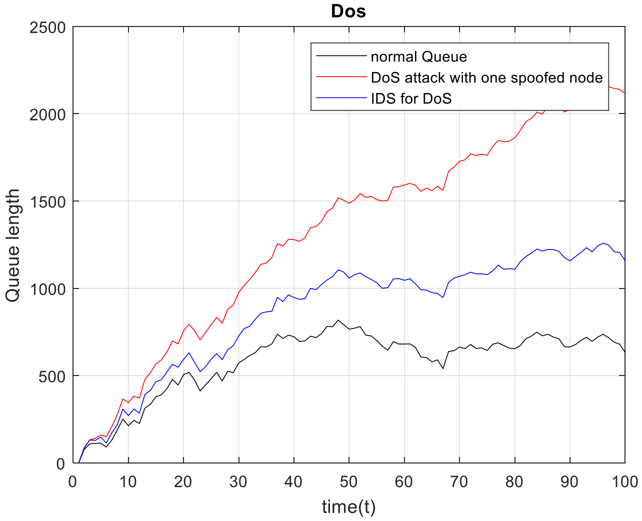


Figure. 24 DoS attack queue length using IDS for normal data packets

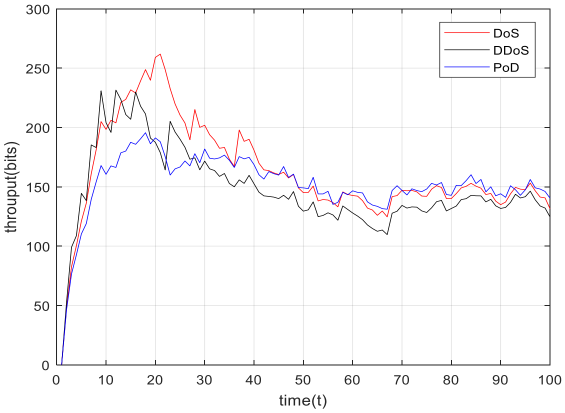


Figure. 25 Throughput study of security attacks using Markov Distribution

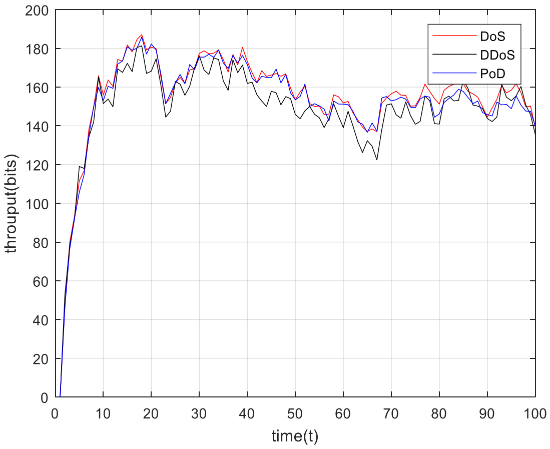


Figure. 26 Throughput analysis of cyber threats using Binomial Distribution

Table. 1 Packet Drop Rate Analysis using DoS, D-DoS & PoD Security Threats

Packet Drops	DoS Attack	DDoS Attack	PoD attack
Markov binomial	49	222	19
Markov	75	273	60

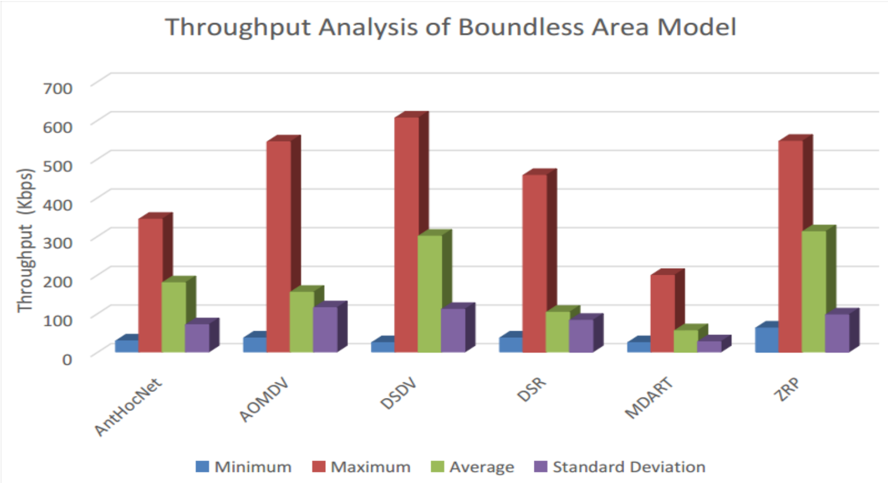
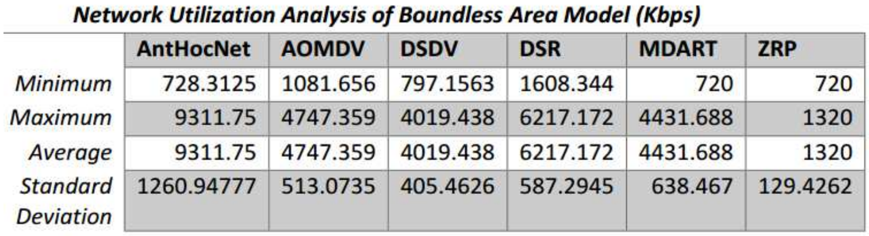


Figure. 27 Throughput Analysis AntHocNet with other protocols

Table.2 Network Utilization Analysis of Boundless Area Model



Network Utilization Analysis of Boundless Area Model (Kbps)

	AntHocNet	AOMDV	DSDV	DSR	MDART	ZRP
Minimum	728.3125	1081.656	797.1563	1608.344	720	720
Maximum	9311.75	4747.359	4019.438	6217.172	4431.688	1320
Average	9311.75	4747.359	4019.438	6217.172	4431.688	1320
Standard Deviation	1260.94777	513.0735	405.4626	587.2945	638.467	129.4262

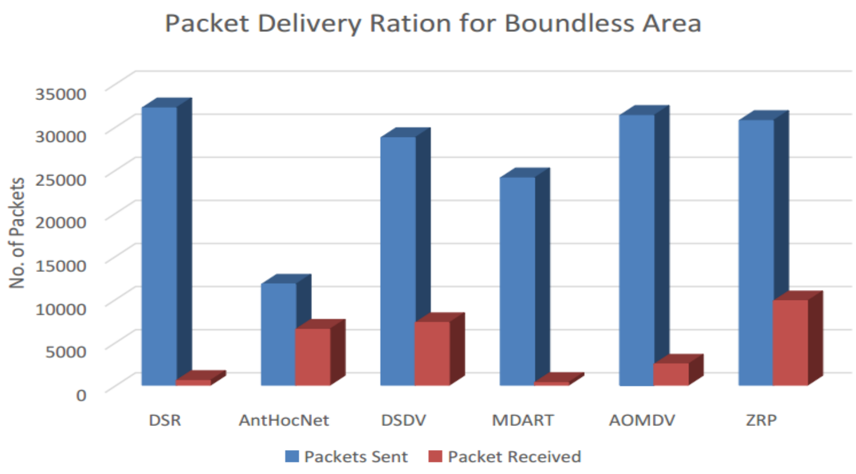


Figure.28 Packet Delivery ratio

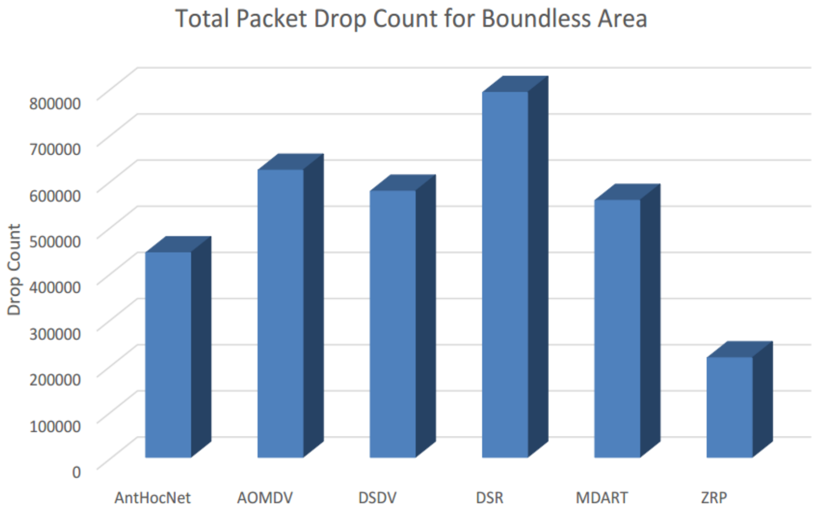


Figure. 29 Packet drop count analysis

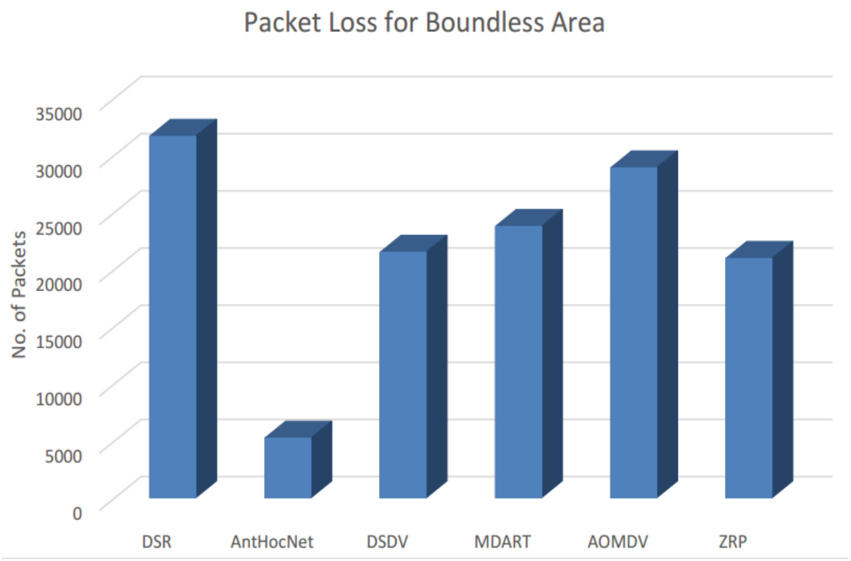


Figure. 30 Packet Loss study

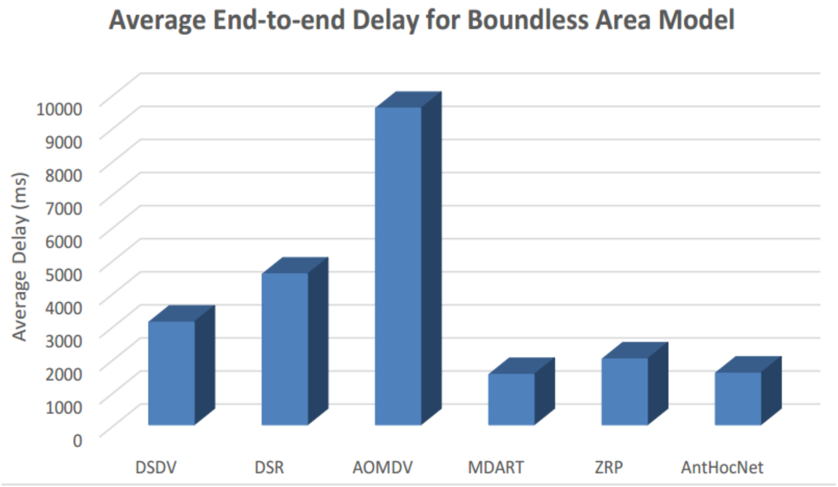


Figure. 31end-to-end delay or jitter

9. Results Discussion

Optimization of connection links will re-shape the entire planet therefore safety of this society needs countermeasures to make the information-age secure. For the security of modeled smart city having drones to stabilize path flying things detection system is launched to detect some cyber-threats include third-party-attack, D-DoS, and a special version is identified where attacker-UAV try to crash or destabilize the aerial network which we call ping-of-death. Due to high network performance the detection-system attempts to trade-off between missed detection probability and false alarm probability. This concept assists researchers to have interconnectivity having maximum missed detection probability along with minimum false alarm prospects. However, ant-learning routing protocol exhibits better outcome in comparison with other standard computations. This research study is one of a kind works where routing protocols and cyber-attacks are properly demonstrated using various parameters also markov chain probability distribution is used to enhance the working principal of intrusion detection system. Apart from that binomial randomness shows variation while incorporating this method with flying detection system to remove abnormal queues in the aerial networks.

10. Conclusion

The world is transforming into smart-world which has identified so many cyber security attacks vulnerabilities. Smart cities are integrated with flying things to improve the quality of experience in communication channels where in this study, IoFT use boundless simulation area mobility pattern to boost-up the technological era. In addition, security risks like denial-off-service, distributed-denial-off-service and ping-of-death attacks are demonstrated in the framework of smart cities also markov-chain stochastic process is merged, which assist to find the gateway approach for flying vehicles. Communication comprises drone-2-drone & land-station-2-aerial-vehicles have used, IEEE 802.11 wireless technology to improve transmission routes. The regular swapping in network structure makes hard to implement routing control scheme known as flying-AntHocNet motivated from systematic environment-based approach which show optimal simulation results in metrics like end-2-end-delay, packet loss, data-packet-drop-count, as well as in throughput analysis in comparison with conventional routing techniques include DSDV, DSR, AOMDV, M-DART, Z-R-P are introduced in aerial networks. Accordingly, internet-of-everything abstraction in smart cities is technologized to secure the society from cyber-attacks.

Declarations

Funding No funding agency was involved in the funding of the research.

Conflicts of interest/Competing interest Authors declare that there is no conflict of interest amongst authors regarding the publication of the research paper.

Availability of data and material Data and material used in this research work are available from corresponding author upon request

Code availability Code used for the experiments in this research is available from corresponding author upon request

Authors contributions Inam Ullah Khan (Data curation, formal analysis, methodology, original manuscript writing), Arsin Abdollahi (Data analysis, methodology, experiments, original manuscript writing), Muhammad Asghar Khan (Fund acquisition, formal analysis, data analysis, visualization, manuscript revision), M. Irfan Uddin (supervision, formal analysis, visualization, manuscript revision), Insaf Ullah (supervision, formal analysis, visualization, manuscript revision)

References

1. Noor F, Khan MA, Al-Zahrani A, Ullah I, Al-Dhlan KA. A Review on Communications Perspective of Flying Ad-Hoc Networks: Key Enabling Wireless Technologies, Applications, Challenges and Open Research Topics. Drones. 2020; 4(4):65.
2. Abdollahi, A., Fathi, M. An Intrusion Detection System on Ping of Death Attacks in IoT Networks. *Wireless Pers Commun* 112**,** 2057–2070 (2020). https://doi.org/10.1007/s11277-020-07139-y.
3. D. Pliatsios, P. Sarigiannidis, T. Lagkas and A. G. Sarigiannidis, "A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics," in *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1942-1976, thirdquarter 2020, doi: 10.1109/COMST.2020.2987688.
4. W. A. Al-Khater, S. Al-Maadeed, A. A. Ahmed, A. S. Sadiq and M. K. Khan, "Comprehensive Review of Cybercrime Detection Techniques," in *IEEE Access*, vol. 8, pp. 137293-137311, 2020, doi: 10.1109/ACCESS.2020.3011259.
5. R. N. Akram *et al*., "Security, privacy and safety evaluation of dynamic and static fleets of drones," *2017 IEEE/AIAA 36th Digital Avionics Systems Conference (DASC)*, St. Petersburg, FL, 2017, pp. 1-12, doi: 10.1109/DASC.2017.8101984.
6. M. Albalawi and H. Song, "Data Security and Privacy Issues in Swarms of Drones," *2019 Integrated Communications, Navigation and Surveillance Conference (ICNS)*, Herndon, VA, USA, 2019, pp. 1-11, doi: 10.1109/ICNSURV.2019.8735133.
7. J. Chen, Z. Feng, J. Wen, B. Liu and L. Sha, "A Container-based DoS Attack-Resilient Control Framework for Real-Time UAV Systems," *2019 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, Florence, Italy, 2019, pp. 1222-1227, doi: 10.23919/DATE.2019.8714888.
8. S. Garg, G. S. Aujla, N. Kumar and S. Batra, "Tree-Based Attack–Defense Model for Risk Assessment in Multi-UAV Networks," in *IEEE Consumer Electronics Magazine*, vol. 8, no. 6, pp. 35-41, 1 Nov. 2019, doi: 10.1109/MCE.2019.2941345.
9. M. Hooper *et al*., "Securing commercial WiFi-based UAVs from common security attacks," *MILCOM 2016 - 2016 IEEE Military Communications Conference*, Baltimore, MD, 2016, pp. 1213-1218, doi: 10.1109/MILCOM.2016.7795496.
10. C. Lin, D. He, N. Kumar, K. R. Choo, A. Vinel and X. Huang, "Security and Privacy for the Internet of Drones: Challenges and Solutions," in *IEEE Communications Magazine*, vol. 56, no. 1, pp. 64-69, Jan. 2018, doi: 10.1109/MCOM.2017.1700390.
11. R. Mohan, C. V. Raj, P. Aswathi and R. R. Bhavani, "UAV based security system for prevention of harassment against woman," *2017 International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)*, Kannur, 2017, pp. 874-879, doi: 10.1109/ICICICT1.2017.8342680.
12. M. Podhradsky, C. Coopmans and N. Hoffer, "Improving communication security of open source UAVs: Encrypting radio control link," *2017 International Conference on Unmanned Aircraft Systems (ICUAS)*, Miami, FL, USA, 2017, pp. 1153-1159, doi: 10.1109/ICUAS.2017.7991460.
13. Chaitanya Rani, Hamidreza Modares, Raghavendra Sriram, Dariusz Mikulski, and Frank L Lewis," Security of unmanned aerial vehicle systems against cyber-physical attacks", Journal of Defense Modeling and Simulation: Applications, Methodology, Technology, Nov,2015.
14. F. Restuccia, S. D'Oro and T. Melodia, "Securing the Internet of Things in the Age of Machine Learning and Software-Defined Networking," in *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 4829-4842, Dec. 2018, doi: 10.1109/JIOT.2018.2846040.
15. F. E. Salamh, U. Karabiyik, M. Rogers and F. Al-Hazemi, "Drone Disrupted Denial of Service Attack (3DOS): Towards an Incident Response and Forensic Analysis of Remotely Piloted Aerial Systems (RPASs)," *2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)*, Tangier, Morocco, 2019, pp. 704-710, doi: 10.1109/IWCMC.2019.8766538.
16. A. Sehrawat, T. A. Choudhury and G. Raj, "Surveillance drone for disaster management and military security," *2017 International Conference on Computing, Communication and Automation (ICCCA)*, Greater Noida, 2017, pp. 470-475, doi: 10.1109/CCAA.2017.8229846.

17. Wang, C.; Zhu, L.; Gong, L.; Zhao, Z.; Yang, L.; Liu, Z.; Cheng, X. Accurate Sybil Attack Detection Based on Fine-Grained Physical Channel Information. *Sensors* 2018, *18*, 878.
18. Thomas Lagkas , Vasileios Argyriou , Stamatia Bibi and Panagiotis Sarigiannidis , “UAV IoT Framework Views and Challenges: Towards Protecting Drones as “Things””, *Sensors* 2018, *18*, 4015; doi:10.3390/s18114015.
19. A. Singandhupe, H. M. La and D. Feil-Seifer, "Reliable Security Algorithm for Drones Using Individual Characteristics From an EEG Signal," in *IEEE Access*, vol. 6, pp. 22976-22986, 2018, doi: 10.1109/ACCESS.2018.2827362.
20. G. Vasconcelos, G. Carrijo, R. Miani, J. Souza and V. Guizilini, "The Impact of DoS Attacks on the AR.Drone 2.0," *2016 XIII Latin American Robotics Symposium and IV Brazilian Robotics Symposium (LARS/SBR)*, Recife, 2016, pp. 127-132, doi: 10.1109/LARS-SBR.2016.28.
21. E. Vattapparamban, İ. Güvenç, A. İ. Yurekli, K. Akkaya and S. Uluağaç, "Drones for smart cities: Issues in cybersecurity, privacy, and public safety," *2016 International Wireless Communications and Mobile Computing Conference (IWCMC)*, Paphos, 2016, pp. 216-221, doi: 10.1109/IWCMC.2016.7577060.
22. Z. Zaheer, A. Usmani, E. Khan and M. A. Qadeer, "Aerial surveillance system using UAV," *2016 Thirteenth International Conference on Wireless and Optical Communications Networks (WOCN)*, Hyderabad, 2016, pp. 1-7, doi: 10.1109/WOCN.2016.7759885.
23. M. Y. Arafat and S. Moh, "Routing Protocols for Unmanned Aerial Vehicle Networks: A Survey," in *IEEE Access*, vol. 7, pp. 99694-99720, 2019, doi: 10.1109/ACCESS.2019.2930813.
24. Chen, X.; Tang, J.; Lao, S. Review of Unmanned Aerial Vehicle Swarm Communication Architectures and Routing Protocols. *Appl. Sci.* **2020**, *10*, 3661.
25. T. Nishitha and P. C. Reddy, "Performance Evaluation of AntHocNet Routing Algorithm in Ad Hoc Networks," *2012 International Conference on Computing Sciences*, Phagwara, 2012, pp. 207-211, doi: 10.1109/ICCS.2012.58.
26. Wu J., Shi S., Liu Z., Gu X. (2019) Optimization of AODV Routing Protocol in UAV Ad Hoc Network. In: Han S., Ye L., Meng W. (eds) Artificial Intelligence for Communications and Networks. AICON 2019. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 286. Springer, Cham. https://doi.org/10.1007/978-3-030-22968-9_43.
27. A. Garcia-Santiago, J. Castaneda-Camacho, J. F. Guerrero-Castellanos and G. Mino-Aguilar, "Evaluation of AODV and DSDV routing protocols for a FANET: Further results towards robotic vehicle networks," *2018 IEEE 9th Latin American Symposium on Circuits & Systems (LASCAS)*, Puerto Vallarta, 2018, pp. 1-4, doi: 10.1109/LASCAS.2018.8399972.
28. A. Nayyar, "Flying Adhoc Network (FANETs): Simulation Based Performance Comparison of Routing Protocols: AODV, DSDV, DSR, OLSR, AOMDV and HWMP," *2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD)*, Durban, 2018, pp. 1-9, doi: 10.1109/ICABCD.2018.8465130.
29. Marcello Caleffi, Luigi Paura,” M-DART: multi-path dynamic address routing”, Wireless Communications & Mobile Computing, March 2011, 10.1002/wcm.986.

Figures

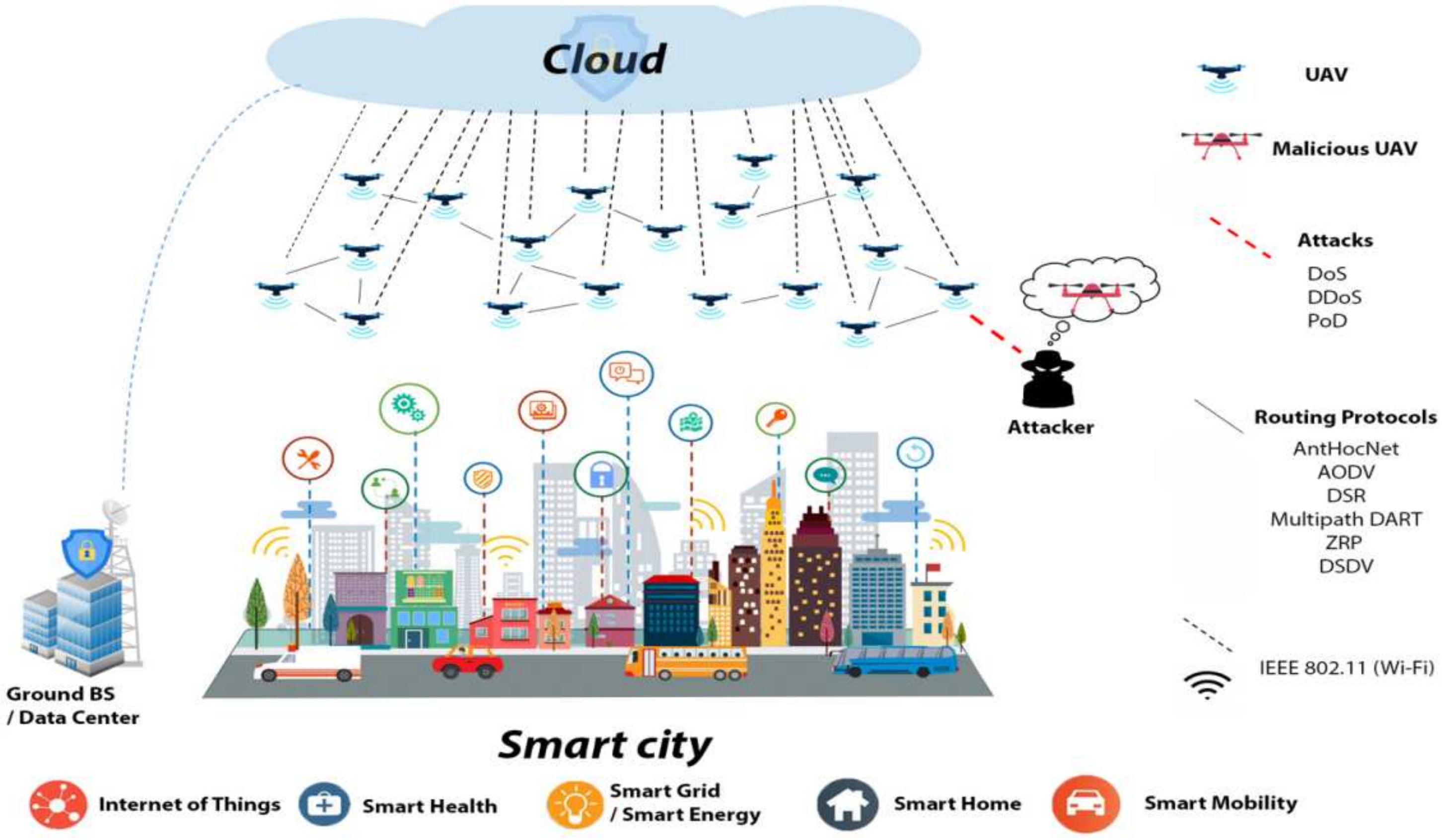


Figure 1

A sample architecture of Internet of Flying Things for smart cities applications.

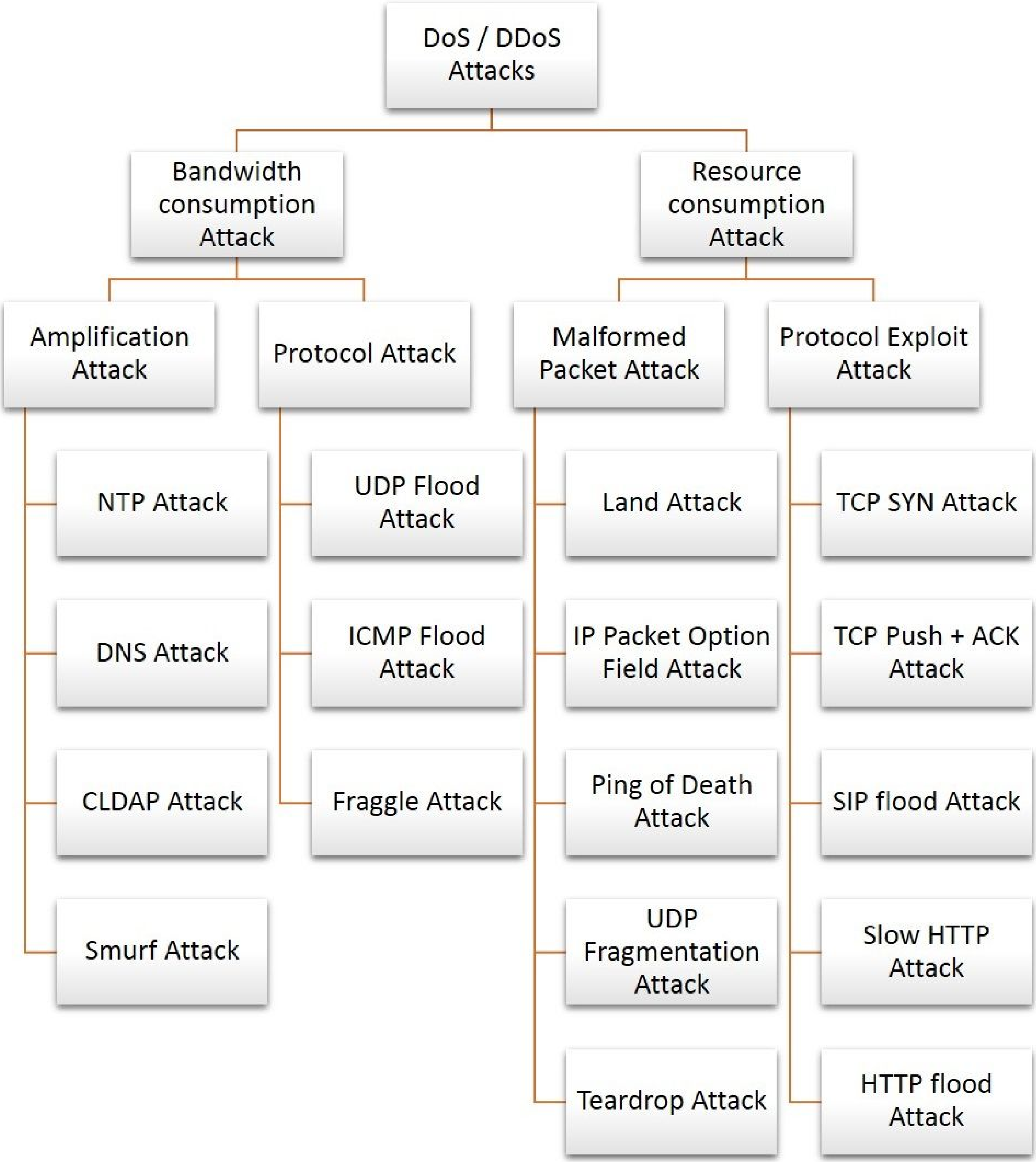


Figure 2

Classification of DoS/D-DoS Security Threats

Image not available with this version

Figure 3

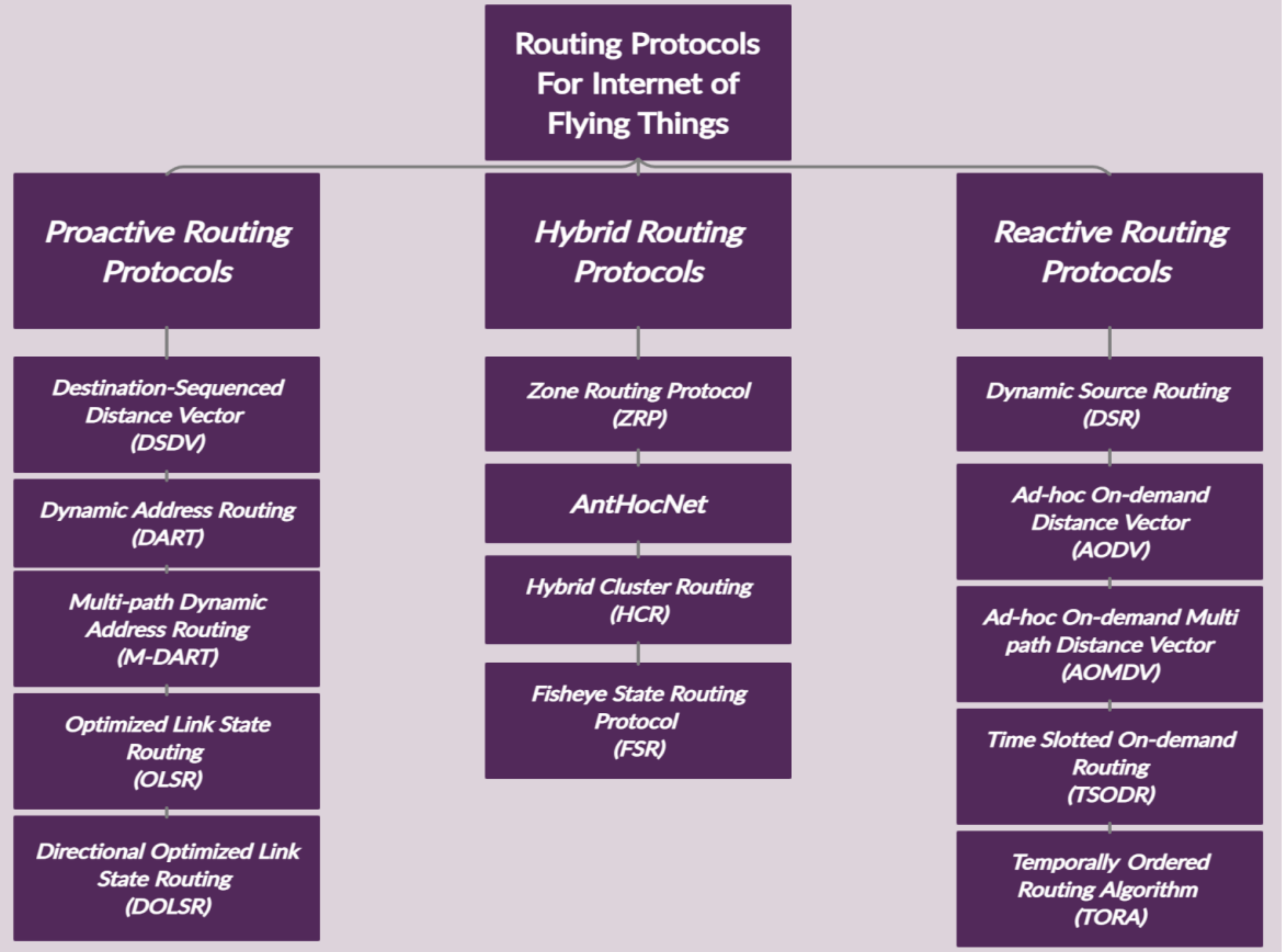

Routing Protocols For Internet of Flying Things
Proactive Routing Protocols
Hybrid Routing Protocols
Reactive Routing Protocols
Destination-Sequenced Distance Vector (DSDV)
Dynamic Address Routing (DART)
Multi-path Dynamic Address Routing (M-DART)
Optimized Link State Routing (OLSR)
Directional Optimized Link State Routing (DOLSR)
Zone Routing Protocol (ZRP)
AntHocNet
Hybrid Cluster Routing (HCR)
Fisheye State Routing Protocol (FSR)
Dynamic Source Routing (DSR)
Ad-hoc On-demand Distance Vector (AODV)
Ad-hoc On-demand Multi path Distance Vector (AOMDV)
Time Slotted On-demand Routing (TSODR)
Temporally Ordered Routing Algorithm (TORA)

Figure 4

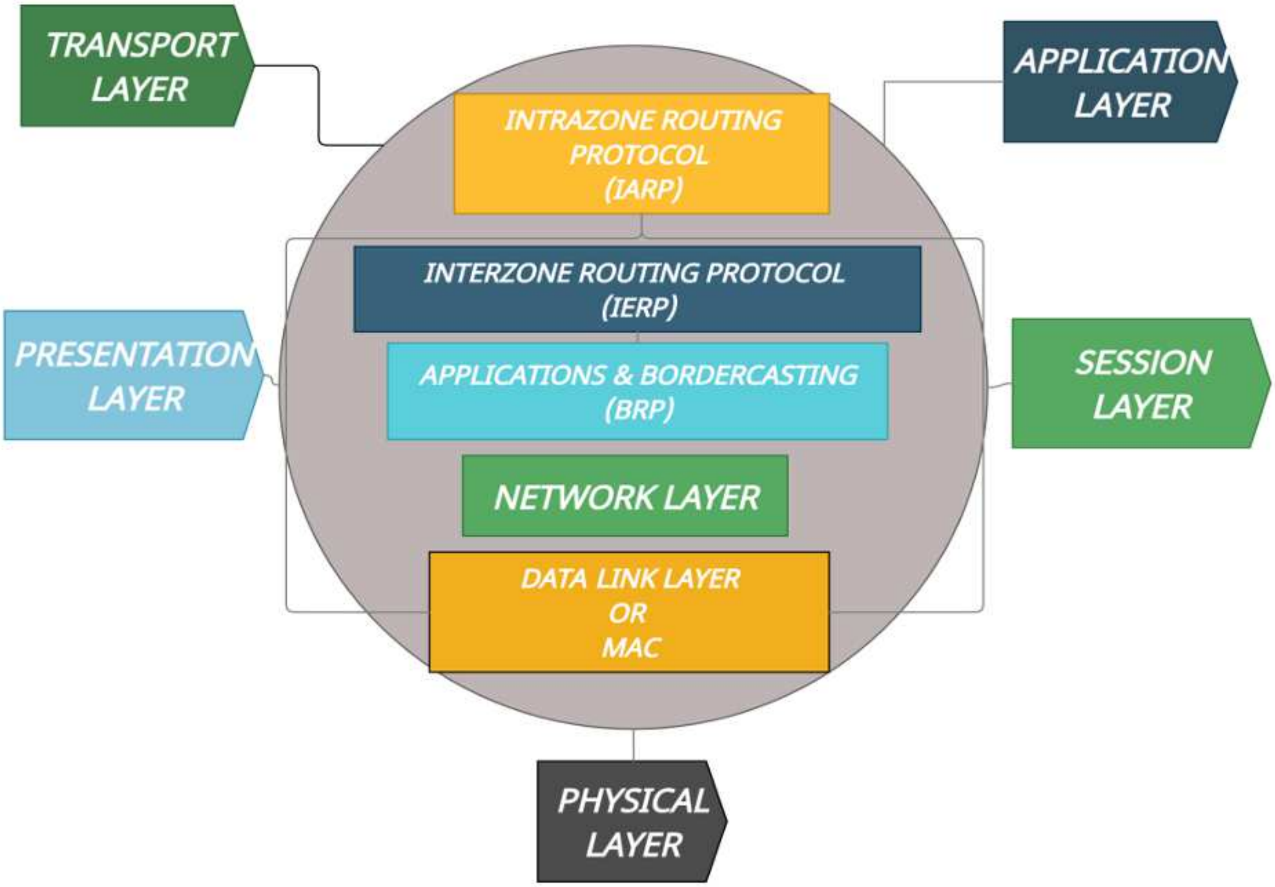
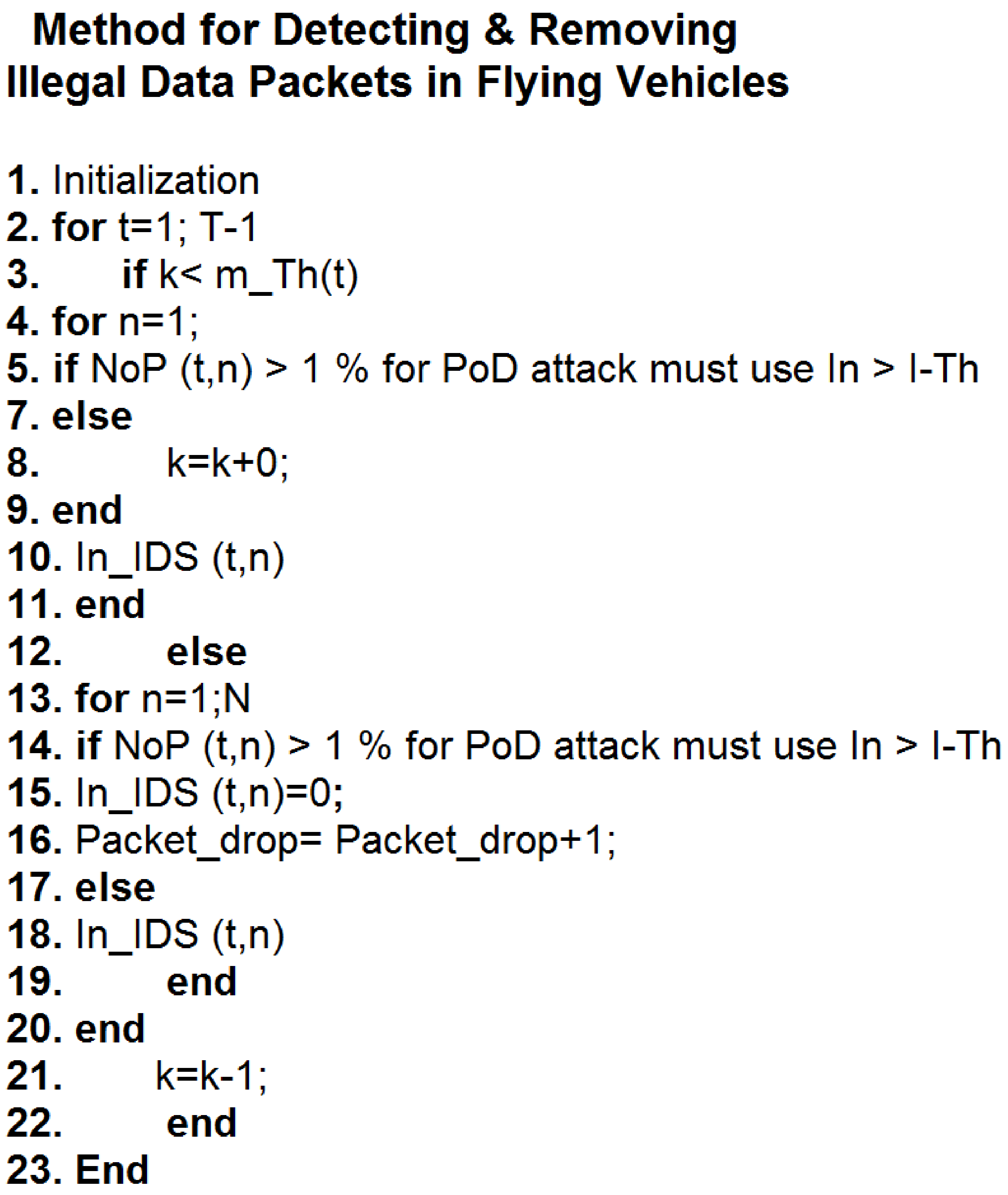


Figure 5

OSI Model with Detailed Architectural Design of ZRP



Method for Detecting & Removing Illegal Data Packets in Flying Vehicles

```
Initialization
for t=1; T-1
      if k< m_Th(t)
for n=1;
if NoP (t,n) > 1 % for PoD attack must use In > I-Th
else
          k=k+0;
end
In_IDS (t,n)
end
        else
for n=1;N
if NoP (t,n) > 1 % for PoD attack must use In > I-Th
In_IDS (t,n)=0;
Packet_drop= Packet_drop+1;
else
In_IDS (t,n)
        end
end
       k=k-1;
        end
End
```

Figure 6

Algorithm for Detecting & Removing illegal data packets

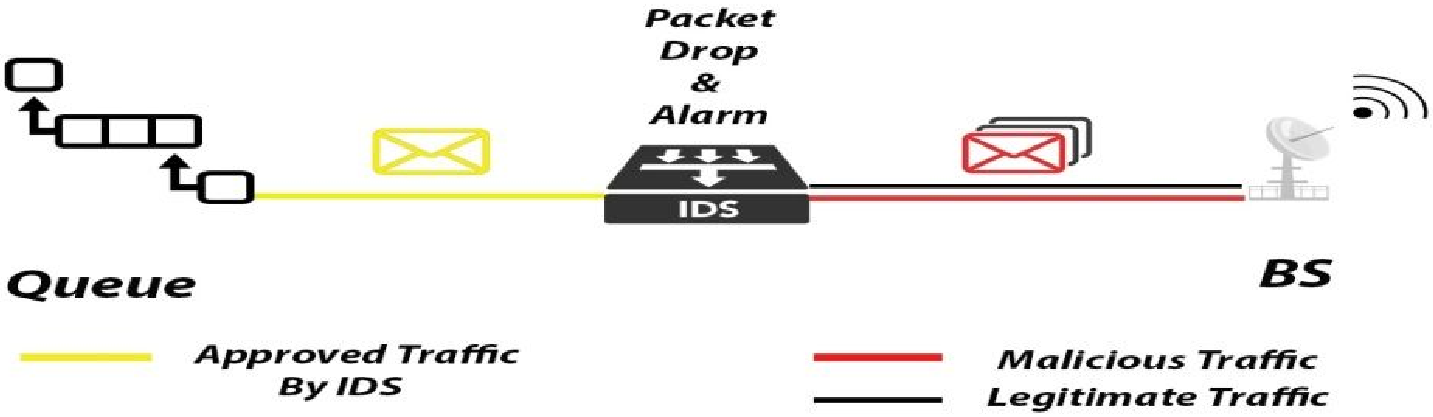


Figure 7

Physical Structure of IDS in land-Station

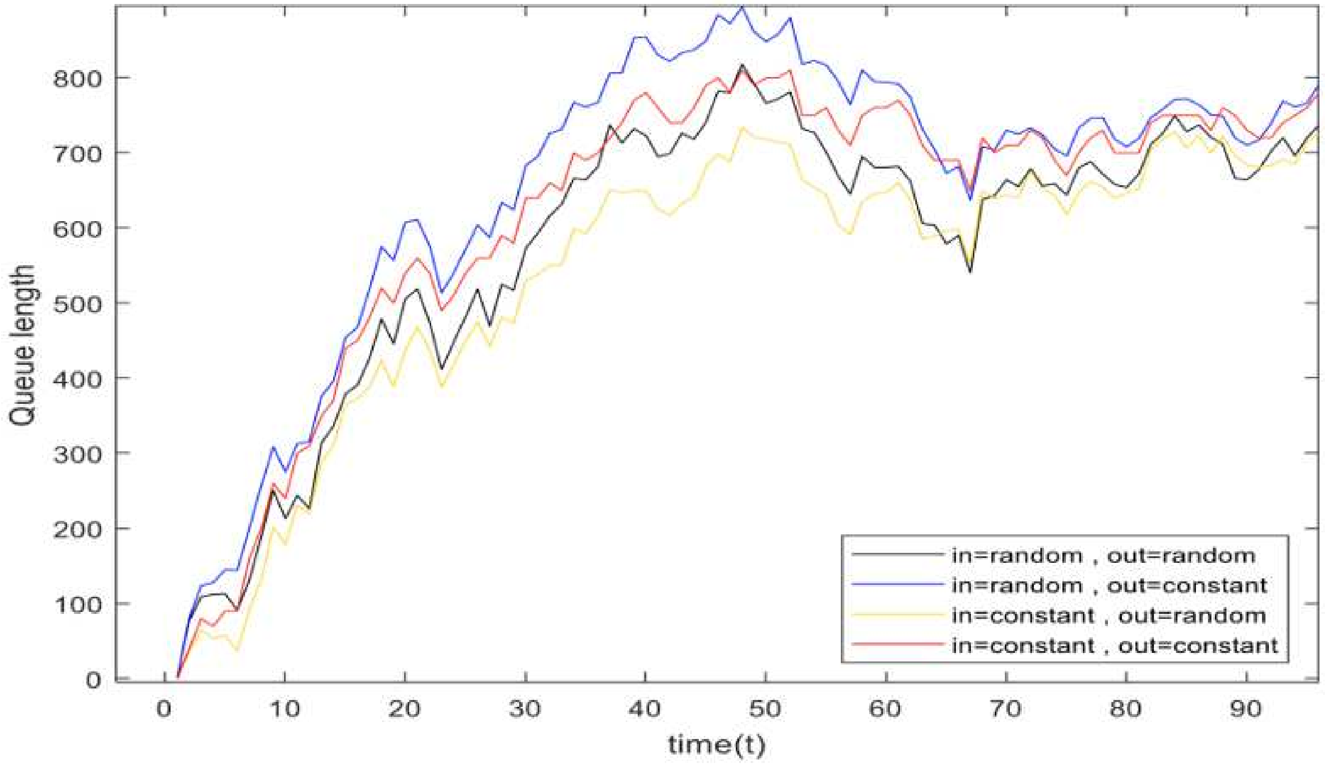


Figure 8

Probabilistic experimentation for generating queue

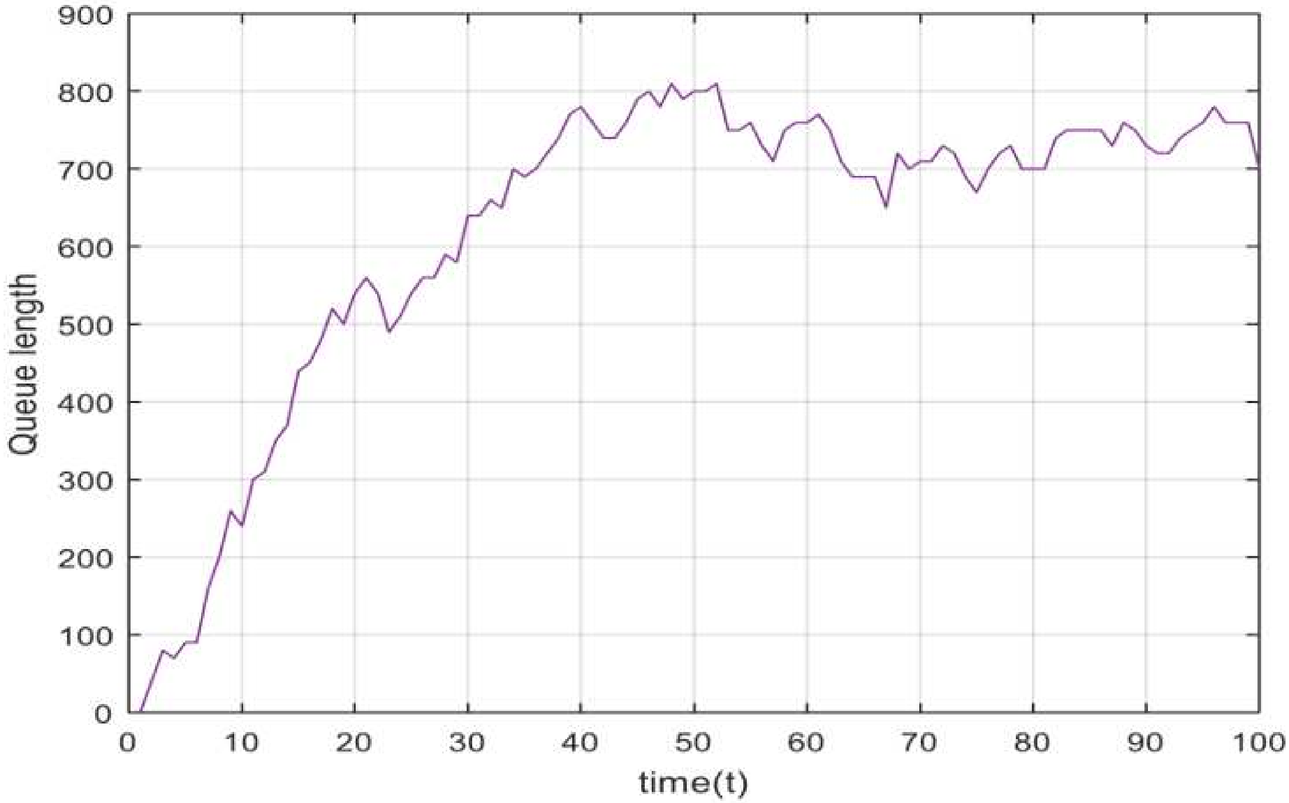


Figure 9

Queue length over time duration without attack

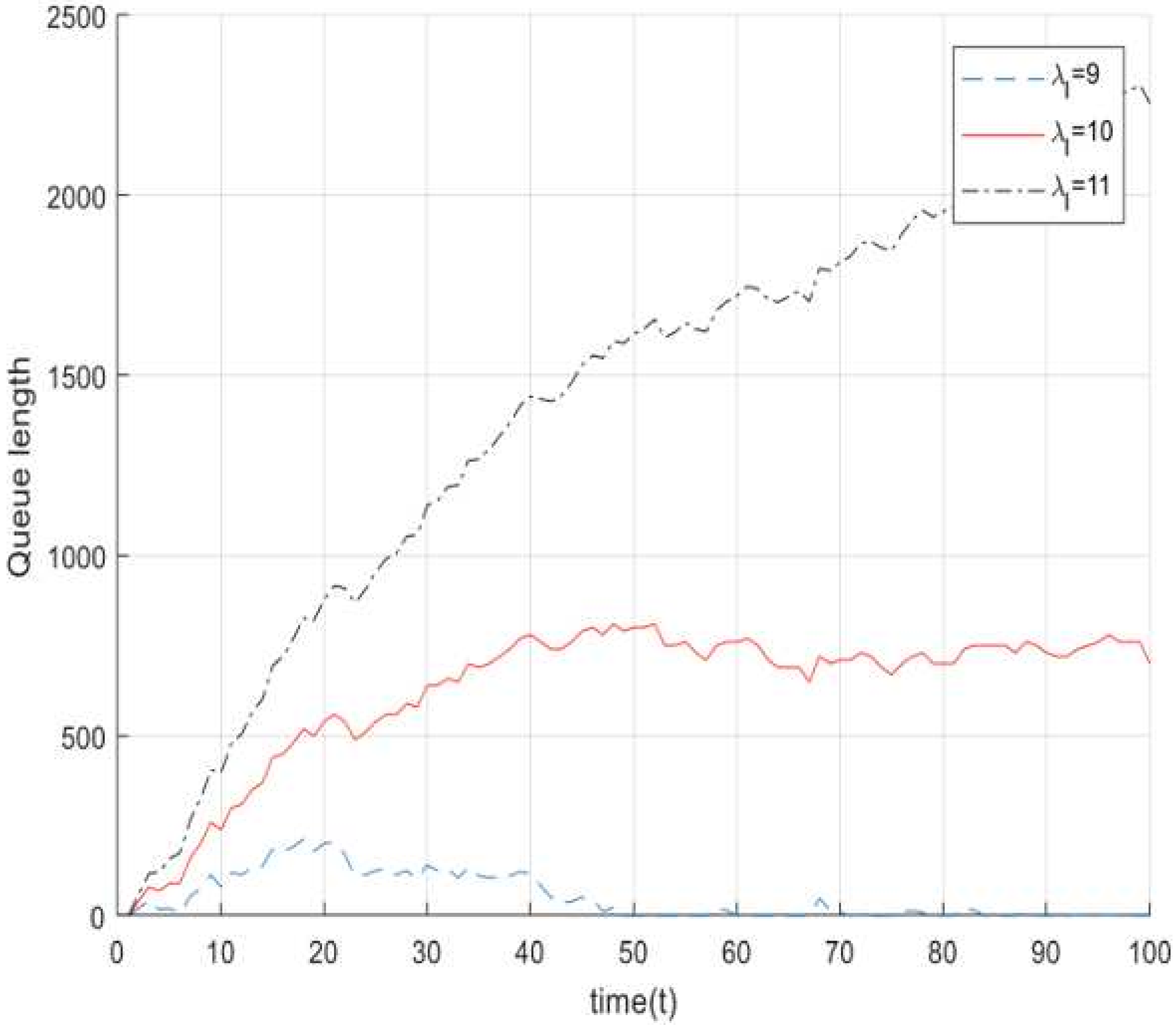


Figure 10

Independent Input rate of queue

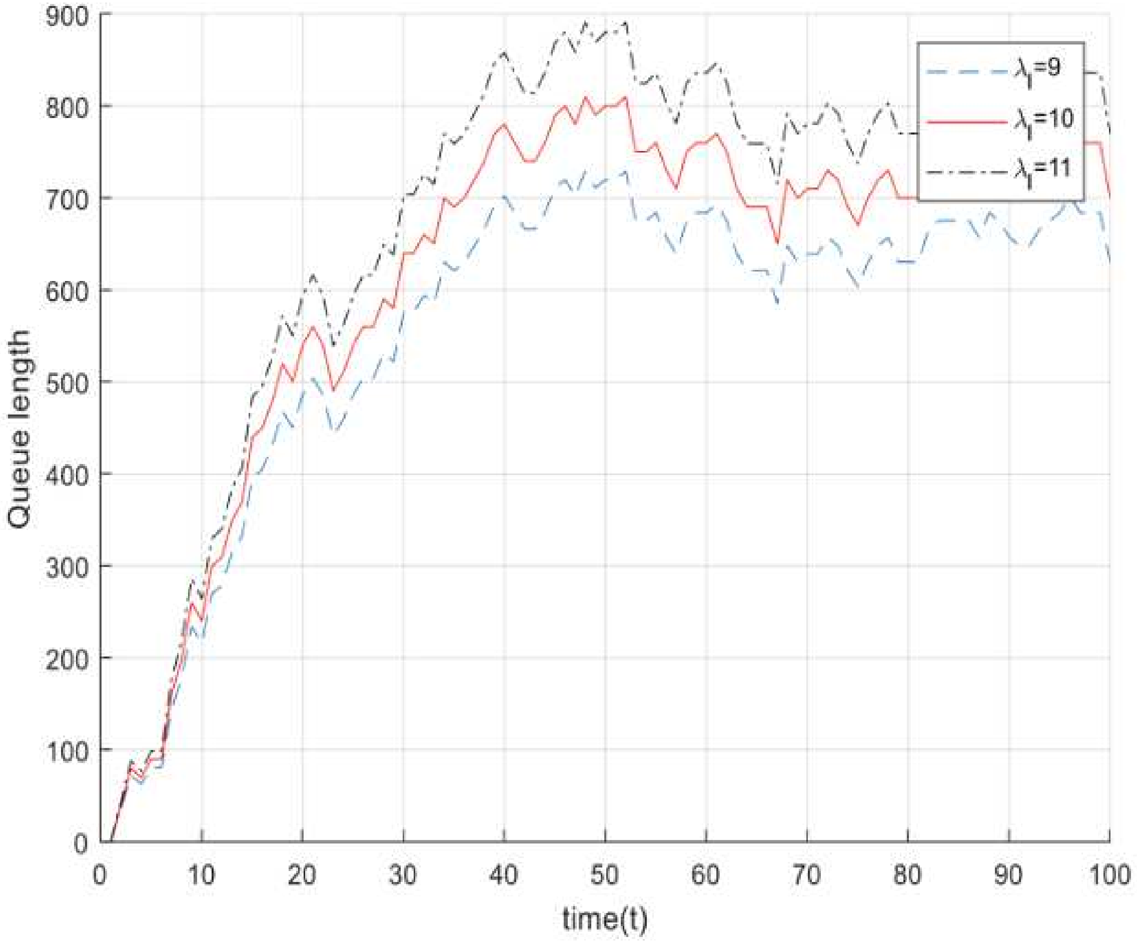


Figure 11

Queue depending on input rate

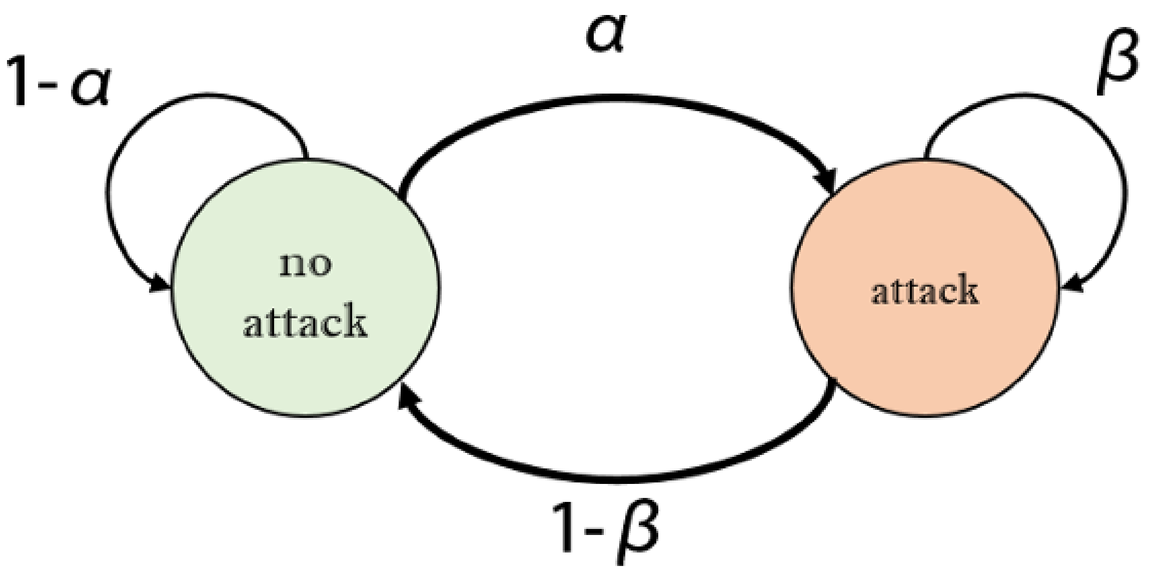


Figure 12

Two-state Markove Process

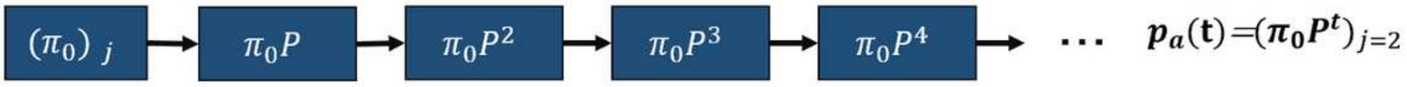

$(\pi_0)_j$
$\pi_0 P$
$\pi_0 P^2$
$\pi_0 P^3$
$\pi_0 P^4$
$\cdots$ $\boldsymbol{p_a}(\mathbf{t})=(\boldsymbol{\pi_0 P^t})_{j=2}$

Figure 13

Attack Probability at each time slot for desired markov chain

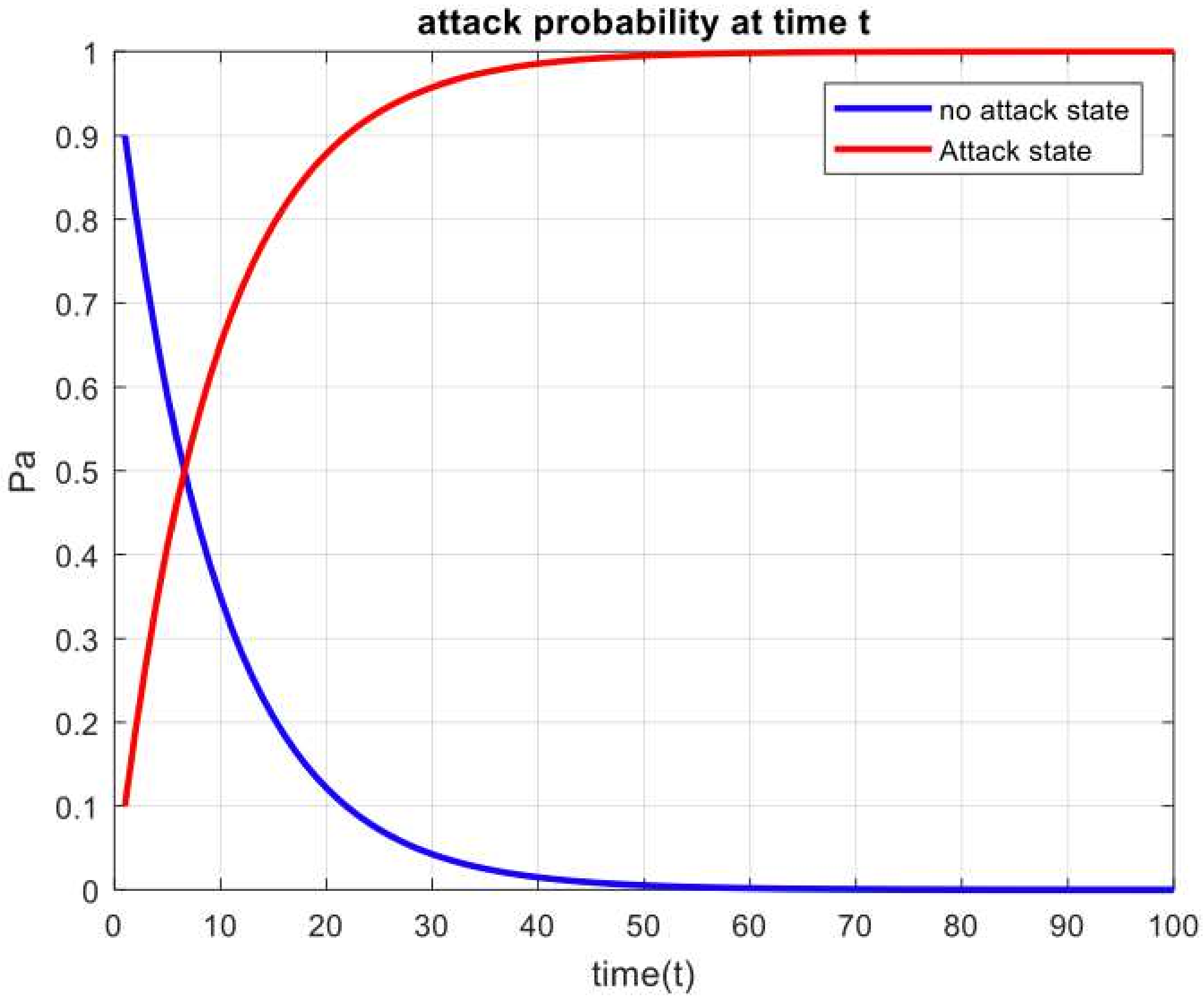


Figure 14

Attack randomness of Markov chain states at time t

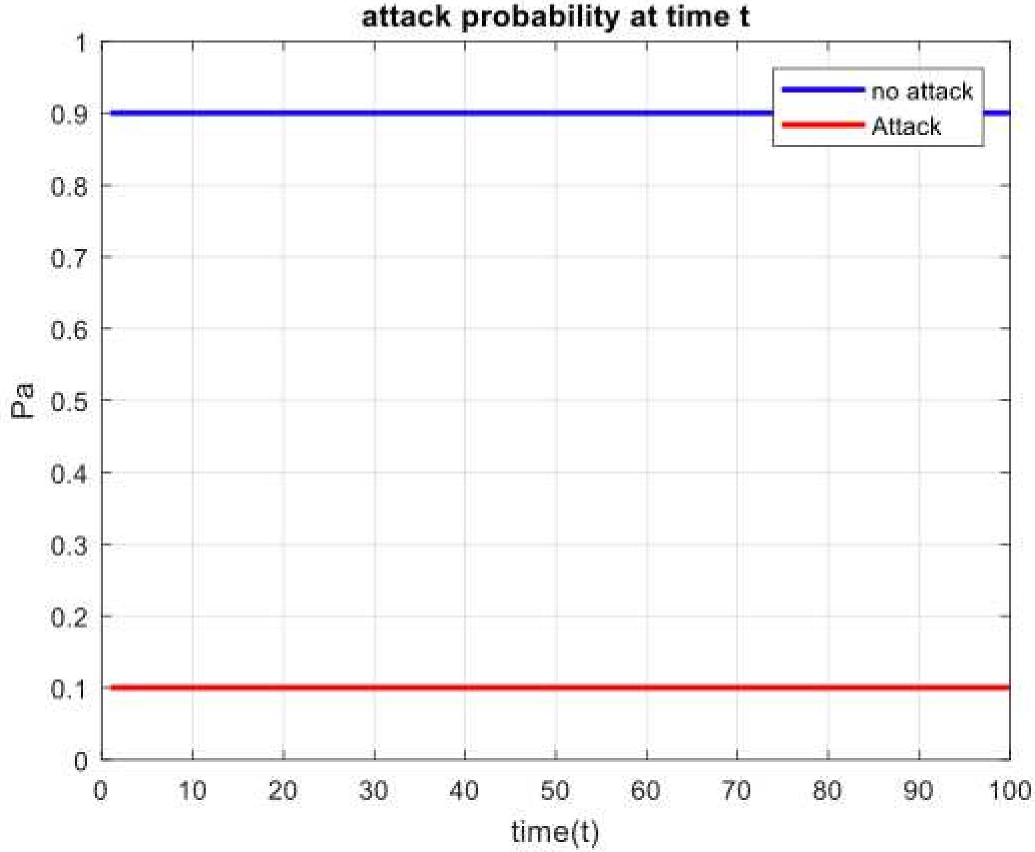


Figure 15

Attack Probability of Markov Binomial Distribution

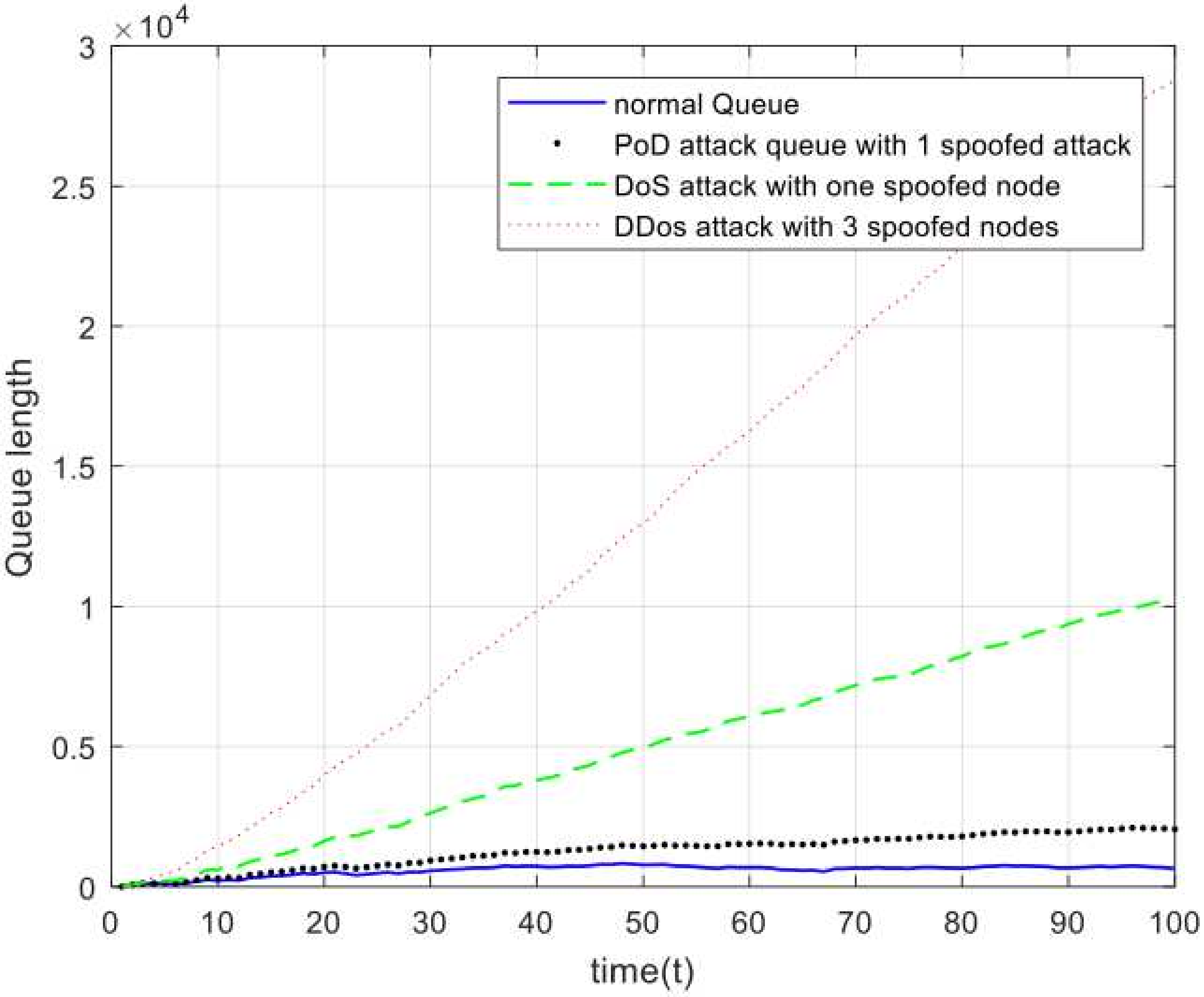


Figure 16

Queue Length generation using Cyber-attacks for Markov Chain

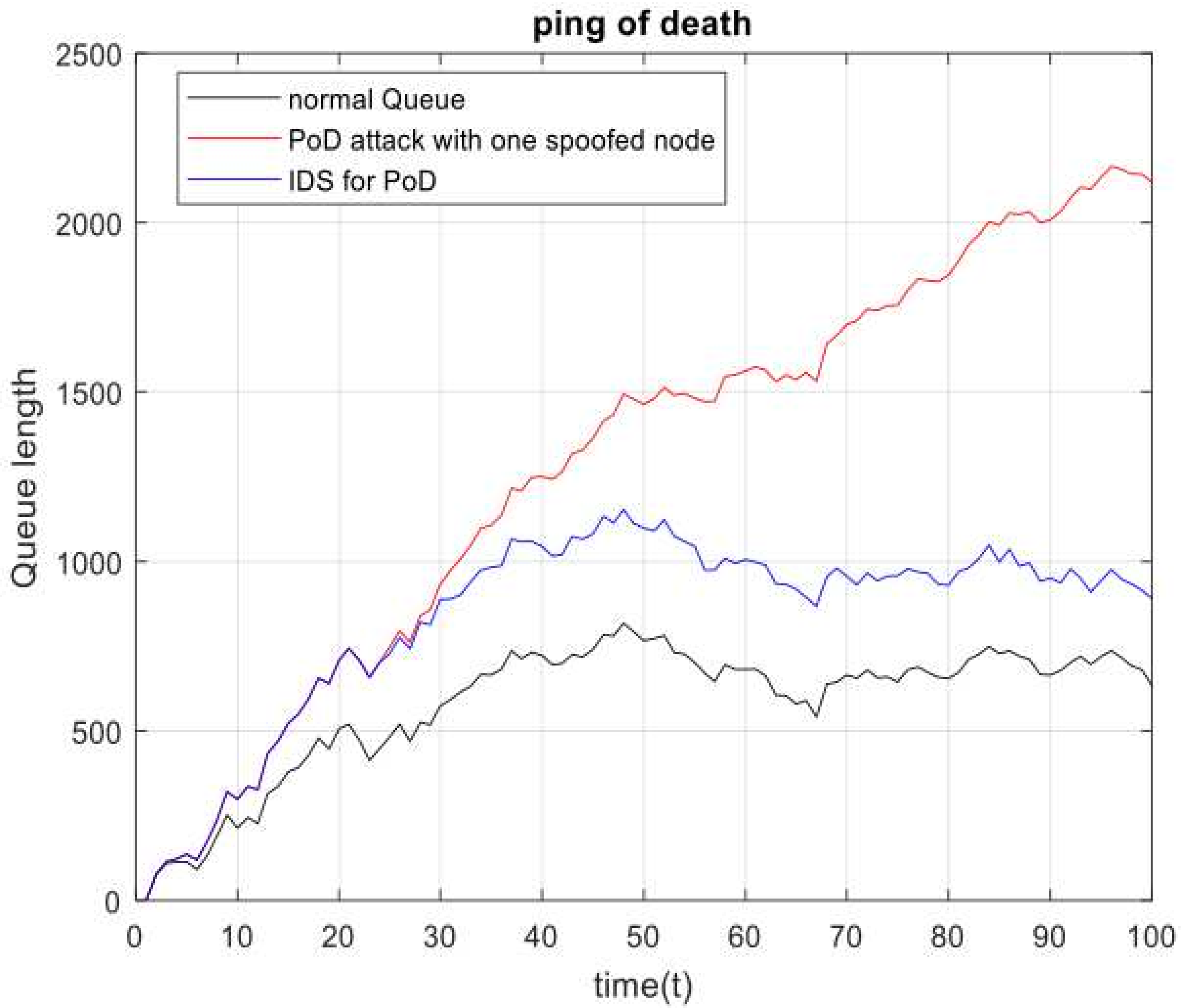


Figure 17

Shrinking queue length using IDS for Ping-of-death using Markov Distribution

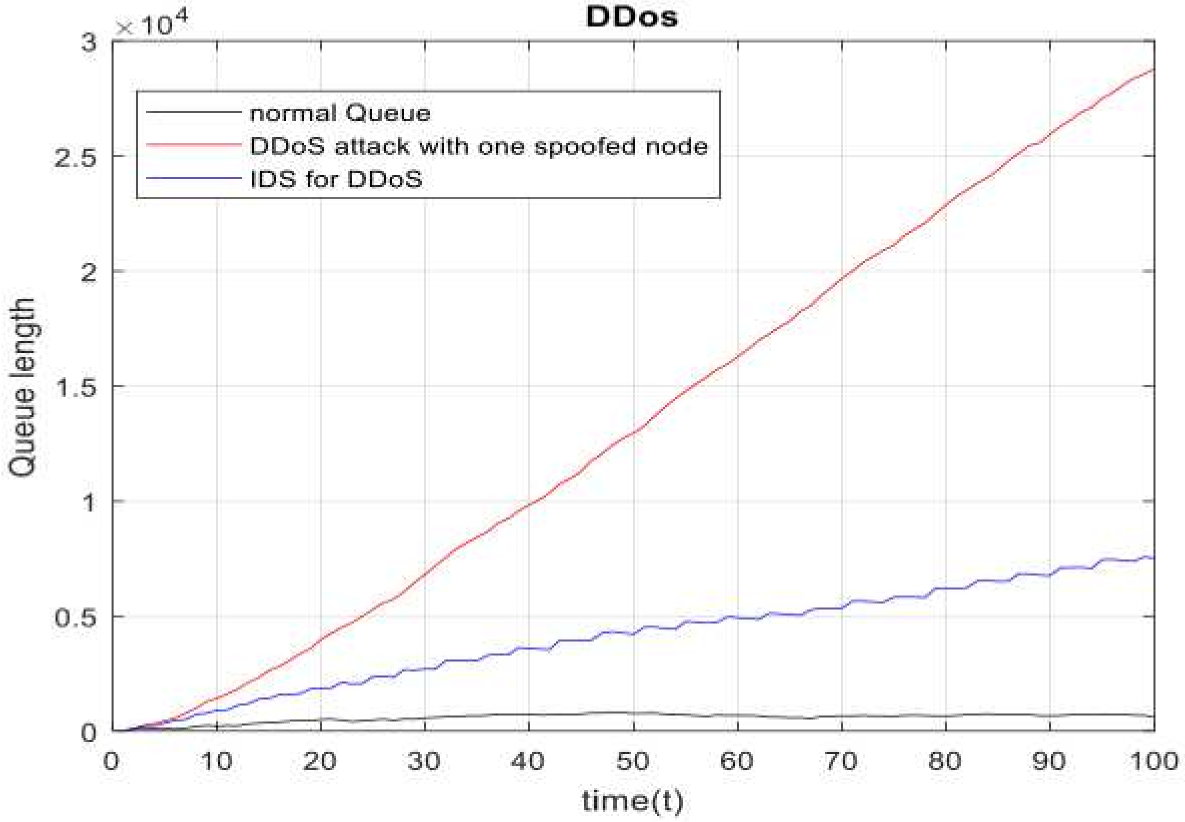


Figure 18

Reducing queue length for D-DoS attack utilizing Markov

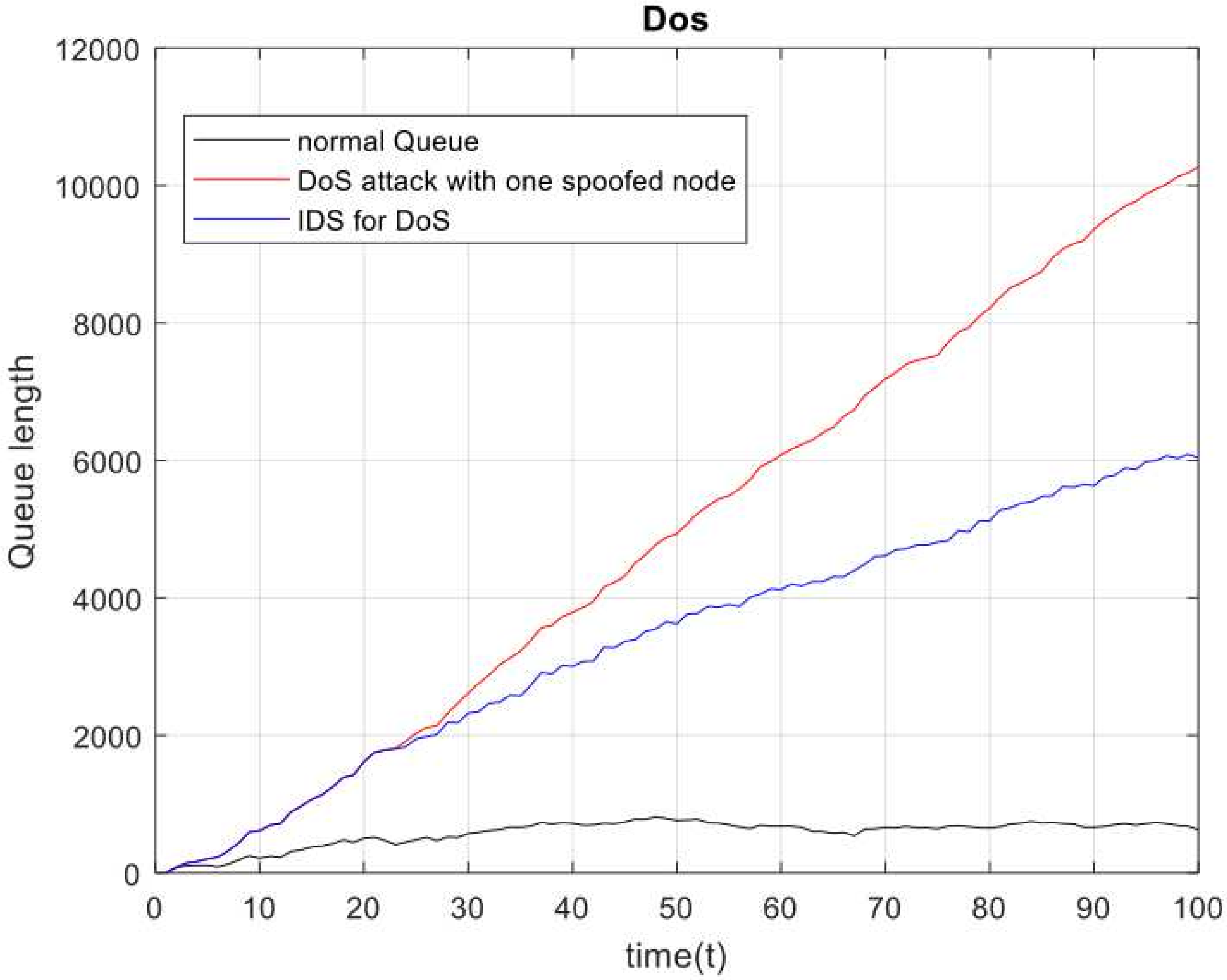


Figure 19

Minimizing queue length for DoS attack using markov chain

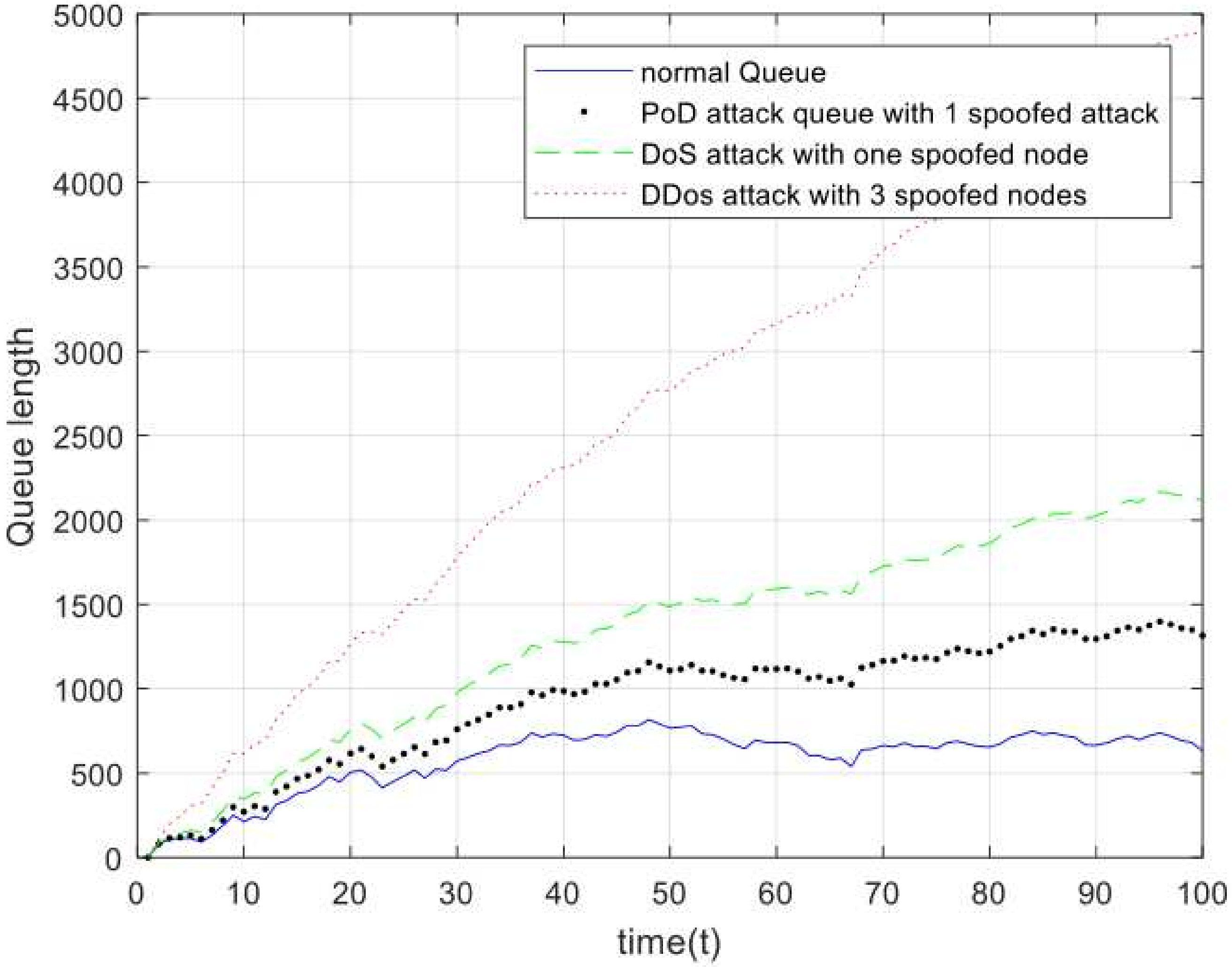


Figure 20

Mitigating queue length for Security threats using markov binomial

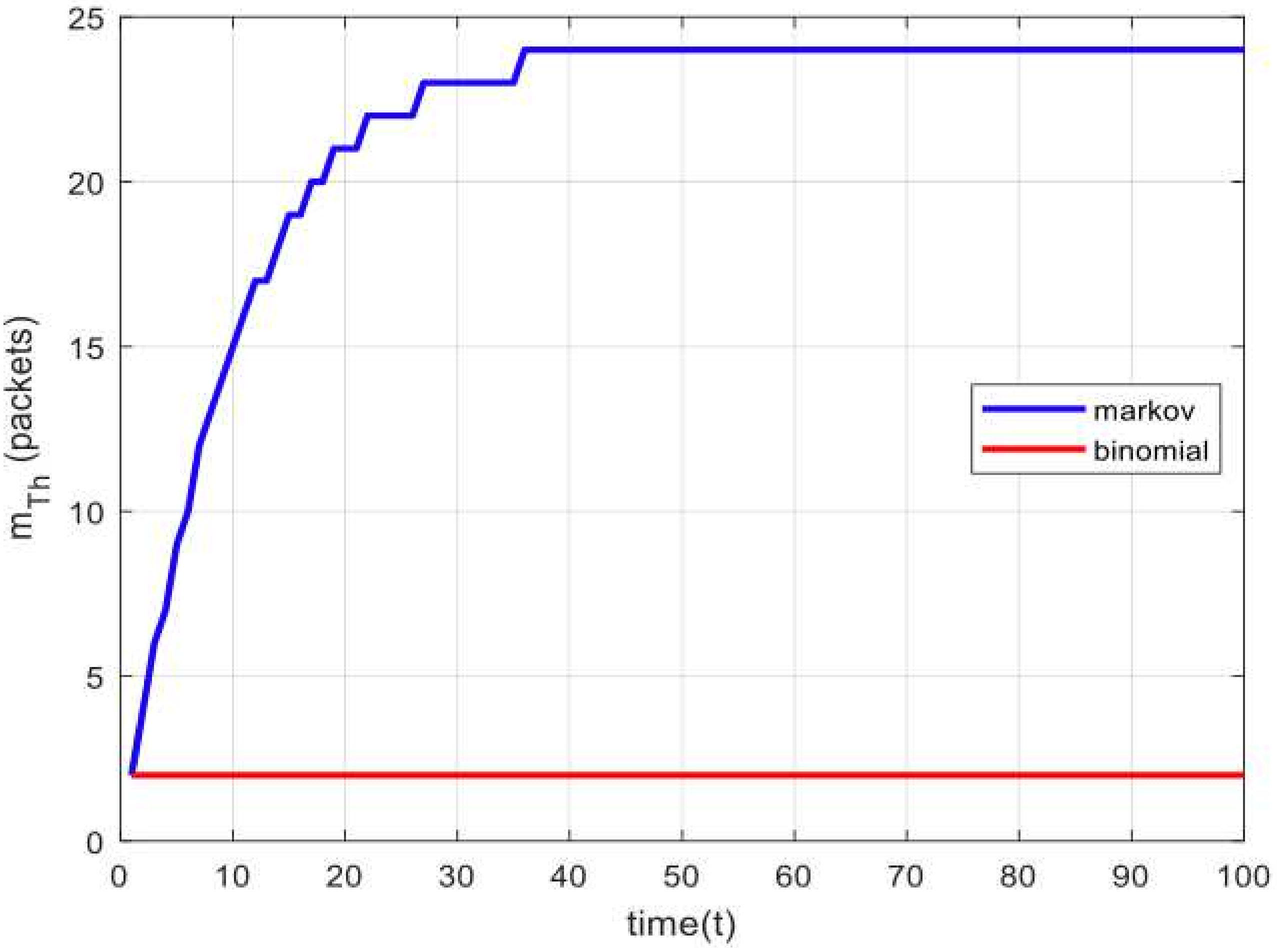


Figure 21

Threshold result of Markov and Binomial distribution

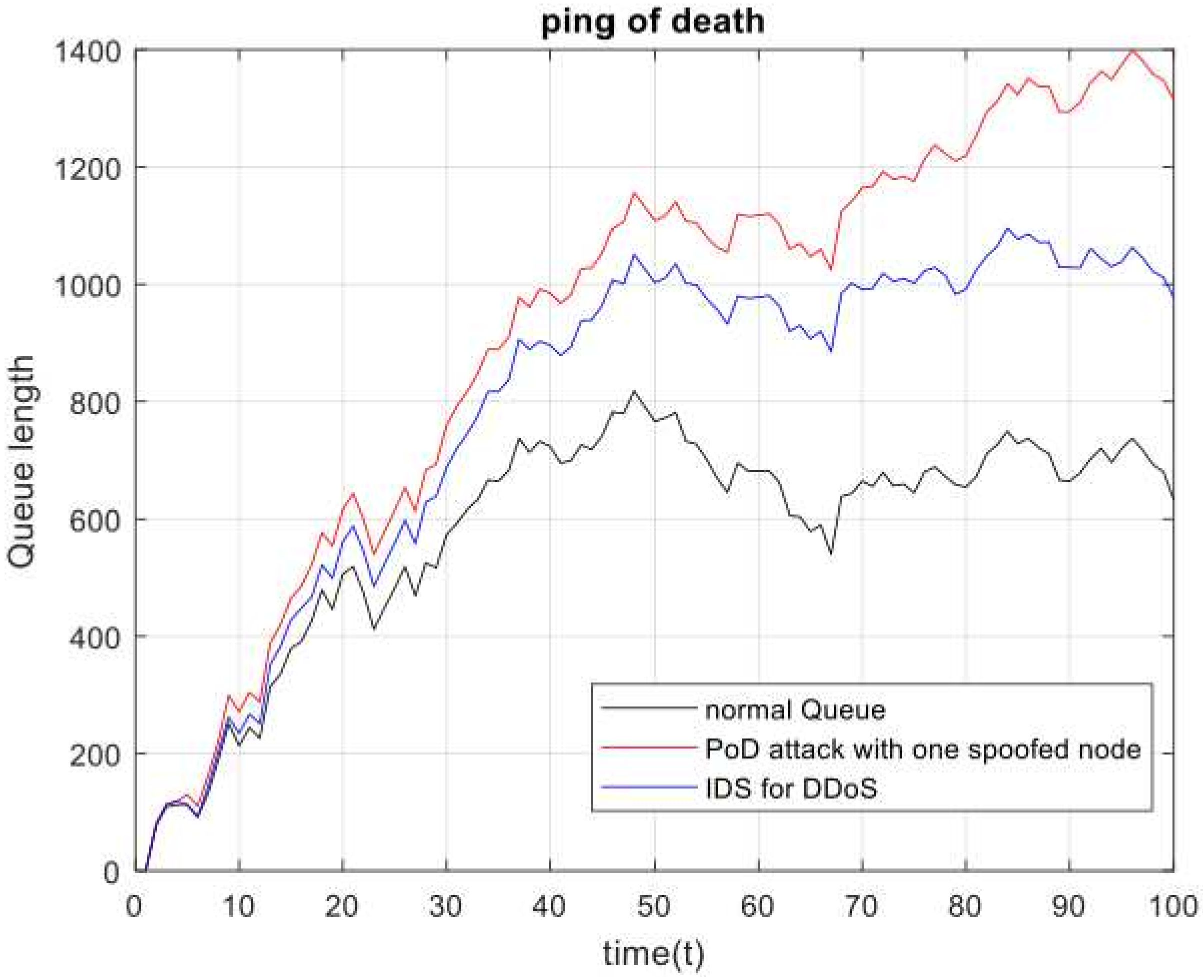


Figure 22

PoD analysis for Queue length making use of Binomial markov

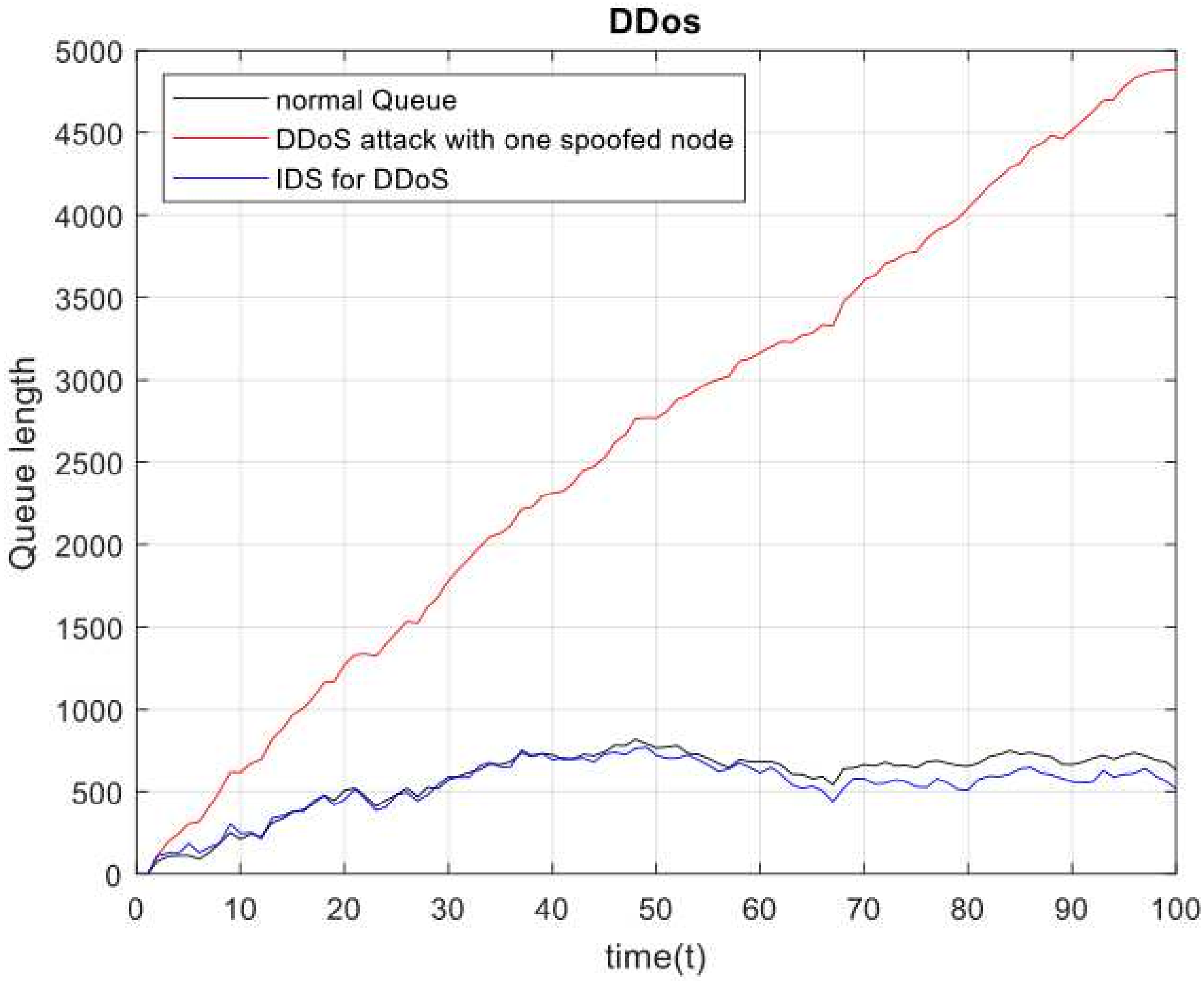


Figure 23

D-Dos study for Queue length employing Binomial markov

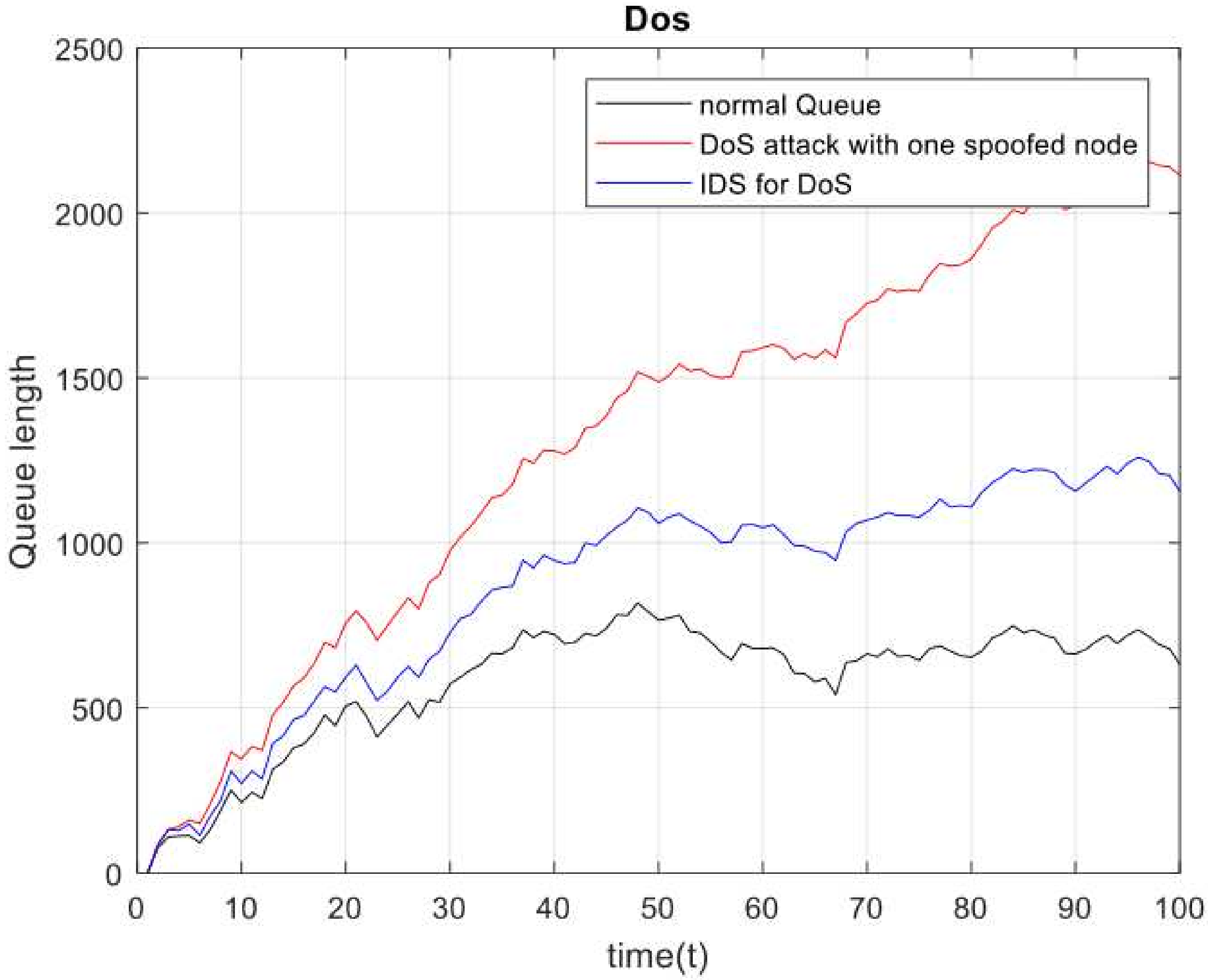


Figure 24

DoS attack queue length using IDS for normal data packets

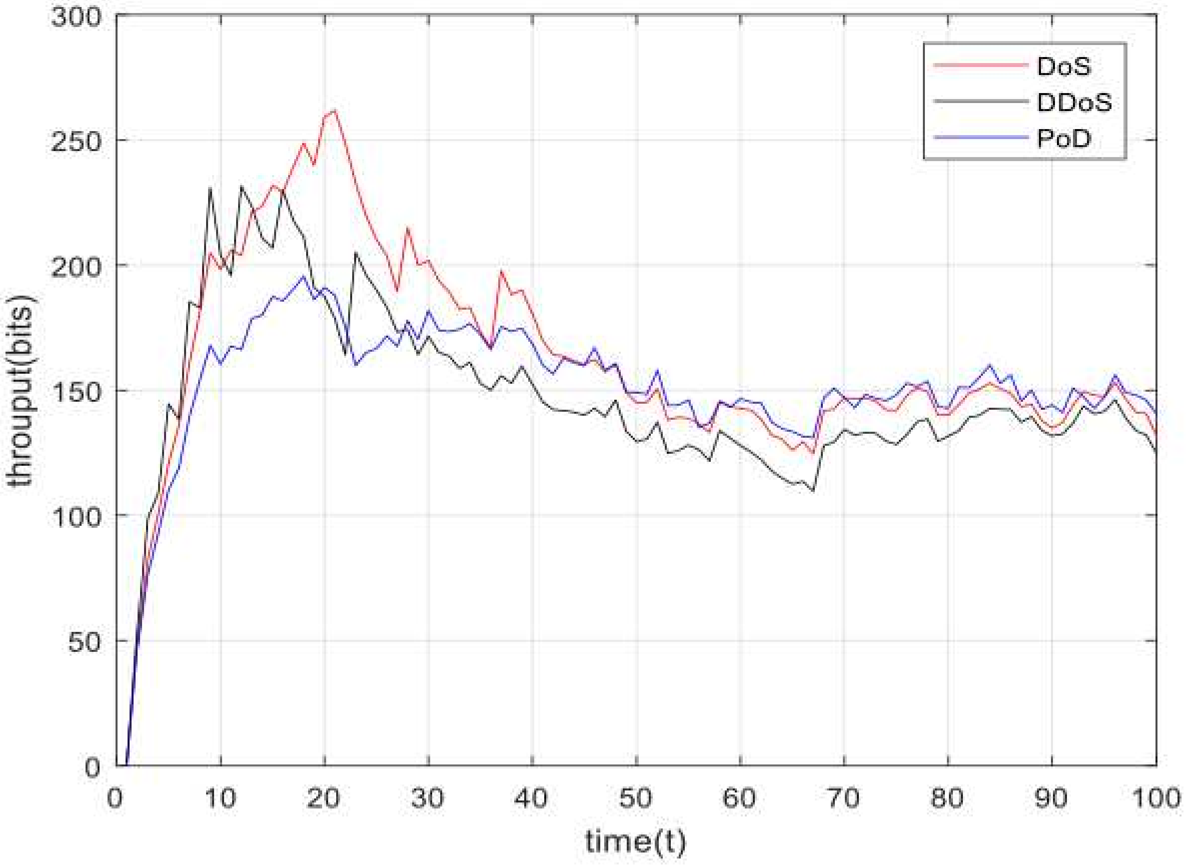


Figure 25

Throughput study of security attacks using Markov Distribution

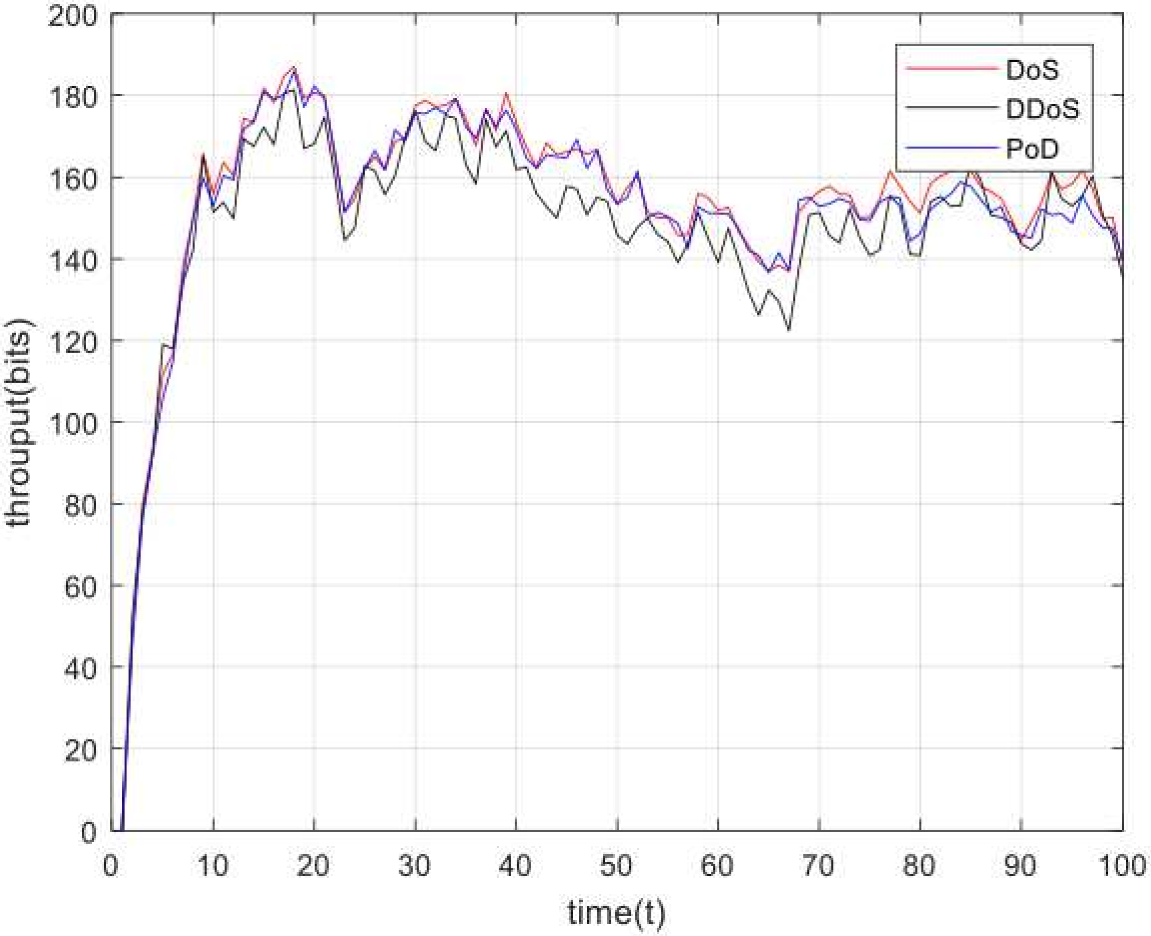


Figure 26

Throughput analysis of cyber threats using Binomial Distribution

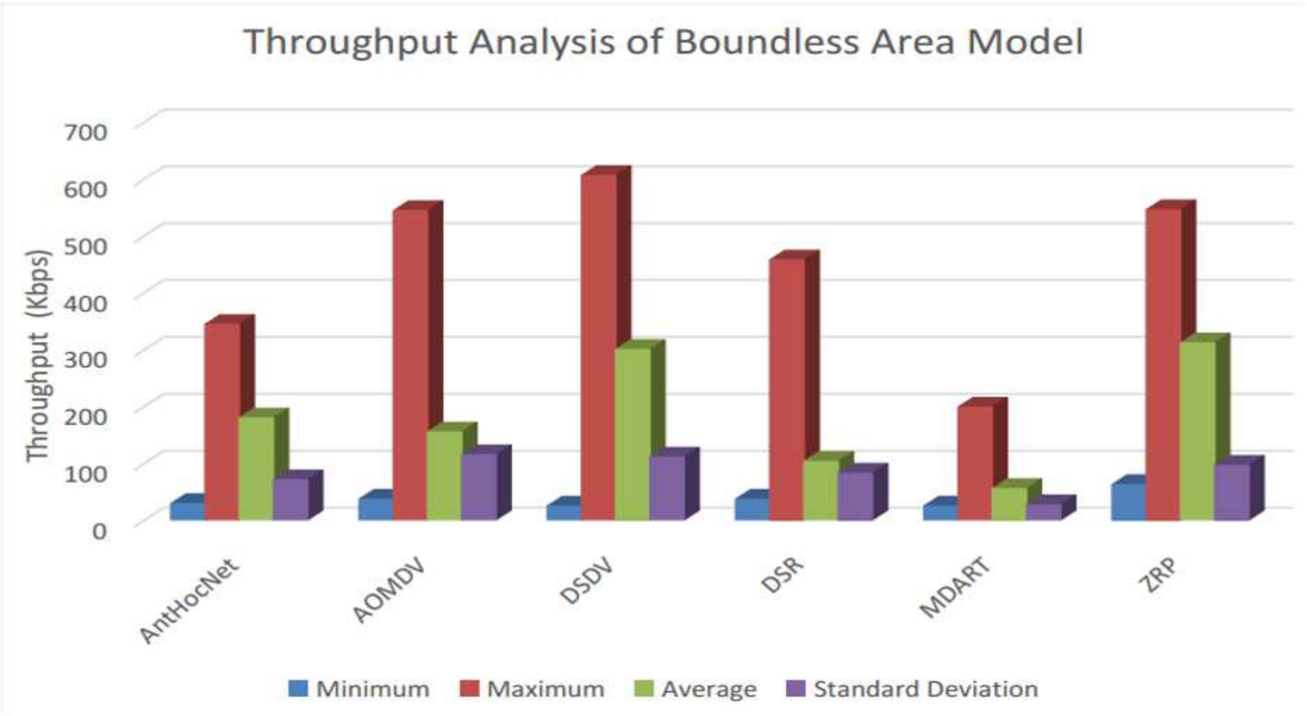


Figure 27

Throughput Analysis AntHocNet with other protocols

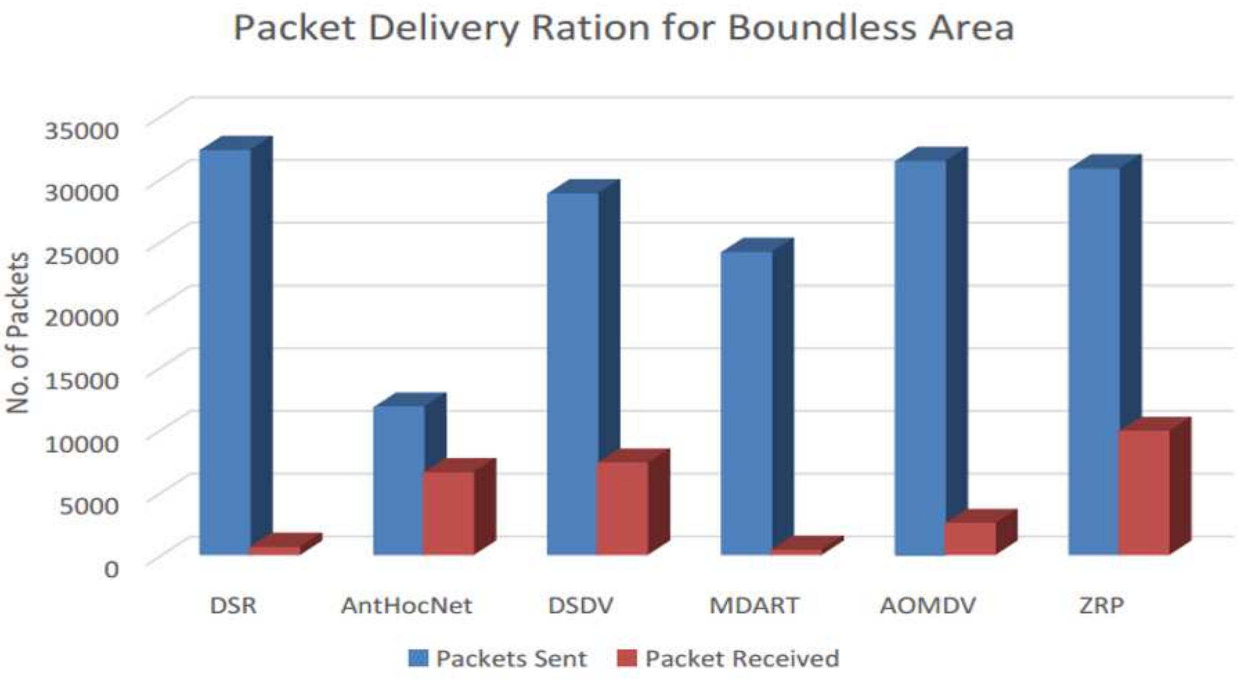


Figure 28

Packet Delivery ratio

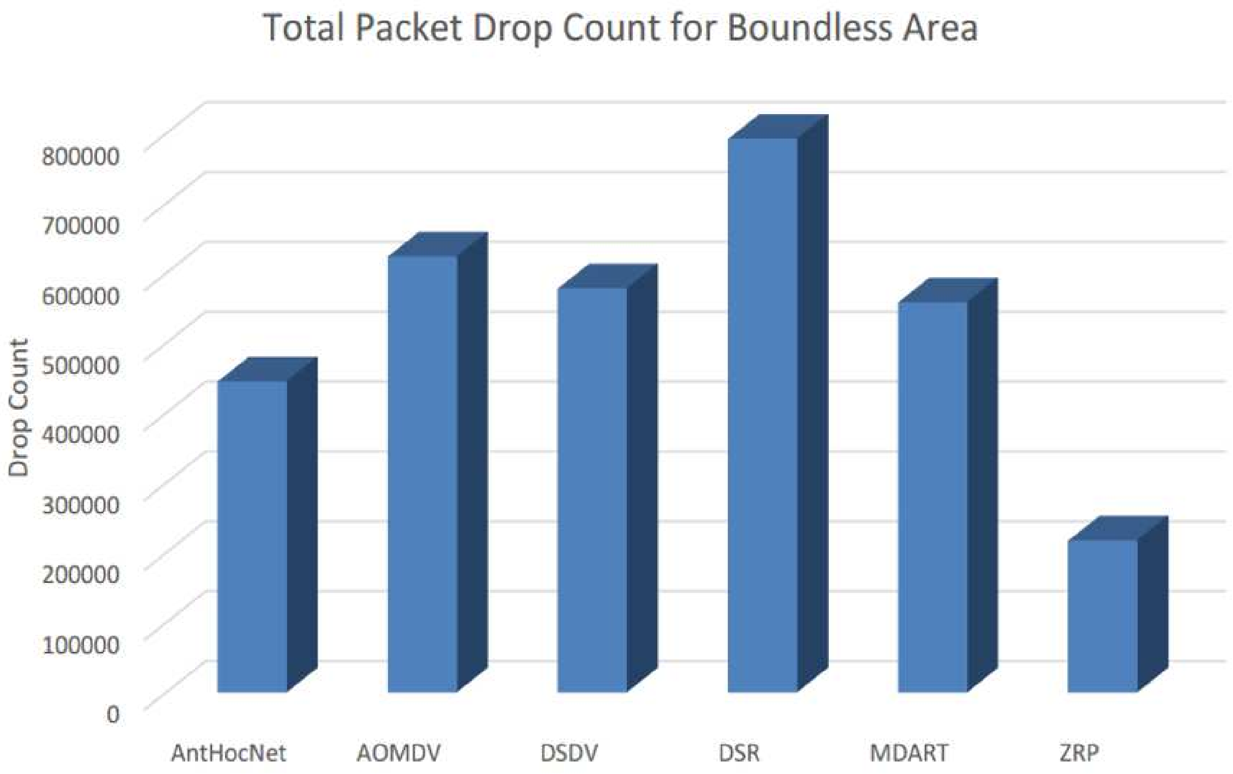


Figure 29

Packet drop count analysis

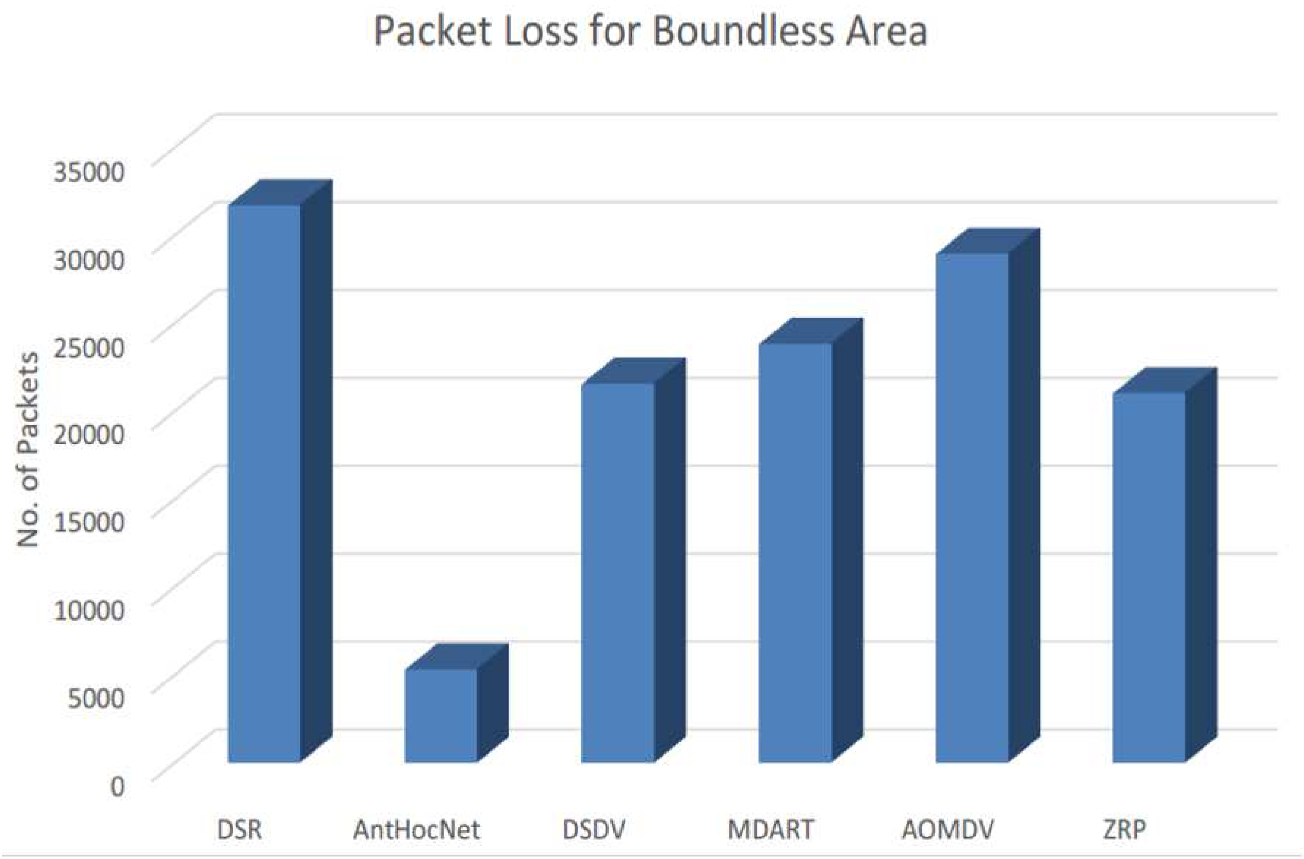


Figure 30

Packet Loss study

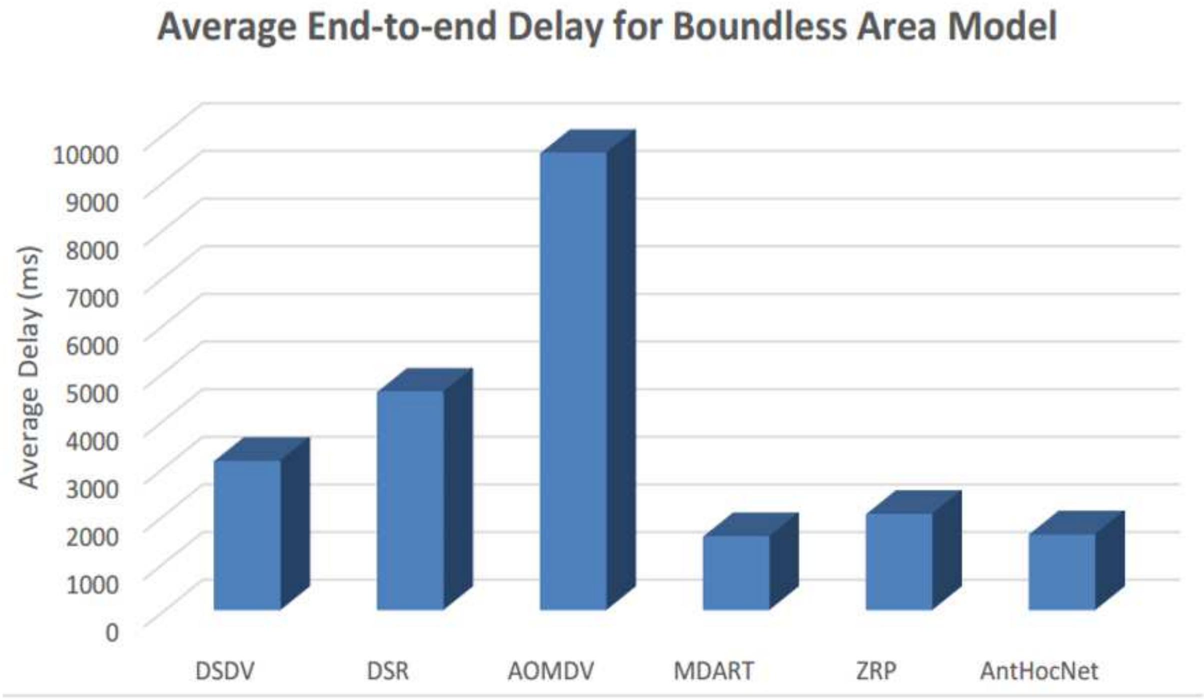


Figure 31

end-to-end delay or jitter