Soft Computing
https://doi.org/10.1007/s00500-019-04573-4

METHODOLOGIES AND APPLICATION

Enhancement of security using optimized DoS (denial-of-service) detection algorithm for wireless sensor network

E. Suryaprabha[1] · N. M. Saravana Kumar[2]

© Springer-Verlag GmbH Germany, part of Springer Nature 2019

Abstract
Wireless sensor networks involved every part of application in today's life. This can detect the various type of information from environment and communicated to users in real time. Information is stored by using cloud technology and that can be accessed by the users. The information is prone to attacks as they are part of cooperative communication. Building algorithms at node level is not secured as they transfer data in open traffic. This has provided scope for this study to concentrate on algorithms that are available for denial-of-service attacks as they put down the network performance to a less minimum. The paper henceforth proposes optimized energy-based constraint DoS (denial-of-service) detection algorithm, i.e., OBES algorithm for handling denial-of-service attacks that learns the network traffic and manages the intruders. This has been compared with denial-of-service attack detection with energy constraint in WSN. The implementation has been done in NS2. The performance has been presented in terms of nodes, interval and lifetime. From results, it can be observed that the proposed OBES algorithm is efficient as it achieves more available energy, less delay, less packet loss and more lifetime for the network. From results, it can be observed that OBES algorithm performs well compared to denial-of-service attack detection with energy constraint algorithm.

Keywords Sensors · Denial of service · Attack · Wireless sensor network

1 Introduction

Wireless sensor network has a set of sensor nodes communicating for a purpose. The sensor nodes have challenges like energy, storage and bandwidth (Chen et al. 2019). They can be used in many applications including military and data communication (Qin et al. 2018). Wireless sensor network suffers from challenges like data security and energy management. They fall with attacks from intruders that are part of the network and outside. This leads to a scenario of attacks that results in false traffic in the network. Building algorithms for them is important as they provide false proof solutions for the network. The voltage as part of the IoT model also affects the energy of the sensor network (Daud et al. 2018).

The attacks are classified into active and passive. The active attacks are hard to handle and challenging. The other type of category is attacks based on network layers and security algorithms. Each layer of attack is specific in functions and challenging (Girish et al. 2016).

Optimized denial of service considers attacks to be in distributed manner. Denial-of-service attack is most vulnerable attack, and it leads to error in many important domains such as health sector, military sector, banking sector and government sector. In DDoS attack, attackers utilize all resource information and it will not allow the authorized user to receive the actual information. The level of attack can span from one to many nodes (Osanaiye et al. 2018). The attack level can increase over time. The manner in which attacks spread is hard to manage and needs some level of analysis over time and traffic (Balaji and Sasilatha 2018). Learning the packet traffic can improve the analysis in a better manner. This is the main scope of the paper.

Communicated by V. Loia.

✉ N. M. Saravana Kumar
saravanakumaar2008@gmail.com

E. Suryaprabha
suryapraba10@gmail.com

[1] Anna University, Chennai, India

[2] Department of Computer Science and Engineering, Vivekanandha College of Engineering for Women, Tiruchengode, India

Published online: 06 December 2019

2 Related work

Chen et al. (2019) analyzed Hilbert–Huang transform, correlation coefficient, Kolmogorov–Smirnov algorithm for a Zigbee network. The performance parameters are RREQ number, time and phase frequency. Osanaiye et al. (2018) proposed immune-based detection system for a wireless sensor network. The performance parameters are detection speed, efficiency, overhead, classification accuracy, false alarm rate and detection time. Balaji and Sasilatha (2018) proposed a school bus routing approach for wireless sensor network. The performance parameters used are throughput, packet loss ratio and packet delivery ratio. Krishnan (2019) proposed a hierarchical clustering approach for Wireless Sensor Network. The performance parameters are number of points, execution time and number of partitions. The packet traffic with growing overhead is an important optimization criterion.

Pareek and Sharma (2018) proposed a dendritic cell algorithm for wireless sensor network. The performance parameters are packet delivery ratio, throughput and end-to-end delay. Sicari et al. (2018) analyzed REATO algorithm for IoT application. The performance parameters are computing effort, latency and recovery time. Wen et al. (2018) proposed a dynamic pricing algorithm for wireless Networked control systems. The performance parameters are channel gain, interference gain, background noise, spreading gain, channel data rate, channel bandwidth and packet bit number. Pu and Song (2018) analyzed RPL routing protocol for wireless sensor networks. The performance parameters analyzed are packet delivery ratio, throughput, energy consumption, number of generated attack packets and attack energy inefficiency. Cao et al. (2019) proposed AccFlow algorithm. The performance parameters analyzed are throughput. Pereira de Almeida et al. (2018) analyzed packet level authentication for wireless sensor networks by considering the number of packets as main factor. Pourazarm and Cassandras (2017) proposed general dynamic battery model for wireless sensor networks considering throughput as main performance parameter. Ma et al. (2017) suggested optimal defense strategy for a packet-dropping wireless sensor network. The contribution is analyzed for different types of transmissions. Optimization is also presented with learning different types of transmissions.

Moser et al. (2019) analyzed distributive interference primer approach for wireless networks. The performance parameters analyzed are transmission power and amplitude error. Chang et al. (2019) proposed threat model for denial of service. The performance parameter analyzed is power transfer. Debayan et al. (2019) proposed cross-device deep learning side-channel attack for ad hoc network. The performance parameters analyzed are accuracy, signal-to-noise ratio. Bashaa et al. (2019) proposed a secret key generation protocol for wireless sensor network. The performance parameter analyzed is throughput. Cheng et al. (2019) proposed the distribution denial-of-service attacks depend on the generalized multiple kernel learning approach. It helps to detect the attacks in complex situation and by calculating the constant parameter R. In result section, parameters will be selected based on the constant parameter and that reduces the error rate and improves the detection rate. Sarwar et al. (2019) implemented the optimized DDoS attacks in software-defined network, and it enhances the network security in IoT environment. Here, attack mitigation scheme developed based on the parameters involved such as scheduling, entropy, time and trust management. Dwivedi et al. (2019) introduced the blockchain technology in IoT healthcare domains to improve security, and it involves secure communication between the users. Aamir and Zaidi (2019) applied machine learning approach in the featured engineering datasets to implement high-security model. This achieves the faster DDoS detection and higher accuracy level in DDoS detection.

From the study, faulty conditions can be due to:

- Node is not working.
- Sensors are transmitting more packets with high energy.
- Sensors have high packet loss.
- Cluster distribution is not uniform.

3 Proposed work

The proposed work enhances the security mechanism for wireless sensor network using optimized DoS (denial-of-service) detection algorithm. The framework will have the following modules:

a. Optimal DoS attack detection.
b. Optimized energy-based security model.

The proposed model consists of the following components:

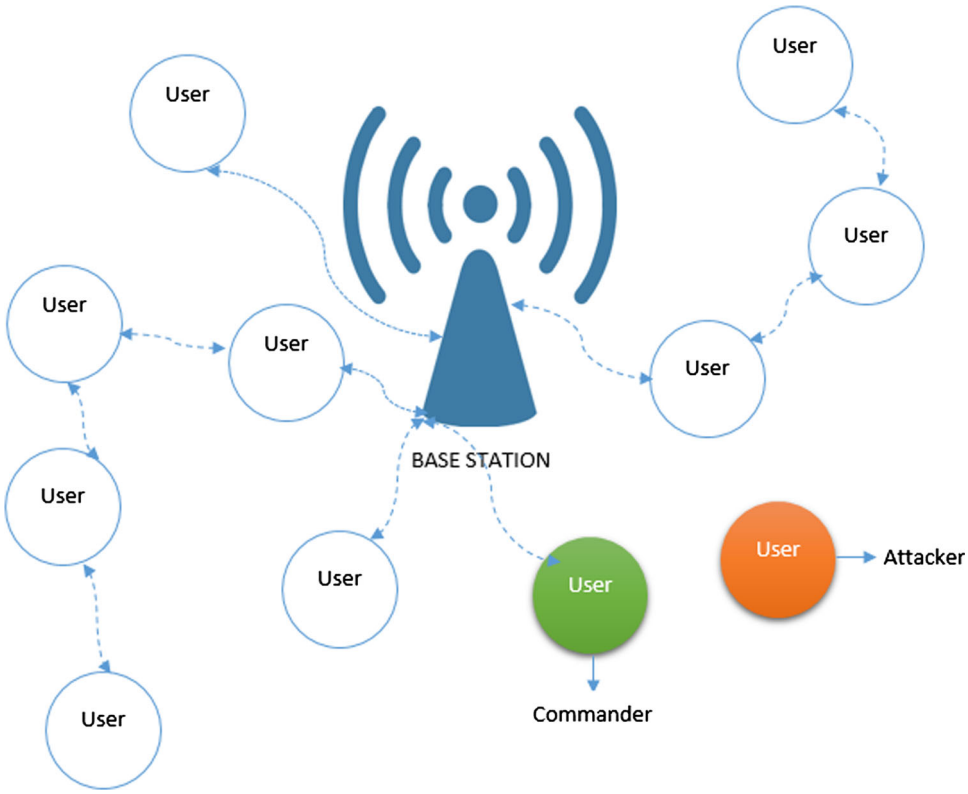
- *Sensor* Devices deployed in the network region to monitor the environmental phenomena.
- *Base Station* Central controller to collect the sensed data.
- *DDoS* Attacker nodes to reduce the QoS in network by transmitting the invalid data.
- *Commander* Central commander for DDoS attacker to probe the falsified data transmission.
- *Packet Dropper* Attacker node to capture and drop the legitimate data to reduce the QoS.

- *Energy Monitoring Unit* On-board unit (OBU) to monitor the energy consumption of each sensor device.
- *Bandwidth Monitoring Unit* OBU to observe the data transmission and corresponding bandwidth consumption. This also has a bandwidth allocator that allocates frequency channels on a needed basis. Each packet is samples with a frequency level based on a sampling frequency.
- *Detection Unit* OBU to identify and differentiate the normal and attacker behavior in the network.

Figure 1 shows the network model of the proposed algorithm. It consists of base station, sensor nodes, attacker and commander. Here, commander helps to detect the attacker and intimate the information of attacker to all users through base station. This will enhance the security mechanism in the proposed approach.

Assume the data transmission and attacker detection process are executed in the WSN environment. By using the random distribution, wireless sensor devices are deployed in the network area. The hello beacon message is broadcasted by sensor device to maintain the neighbor communication. The sensor devices present in the communication region receive the hello message and update the neighbor table entry for the sender of the beacon message. The expired neighbor table entry is updated by using the neighbor timer in each sensor device. Sensor devices sense the environment and initiate the data transmission by signaling the data to the network layer. During the data transmission and forwarding operation, it performs validation for the route availability by searching the routing table entry for the intended destination. The route discovery process is initiated by the source sensor devices if no routing table entry is found for the particular destination. Initially, the devices do not have path to reach the destination if it is not found in the neighbor table. During the route discovery process, source node sends the RREQ message as network-wide broadcast message. The receiver node for the RREQ message validates the control message for the following constraints: packet freshness by checking the sequence number and routing loop by checking the sender id. The control message can handle the attack nature and route the traffic accordingly. Upon successful validation, the intermediate devices add/update the reverse routing table entry for the source node and rebroadcast the RREQ message to its neighbor nodes. Once the message reached the destination, it sends the RREP message to unicast message to the source node using the reverse path constructed during the RREQ forwarding process. During the RREP forwarding operation, routing table entry for the destination is updated. The routing table can be formed based on the new path. This can help in learning the attack behavior in the network.

Fig. 1 Network model



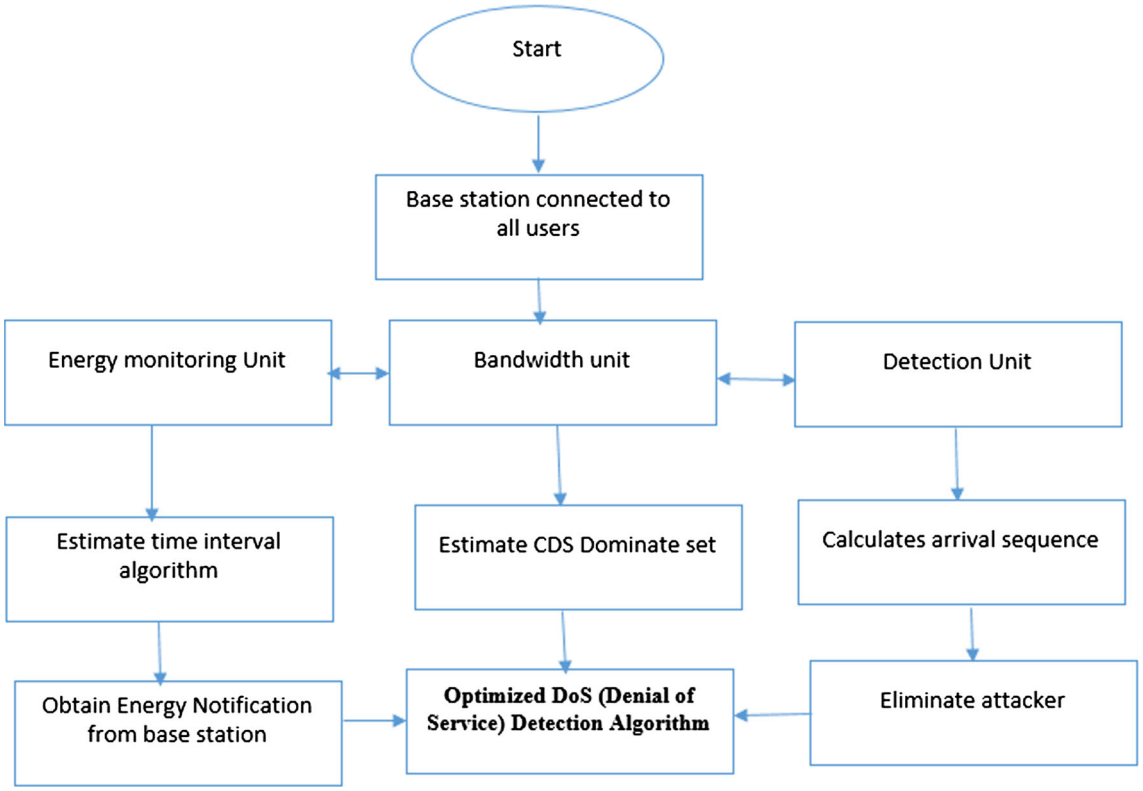


Fig. 2 Structural procedure of the proposed algorithm

Figure 2 shows the structural procedure of the proposed algorithm. It consists of three different units such as energy monitoring unit, bandwidth unit and detection unit. These three units estimate the time interval, CDS dominating set and arrival sequence, respectively. The proposed optimized denial-of-service attack detection algorithm resumes energy consumption, utilizes more bandwidth and eliminates the attacker.

3.1 Optimized attack detection procedure

The data transmission is considered as the linear time invariant, and the transmission information is identified by the sensor devices. The transmission model is represented with the zero mean and the Gaussian noise in the LTI. The equality for the transmission is defined in both attacker probability and normal probability. Packet dropout DoS policy and the transmission policy are provided from the attacker probability and normal probability, respectively. The policies are defined by considering the data transmission in terms of Bernoulli process. The probability distribution in the Bernoulli process is indicated as follows:

$$\text{Bernoulli distribution} = (1 - \text{lambda}) * (1 - \text{alpha}) + \text{lambda} * (1 - \text{beta}) \quad (1)$$

where lambda = weighting parameter, alpha = packet dropout probabilities under the DoS attack, and beta = packet dropout probabilities in the absence of attack.

The remote estimator for the data transmission is estimated from the transmission power, transmission gain of the sensor and attacker as follows:

$$\text{Remote estimator} = \text{del_s} * G_\text{s}/(\text{del_a} * G_\text{a} + \text{del2}) \quad (2)$$

where del_s = transmission power of sensor, del_a = transmission power of attacker, G_s = transmission gain of sensor, G_a = transmission gain of attacker, and del2 = noise power.

The remote estimation limit is dependent on the transmission power of sensor. From the calculated remote estimator, the integrated value over the negative exponential distribution with the second order is estimated to compute the initial value of the packet arrival probability.

$$Q_x = 1./\text{sqrt}((2 * M_\text{PI})) * 2 * \text{prob} * \exp(-\text{pow}(\text{prob}, 2)); \quad (3)$$

By using the exponential convergence in the steady-state data transmission operation, the packet arrival probability is computed.

$$p = (1 - Q_x); \quad (4)$$

The estimated values are organized into the array list, and error covariance is estimated from the values of the mean, difference sum, variance and standard deviation.

$$\text{diffSum} = \Sigma\text{sqrt}\ (\text{pow}((\text{avg} - \text{expected value}), 2)); \quad (5)$$

The estimated covariance and the corresponding probability are organized into the *n*-size column vector. From the organized probability values, the arrival sequence for the attacker strategy is based on the deviation degree of the attack strategy.

$$J = 1/T * \Sigma\text{prob_in_column_vector} * \Sigma\text{prob_in_row_vector} \quad (6)$$

Based on the arrival sequence of the data transmission, the final consecutive probability of the attacker is calculated and the corresponding nodes are eliminated from the network.

3.2 Optimized energy-based security model

The sensor device is equipped to monitor the resource with two periodical timer, namely energy monitoring timer and bandwidth timer. The energy monitoring timer validates the unit energy consumption to compute the average lifetime of the device as well as minimum lifetime of the device. The lifetime of the sensor node based on energy consumption is validated by the unit energy consumption. The unit energy consumption is computed as follows:

$$\text{Unit_consumption} = \text{CURRENT_TIME}/\text{energy_consumed} \quad (7)$$

$$\text{Energy}_{\text{consumed}} = \text{Initial Energy} - \text{Current Energy} \quad (8)$$

$$\text{Average lifetime} = \text{Unit_consumption} * \text{Initial Energy} \quad (9)$$

Distributed energy consumption is applied by the periodical monitoring of available energy in each time period. The energy difference in each consecutive time interval is estimated, and the corresponding average value is calculated for the distributed energy consumption.

Time interval algorithm:

$sum = 0;$
$for(i = 0; i < (ecount - 1); i++)$
$\{$
$sum+ = (energyLevel[i] - energyLevel[i + 1]);$
$\}$
$Avg = sum/(ecount - 1)$
$energyLevel[i] = remaining\ energy\ in\ each\ energy\ level$
$ecount = no\ of\ energylevel$

The difference sum of the average energy level and the difference of consecutive remaining energy are computed with the square root of second-order power. The variance and the standard deviation are estimated from the difference sum value by ecount dividing and square root of the divided value, respectively. The upper bound expected value for the energy consumption with the maximum distributed deviation is estimated by merging the average difference and the standard deviation. The distributed unit energy consumption is computed as follows:

$$\text{Distributed Unit Consumption} = (\text{Monitoring_interval}/\text{upperBound}); \quad (10)$$

Distributed minimum lifetime of the sensor node is estimated by using the following,

$$\text{Distributed Lifetime} = \text{distributed Unit Consumption} * \text{Initial_Energy} \quad (11)$$

The weighted lifetime is estimated by merging the average lifetime and the distributed lifetime with the corresponding weight values. If the energy of the node is completely reduced with the short period, then the sensor node intimates the energy consumption by sending the energy notification message to the base station. The centralized communication is initiated by the base station by sending the base station announcement. The BS announcement is network-wide broadcast message which is received and rebroadcasted by sensor nodes in the network until reaching all devices. The sensor devices receive the broadcast message and store the information about base station id. The sensor device sends its own information such as location coordinates, the energy consumption and the available bandwidth of the device. The information is collected and maintained in the table which is used to divide the network into optimal connected dominating set. Instead of collecting the information periodically by sending the announcement, the broadcast requirement is validated for all sensors which reduce the energy consumption. The broadcast requirement is validated by checking the uniform distributed energy consumption of the device which is used to compute the average lifetime. The estimation of the average lifetime is similar to the energy monitoring computation of the sensor with the consideration of the each sensor device. The broadcast requirement is also validated by checking the reception of the energy notification message of the sensor. After receiving the information about all sensor nodes in the network, the BS starts forming the connected dominating set. The set formation is done with the assistance of the optimal selection criteria by computing the CDS probability.

3.3 Steps of optimal CDS probability algorithm

The optimal CDS probability is estimated from the following constraints: connection probability and forwarding probability. Connection probability is estimated by neighbor degree, unit energy requirement, EWMA value of the energy consumption and EWMA value consumption. The forwarding probability is estimated from the normalized forwarding distance and forwarding energy and bandwidth consumption.

1. Neighbor degree = No. of neighbor of the sensor/Total no. of sensor in the network
2. Unit Energy Requirement = Sum of (Energy consumption for unit data transmission + Energy consumption for unit data reception)
   in the set connection with the neighborhood communication.
3. EWMA_Energy = w1 * current_energy/initial_energy + w2 * average_energy_consumption
4. EWMA_Bandwidth = w1 * current_bandwidth/System BW + w2 * average_bandwidth_consumption
5. Connection_Probability = alpha1 * Neighbor degree + alpha2 * Unit Energy Requirement + alpha3 * EWMA_Energy + alpha4 * EWMA_Bandwidth.
6. Normalized forwarding distance = maximum distance between sensor and base station/Topology distance
7. Forward Energy Requirement = Sum of (Energy consumption for forwarding the data to BS + Energy consumption for data reception by intermediate devices)
   in the set connection with the forwarding route of the destination.
8. Forward BW Requirement = Sum of BW consumption for forwarding the data to BS and BW consumption
   for data reception by intermediate devices.
9. Forwarding probability = beta1 * Normalized forwarding distance + beta2 * Forward Energy Requirement + beta3 * Forward BW Requirement
10. CDS_Prob = delta1 * Connection_Probability + delta2 * Forwarding probability

Optimal metric of CDS_Prob is being evaluated for learning the traffic nature. The model results are presented in Sect. 4 of the paper.

4 Results and discussion

The proposed optimized DoS (denial-of-service) detection algorithm is being implemented in NS2. It is compared with the denial-of-service attack detection with energy constraint in WSN using the proposed framework discussed in Sect. 3.

The runtime environment is set up with the following parameters:

The graph marked OBES_BA and OBES_AA indicates the optimized DoS (denial-of-service) detection algorithm (OBES) before attackers and after attacker detection, respectively, and ODSA_BA and ODSA_AA indicate the off-loading denial-of-service attack detection (ODSA) before attackers and after attacker detection, respectively.

From Fig. 3, it can be observed that throughput is high for OBES algorithm before and after attack detection compared to the off-loading denial-of-service attack detection (ODSA). High throughput achieves the high scalability in network and provides the high goodput for OBES algorithm. The users will have high quality of

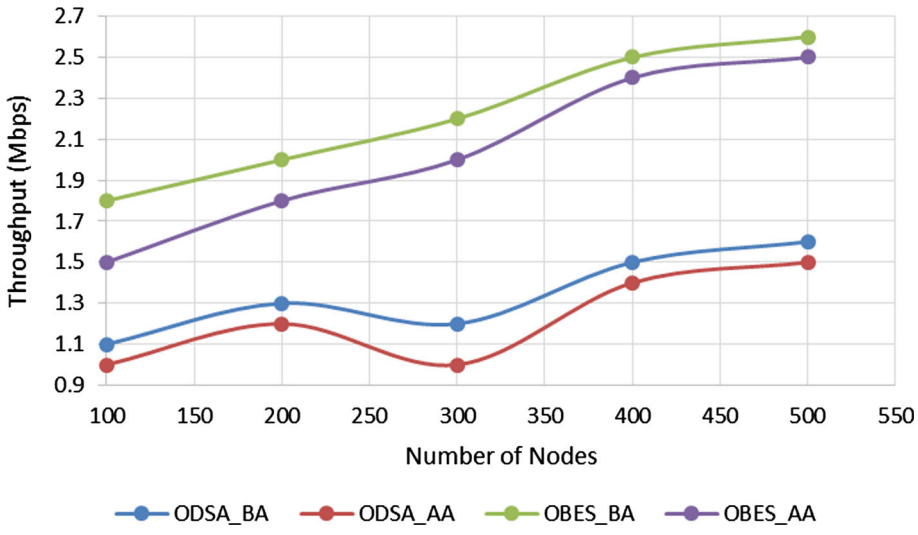


Fig. 3 Throughput analysis

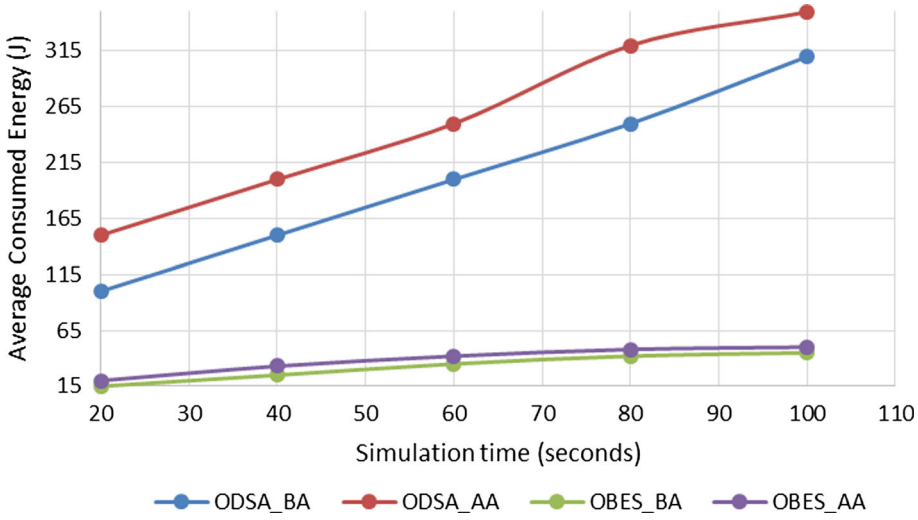


Fig. 4 Time versus average consumed energy

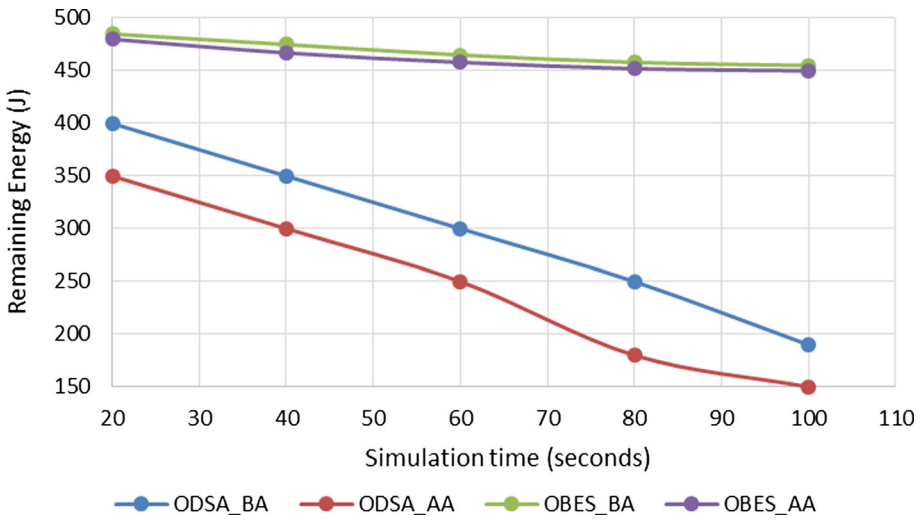


Fig. 5 Time versus average remaining energy

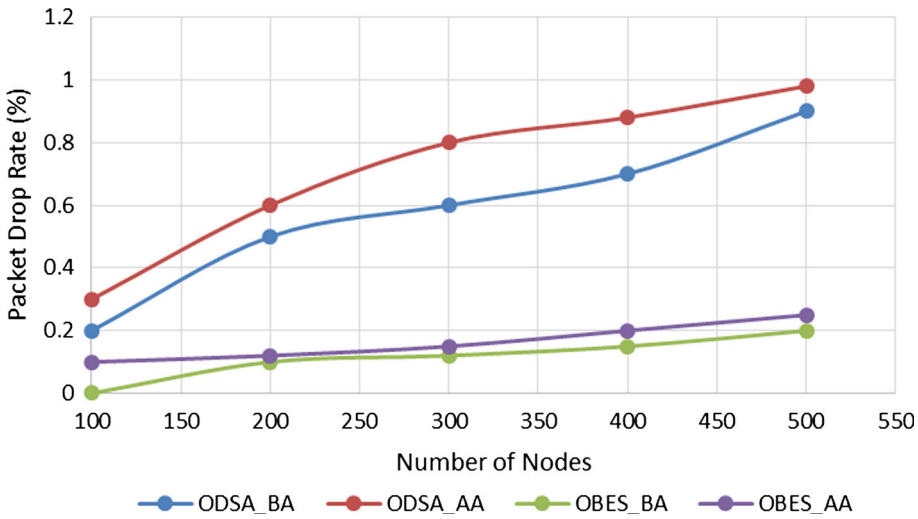


Fig. 6 Packet drop rate analysis

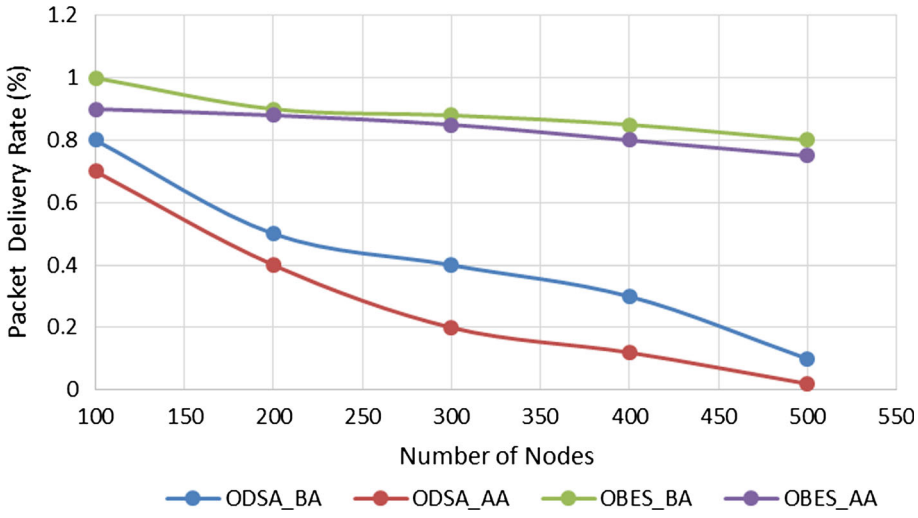


Fig. 7 Packet delivery rate analysis

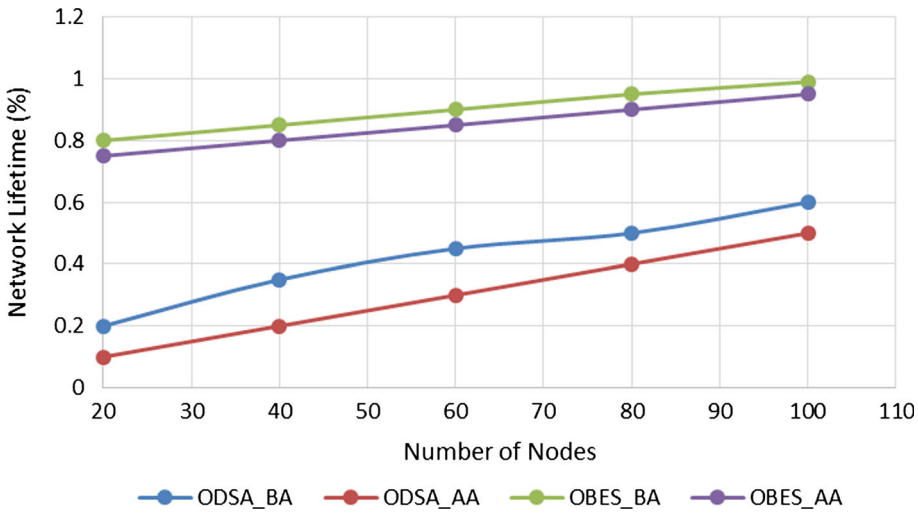


Fig. 8 Network lifetime analysis

Table 1 Simulation setup

Parameter	Value
No. of nodes	500 (sensor) + 1 (BS)
Mac type	Sensor Mac with base standard IEEE 802.11
Queue type	Priority queue
Coverage area	80 m
Topology area	500 × 500
Antenna type	Omni directional
Packet size	512
Connection type	UDP
Application type	Sensor (temperature)
Packet generation interval	0.1, 0.15, 0.2, 0.25, 0.3
Data rate	3 mbps
Simulation time	100–200 s
No. of attacker	5 (DDoS) + 1 (dropper)
Initial energy	500 J

Table 2 Number of nodes versus different parameters

Parameters	Throughput				Drop rate				Delivery ratio			
Nodes	ODSA_BA	ODSA_AA	OBES_BA	OBES_AA	ODSA_BA	ODSA_AA	OBES_BA	OBES_AA	ODSA_BA	ODSA_AA	OBES_BA	OBES_AA
100	1.1	1	1.8	1.5	0.8	0.7	1	0.9	0.8	0.7	1	0.9
200	1.3	1.2	2	1.8	0.5	0.4	0.9	0.88	0.5	0.4	0.9	0.88
300	1.2	1	2.2	2	0.4	0.2	0.88	0.85	0.4	0.2	0.88	0.85
400	1.5	1.4	2.5	2.4	0.3	0.12	0.85	0.8	0.3	0.12	0.85	0.8
500	1.6	1.5	2.6	2.5	0.1	0.02	0.8	0.75	0.1	0.02	0.8	0.75

Table 3 Simulation time versus different parameters

Parameters	Network lifetime				Average consumed energy				Average remaining energy			
Simulation time	ODSA_BA	ODSA_AA	OBES_BA	OBES_AA	ODSA_BA	ODSA_AA	OBES_BA	OBES_AA	ODSA_BA	ODSA_AA	OBES_BA	OBES_AA
20	0.2	0.1	0.8	0.75	100	150	15	20	400	350	485	480
40	0.35	0.2	0.85	0.8	150	200	25	33	350	300	475	467
60	0.45	0.3	0.9	0.85	200	250	35	42	300	250	465	458
80	0.5	0.4	0.95	0.9	250	320	42	48	250	180	458	452
100	0.6	0.5	0.99	0.95	310	350	45	50	190	150	455	450

transmission and less jitter. This means that the network provides less error during data transmission. The users will have high reliable transmission in wireless sensor network.

Figure 4 shows the average consumed energy for proposed and existing approach with before and after attack detection models. Energy consumption is very low in the proposed OBES algorithm compared to the existing ODSA algorithm. It provides long network lifetime.

From Fig. 5, it can be observed that relationship of internal time versus average energy is less for OBES algorithm. This means that the network has less energy utilization, and it provides the total remaining energy is high for OBES algorithm. It allows more users to communicate in the wireless sensor network.

From Fig. 6, it can be observed that relationship of number of nodes versus packet drop rate is very low for OBES algorithm with before and after attacker detection compared to existing ODSA algorithm. This means that if the network provides less packet loss, the reliability of the network is improved. This implies that reliability of data being transferred is high using OBES algorithm.

Figure 7 shows the packet delivery rate, and it is defined as the ratio of successful packet delivered to the transmitted. The proposed OBES algorithm provides high packet delivery ratio in both the before and after attacker detection models. This improves the overall network performance.

From Fig. 8, it can be observed that lifetime is high for OBES algorithm even before and after the attacker detection models. This means that the network will have more lifetime. Based on the energy level obtained in the network model, network lifetime can be calculated. The proposed OBES algorithm provides the high network lifetime.

Tables 1 and 2 show the comparison table with parameters versus number of nodes and simulation time, respectively. By varying number of nodes, high throughput, less drop rate and high packet delivery ratio are achieved. By varying interval time, less energy consumption, high remaining energy and high network lifetime are achieved. This implies that lifetime of the network is high using OBES algorithm. From the graphs, it can be observed that the varying packet traffic is optimally learnt using the proposed algorithm—optimized DoS (denial-of-service) detection algorithm (Table 3).

5 Conclusion

This research work analyzed the performance of the proposed optimized energy-based constraint DoS (denial-of-service) detection algorithm, i.e., OBES algorithm with three different modules such as bandwidth, energy and attacker detection unit, and it is compared with the existing off-loading denial-of-service attack detection with energy constraint in WSN. This proposed work was implemented by using network simulator. From the simulation results, it can be observed that the proposed OBES algorithm is efficient as it provides more available energy, less delay, less packet loss and more lifetime for the network. The proposed OBES algorithm achieves high network lifetime in both before and after attack detection models. The proposed OBES algorithm helps to achieve less energy consumption, high security and high network lifetime in wireless sensor network. The proposed algorithm can be extended in future for understanding scalability of encryption algorithms for handling attacks for large category of users. The network can also be extended with clustering by isolating the clusters and classifying the type of attack.

Acknowledgements This research is not supported by any funding.

Compliance with ethical standards

Conflict of interest The authors declare that they have no conflict of interest.

Human participants and/or animal This article does not contain any studies with human participants or animals performed by any of the authors.

Informed consent All referred study is highlighted in the literature review.

References

Aamir M, Zaidi SMA (2019) DDoS attack detection with feature engineering and machine learning: the framework and performance evaluation. Int J Inf Secur 18(6):1–25

Balaji S, Sasilatha T (2018) Detection of denial of service attacks by domination graph application in wireless sensor networks. Clust Comput 6:1–6

Bashaa MH, Al-Alak SM, Idrees AK (2019) Secret key generation in wireless sensor network using public key encryption. In: Proceedings of the international conference on information and communication technology, pp 106–112

Cao Y et al (2019) AccFlow: defending against the low-rate TCP DoS attack in wireless sensor networks. arXiv:1903.06394

Chang S-Y, Kumar SL, Hu Y-C, Park Y (2019) Power-positive networking: wireless-charging-based networking to protect energy against battery DoS attacks. ACM Trans Sensor Netw 15(3):27

Chen H et al (2019) A novel low-rate denial of service attack detection approach in zigbee wireless sensor network by combining Hilbert–Huang transformation and trust evaluation. IEEE Access 7:32853–32866

Cheng J, Li J, Tang X, Sheng VS, Zhang C, Li M (2019) A novel DDoS attack detection method using optimized generalized multiple kernel learning. arXiv:1906.08204

Daud M, Rasiah R, George M, Asirvatham D, Rahman AFA, Halim AA (2018) Denial of service: (DoS) impact on sensors. In: 2018 4th international conference on information management (ICIM), Oxford, 2018, pp 270–274

Debayan D, Golder A, Danial J, Ghosh S, Raychowdhury A, Sen S (2019) X-DeepSCA: cross-device deep learning side channel attack. In: Proceedings of the 56th annual design automation conference, pp 1–6

Dwivedi AD, Malina L, Dzurenda P, Srivastava G (2019) Optimized blockchain model for internet of things based healthcare applications. arXiv:1906.06517

Girish SV, Prakash R, Swetha SNH, Pareek G, Kumar TS (2016) A network model of GUI-based implementation of sensor node for indoor air quality monitoring. In: Advances in intelligent systems and computing published—Springer, 2016—from the proceedings of international conference ICSCS 2015, vol 397, pp 209–217,. ISBN: 978-81-322-2669-7 (Print) 978-81-322-2671-0 (Online)

Krishnan SSN (2019) Denial of service (DoS) detection in wireless sensor networks applying geometrically varying clusters. In: International conference on computer networks and communication technologies. Springer, Singapore

Ma W, Wu Y, Gong M, Qin C, Wang S (2017) Local probabilistic matrix factorization for personal recommendation. In: 2017 13th international conference on computational intelligence and security (CIS). Hong Kong, pp 97–101

Moser D, Lenders V, Capkun S (2019) Digital radio signal cancellation attacks: an experimental evaluation. In: Proceedings of the 12th conference on security and privacy in wireless and mobile networks, pp 23–33

Osanaiye OA, Alfa AS, Hancke GP (2018) Denial of service defence for resource availability in wireless sensor networks. IEEE Access 6:6975–7004

Pareek S, Sharma PK (2018) Denial of service attack detection by enhanced dendritic cell algorithm. In: 2018 3rd international conference and workshops on recent advances and innovations in engineering (ICRAIE). IEEE

Pereira de Almeida M et al (2018) New DoS defense method based on strong designated verifier signatures. Sensors 18(9):2813

Pourazarm S, Cassandras CG (2017) Energy-based lifetime maximization and security of wireless-sensor networks with general nonideal battery models. IEEE Trans Control Netw Syst 4(2):323–335

Pu C, Song T (2018) Hatchetman attack: a denial of service attack against routing in low power and lossy networks. In: 2018 5th IEEE international conference on cyber security and cloud computing (CSCloud)/2018 4th IEEE international conference on edge computing and scalable cloud (EdgeCom). IEEE

Qin J, Li M, Shi L, Yu X (2018) Optimal denial-of-service attack scheduling with energy constraint over packet-dropping networks. IEEE Trans Autom Control 63(6):1648–1663

Sarwar MA, Hussain M, Anwar MU, Ahmad M (2019) FlowJustifier: an optimized trust-based request prioritization approach for mitigation of SDN controller DDoS attacks in the IoT paradigm. In: Proceedings of the 3rd international conference on future networks and distributed systems. ACM, p 43

Sicari S et al (2018) REATO: REActing TO denial of service attacks in the internet of things. Comput Netw 137:37–48

Wen W, Wen X, Yuan L, Xu H (2018) Range-free localization using expected hop progress in anisotropic wireless sensor networks. EURASIP J Wirel Commun Networking 2018:299

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.