Intelligent Automation & Soft Computing
DOI:10.32604/iasc.2022.022151
Article

Tech Science Press

Novel DoS Attack Detection Based on Trust Mode Authentication for IoT

D. Yuvaraj[1], S. Shanmuga Priya[2,*], M. Braveen[3], S. Navaneetha Krishnan[4], S. Nachiyappan[5], Abolfazl Mehbodniya[6], A. Mohamed Uvaze Ahamed[7] and M. Sivaram[8]

[1]Department of Computer Science and Engineering, Cihan University, Duhok, Kurdistan Region, Iraq
[2]Department of Computer Science and Engineering, M.I.E.T Engineering College, Trichy, Tamilnadu, India
[3]School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, India
[4]Department Electronics and Communication Engineering, SACS MAVMM Engineering College, Madurai, Tamilnadu, India
[5]School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, India
[6]Department of Electronics and Communications Engineering, Kuwait College of Science and Technology (KCST), Kuwait
[7]Department of Information Technology, Qala University College, Erbil, Kurdistan Region, Iraq
[8]Research Center, Labanese French University, Erbil, Iraq
*Corresponding Author: S. Shanmuga Priya. Email: priya501@gmail.com
Received: 29 July 2021; Accepted: 09 December 2021

Abstract: Wireless sensor networks are extensively utilized as a communication mechanism in the field of the Internet of Things (IoT). Along with these services, numerous IoT based applications need stabilized transmission or delivery over unbalanced wireless connections. To ensure the stability of data packets delivery, prevailing works exploit diverse geographical routing with multi-hop forwarders in WSNs. Furthermore, critical Denial of Service (DoS) attacks frequently has an impact on these techniques, where an enormous amount of invalid data starts replicating and transmitted to receivers to prevent Wireless Sensor Networks (WSN) communication. In this investigation, a novel adaptive endorsement method is designed by combining dimensionality reduction based Hilbert-Huang Transformation (DR-HHT) and authentication trust mode (ATM). DR-HHT and ATM defend against the severity of DoS attacks, by fulfilling trust, reliability, stability requirements. ATM also examines the state information (SI) of nodes in wireless links; this SI leverages the performance of ATM to enhance data delivery effectually. Dissimilar to existing routing protocols, DR-HHT and ATM guarantee data integrity by building Kolmogorov_Smirnov based authentication algorithms. Concerning the correlation coefficient, this model isolates DoS attacks and diminishes computational cost. This strategy also eliminates duplicate data transmission and redundant information, offering an effectual trust-based evaluation model from adaptive authentication. Extensive simulation demonstrates that the anticipated model shows a better trade-off than the prevailing techniques and the simulation is carried out in a MATLAB environment.

Keywords: Wireless sensor networks; dimensionality reduction based hilbert-huang transformation; authentication trust model; kolmogorov_smirnov; reliability; stability

This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

1 Introduction

Wireless sensor networks are making an impact in the Internet of Things as well (IoT) and act a significant task to offer an extensive range of applications via sensors like traffic management, smart home, environmental monitoring [1]. WSNs comprise certain sinks or receivers and a huge amount of distributed nodes collaboratively to transmit and collect data to carry out the various missions [2]. The main purpose of constructing WSNs is to provide a stable and consistent data delivery which is expected in IoT applications. One instance of this application is healthcare utilized for purposes like tracking, monitoring and treating patients [3]. In this applications, sensors accumulate patient's data and distribute it to physicians. The doctors are aware of patients' physiological status and make an appropriate analysis with collected data.

Consistent data supply is a key task for successful diagnosis is provided by the above-mentioned programs, Moreover, WSNs are vulnerable to failures of node-link owing to signal fading or signal inference, which may drastically reduce QoS [4]. Henceforth, packet delivery turns to be a confronting task in WSNs. To resolve the above-mentioned crisis, numerous multi-path routing approaches are anticipated to enhance consistent packet delivery. Moreover, dealing with multi-path routing for effectual data flow leads to higher transmission costs for wireless channel unsteadiness [5]. However, as data packets are broadcasted over multiple paths [6], signal interferences and transmission contentions are attained and lead to added network transmission failures [7]. In recent times, an effectual technique is a deal with data reliability and stability requirement is exploited with adaptive routing will not offer routing before transmission [8]. Wireless channels' broadcast nature facilitates transmission to be heard by enormous sensor nodes [9]. Based on single forwarder routing, multiple candidate forwarders are chosen, which are positioned based on priorities determined by the transmitter [10]. Henceforth, transmission is not disrupted, while a single candidate forwarder set successful relays [11]. In contrast to conventional approaches, adaptive routing has superior recital as no added signal interferences or transmission contentions exist amongst candidates [12]. In the traditional approach, geographic routing is more attractive for dynamic wireless links because there is no need to establish or maintain a route from the source to the receiver [13]. Hence, integration of opportunistic and geographic routing is specified as geographic routing [14]. Prevailing routing methods can attain higher consistency over wireless links. Moreover, they are influenced by serious DoS attacks [15]. Malicious attackers intentionally transmit a huge amount of invalid data to sink, targeting to dissipate network resources and WSNs operations [16]. With many potential forwarders and theoretical analysis, routing accentuates DoS, ensuring that faulty data is consistently transmitted to receivers [17]. To preserve these attacks, a security-based authentication strategy is needed, this ensures that the packets are sent by authorized sensor nodes and are not altered or sourced by attackers during transit. Moreover, it leads to a huge amount of open issues. Fig. 1 shows the DoS attack in WSN.

Initially, co-operating prevailing digital signature strategy for authentication tremendously raises sensor node computational cost and enlarges delay of data packet delivery. Sensors are energy and computational constrained typically. The existing investigation has demonstrated that signature requires a certain time for transmission. The node's resources would be quickly depleted if it checked the signature of every incoming data packet. Henceforth, a novel lightweight authentication method to segregate the severity of attackers is essential for WSNs. Subsequently, data packets verification breaks down candidate forwarders priorities described by routing, as delay is usually higher than packets transmission time. Therefore, candidate forwarders priorities are to attain reliability and integrity of data which is an ultimate goal. Third, routing may involve duplicate broadcasting of invalid data. For example, if a candidate drops one valid packet after the verification process, the next candidate will not drop data packets due to link failure or invalid data. It may skip the verification process and leads to invalid packets delivery. The comparison demonstrates that computational resources utilization is reduced by 50%−70%, specifically bandwidth

resources in contrast to prevailing techniques. This investigation is a primary effort for effective and reliable data delivery protocol whilst maintains authentication data explicitly in WSNs. The Scalable DoS attack detection framework is collaborative and hierarchical; it merges the benefits of trust computation and WSN. This novel structural modelling includes monitoring global traffic and validating time-series traffic data for analyzing network attacks.

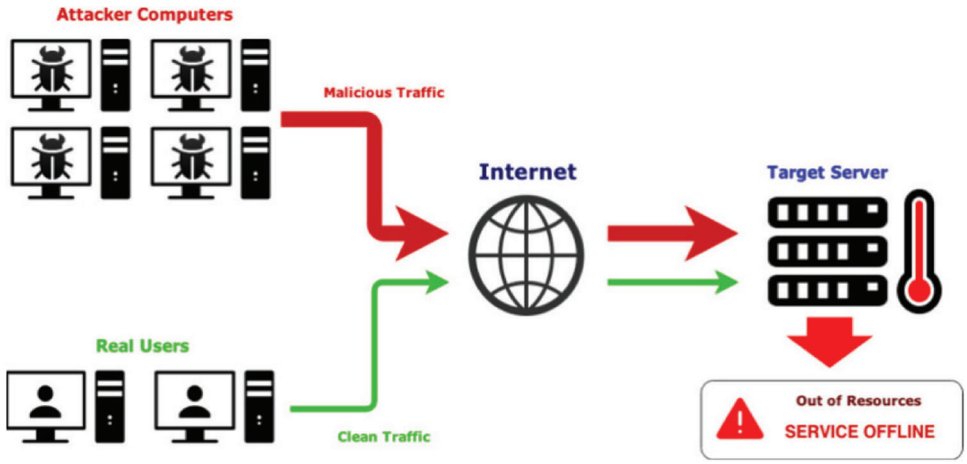

Figure 1: DoS attack in WSN

2 Related Works

Rakesh in [18] investigated Authentication and Security in Mobile sink-supported Internet of Things. Sail fish optimization algorithm is utilized by the author to Secure RPL routing. Moreover, the routing layer of DDoS attacks is considered to offer dependable and secure network services in WSNs.

In [19], Yang et al. Polynomial-based Compromise-Resilient En-route Filtering is an anticipated Polynomial-based Compromise-Resilient En-route Filtering approach that has the potential to filter fake injected data and achieve extremely influenced recovery ability. This strategy utilizes polynomials indeed of Medium access control (MAC) to offer security protection. Moreover, this strategy requires certain added verification computational costs.

Nagarathana and Mercy in [20] tackle DDoS attacks on IoT Servers, which are triggered by malicious wireless IoT devices. They used a learning-driven detection mitigation process with the semi supervised machine-learning algorithm. Yin et al. in [21] represent the SD-IoT (Software-Defined Internet of Things) framework. This framework comprises controller pooling with SD-IoT controllers. An algorithm is anticipated to identify DDoS attacks with this framework. The author also depicts scalable identification architecture to be appropriate for IoT applications. Nain et al. in [22] described a secure IEEE 802.15.4 transceiver strategy that mitigated numerous attacks by physical layer encryption technique that diminishes computational costs at upper layers.

Cao et al. in [23] anticipate that distributed denial of service (DDoS) prevention-based solutions is a significant factor to preserve business online. Moreover, those solutions suffer from defending over large scale DDoS attacks, and not still influencing DDoS attacks offered by unauthorized IoT devices like the attack in IoT devices. Tan et al. in [24], anticipate a computer vision-based technique to identify an attack, which makes records as images. Here, Multiple Channel architecture (MCA) is anticipated to transform records into corresponding images. In the identification scheme, the photos are used as observed objects, sourced on dissimilarity measures. To investigate IDS, the KDD Cup 99 dataset and the

IDS assessment dataset is used. Experimental results suggest that this technique is effective, as well as a novel measure to spot DoS attacks.

Jeong et al. in [25] anticipate a hybrid technique to co-operate analysis with visual analytic to identify network IDS. Principal compound analysis (PCA) and Mobile remote access (MRA) are merged to examine traffic data. To extract features, DWT is used as an MRA approach. PCA is used in this case to turn the retrieved characteristics into main components. Moreover, DWT outcomes are based on Wavelet base function selection [26].

In WSNs, there exist certain other security and trust-based strategies which are provided to eliminate attacks on dissemination protocols that may provide a new programming model to all sensory parts. Nonetheless, all the measures described above have nothing to do with reliability, QoS, trust computation, state information of nodes in WSN [27]. The motivation of this investigation is to effectually merge that anticipated authentication approach with the geographic and selective authentication approach. Therefore, dimensionality reduction based Hilbert-Huang Transformation (DR-HHT) and authentication trust mode (ATM) is designed for minimizing negative impacts caused by existing authentication models [28].

3 Proposed Work

This work assumes multi-hop WSN which comprises a huge amount of nodes and certain receivers which is deployed for IoT application. Nodes that are placed in certain transmission regions 'T_R' can transmit data to one another. While the Euclidian distance is greater than the transmission region, multi-hop communication is facilitated. Consider that nodes in dense network region, where every node has enormous neighborhood nodes. Therefore, the network is modelled by Directed Acyclic Graph (DAG), i.e., $G(S_n;D_l)$ where S_n is sensor node and D_l is a set of direct links amongst sensor nodes. If the Euclidian distance between sensor nodes I S n and receiver nodes j S n is less than the transmission range T R, the link is represented as l (i, j) D1. Consider sensor nodes to be stationary nodes containing information about the sink's location and position. Furthermore, via beacon messages, nodes are generally aware of the location of comparable neighborhood nodes, i.e., sensor nodes broadcast their location information periodically, identity and residual energy [29]. In general, energy is a major crisis that is qualified with devices and subsequent nodes works on limited batteries. Concerning messages, it is probable to acquire energy information of its neighborhood nodes. Here, significant concentration over data delivery performance amongst network layer is depicted. Consider that each sensor node has two keys: a public key and a private key, both of which are used to verify and sign packets. An effectual trust Collision avoidance (CA) should support public keys as sensor nodes' with legal identities. In a real deployment, developers or sink nodes of applications could offer the role of CA [30]. Here, every sensor nodes are aware of the public keys of corresponding neighborhood nodes, whereas it never releases private key to nodes in the network.

3.1 Security Model

In this investigation, the ultimate objective is to model a reliable and effective protocol that usually upholds required authentic data. Henceforth, this significant property for data packets has to be maintained.

3.1.1 Packet Integrity

Before initiating packet transmission, all senor nodes have to guarantee and acknowledge the authenticity of relaying data to its subsequent nodes. Else, sinks nodes will receive a huge amount of invalid data from attackers, by disrupting operations of IoT applications. To offer packet integrity, an effectual authentication strategy is necessary.

3.1.2 Non-Repudiation of Data Packet

Non-repudiation property generally offers the authentication. It enables the sink to verify to a third party that the sensor node is completely accountable for the data packet. In this regard, the receiver can set up a sender with an invalid packet and report it to the trusted CA.

3.1.3 Data Packet Reliability

Because of the shared and broadcast character of the wireless medium, data packets are at risk of being lost if the link fails. Even though the data loss effect is unavoidable, it has no authority to disable the application operations that are related to IoT. Thus, it is necessary to ensure higher consistency for data protocol.

3.1.4 Attack Resistant

Devoid of authentication strategy, attackers may transmit a huge amount of invalid packets to waste resources of the network or interrupt normal data delivery. However, nodes usually have certain restrictions in energy and computational resources [31]. An authentication strategy with low computational cost should be anticipated to defend against DoS attacks.

3.2 Problem Statement

In the case of WSN, routing protocols are extremely simpler; moreover, network performance and topology structure can be influenced by routing protocol during the process of attack. Therefore, a routing protocol is extremely susceptible to DoS like a black hole, clone attack. The conventional DoS attack uses susceptibility of Transmission control protocol (TCP) congestion control approaches, new routing attack model is anticipated to support trust and security-based researches. DoS attack tries to interrupt topology structure-based control method and reduces performance, similarly, average routing traffic is the same as that of general routing traffic to circumvent IDS. Therefore, DoS attack and identification are extremely challenging in recent investigations. Due to the limited resource constraints in WSN, online and complex intrusion detection techniques cannot be openly utilized in WSN nodes. Due to the similarity of DoS attack traffic to normal traffic, traditional threshold-based anomalous detection approaches cannot be used to detect routing-based DoS attacks. Similarly, routing protocols lack a congestion control strategy, making them vulnerable to DoS attacks. As a result, determining a routing layer-based DoS attack poses a bigger challenge. While Hilbert Huang based analysis is cast-off to examine the DoS traffic data, the smaller signal generated using the DoS attack is complex to be identified as the interference of false IMF component. Along with this, computation of trust is quantitative information based security method. The concept of trust computing is used to enhance the reliability of the Intrusion detection system (IDS) technique. It's also tough to evaluate and recognize trustworthy-based Intrinsic Mode Function (IMF) components. WSN has found two key difficulties with DoS assaults as a result of the aforementioned elements. Because DoS attack traffic is identical to normal traffic, traditional DoS detection techniques are difficult to spot black holes and clone attacks. Routing layer-based DoS identification in resource-restricted is also a crisis. In conventional methods, Hilbert-Huang Transformation based time-frequency analysis approach is interfered with as small-signal characteristics of DoS attack, Intrinsic mode function (IMF) components that aren't real are commonly mixed in with real IMF components. The IMF component's estimation of trust is also a major crisis.

3.3 Trust Modelling with State Information

By analyzing and examining neighbourhood data transmission, this work utilizes the number of packets that are transported successfully to the sum of transmitted to classify trust computation. Nodes divide the timeline into a chain of observation intervals with similar 'n' lengths at a higher level. During every interval, it is the probability with 'k' node to wireless link and validates whether data packets are

forwarded truly chosen neighbourhood. For all interims, the total amount of the transmitted data packet by neighbourhood node and the number of data packets transmitted. Henceforth, the node may compute the trust link which is specified as in Eq. (1):

$$T_k^i(n) = \frac{NS_k^i(n)}{ND_k^i(n)} \tag{1}$$

At observation interval, $NS_k^i(n)$ is initialized to 0 and $ND_k^i(n)$ is initialized to 1. When data packets are replayed by node 'k' to 'i' as next-hop nodes, $ND_k^i(n)$ is revised by $\propto ND_k^i(n) + 1$, where $\propto (0 < \propto \leq 1)$ is the adjustment rate in the system. As node determines successful transmission, $NS_k^i(n)$ turns to $\propto ND_k^i(n) + 1$ to establish a trust link that is positively determined. Else, $NS_k^i(n)$ turns to $\propto NS_k^i(n)$ when a transmission fails and the trust degree may be changed negatively. To acquire trust-based stability for candidate selection, trust link at time 't' is revised through nodes iteration during neighbourhood list as in Eq. (2):

$$T_k^i(t) = \omega T_k^i(t-n) + (1-\omega) T_k^i(n) \tag{2}$$

where ω $(0 \leq \omega \leq 1)$ is a weighted balance between present and previous state facts. When there is no ambiguity with time, T_k^i is used for brevity.

3.4 Modelling of Dimensionality Reduction

Consider the network connectivity based on Fig. 2 to analyze the state space of nodes connected in the network as in Eq. (3).

$$x(s+1) = Ax(s) + w(s) \tag{3}$$

where $w(s) \in C^s$ is current process state It is determined that every sensor can accumulate data from state components. When sensor measurements are sent to the appropriate sink, i^{th} sink node dimension is $y_i(s) \in Cq^s$ is modelled as in Eq. (4).

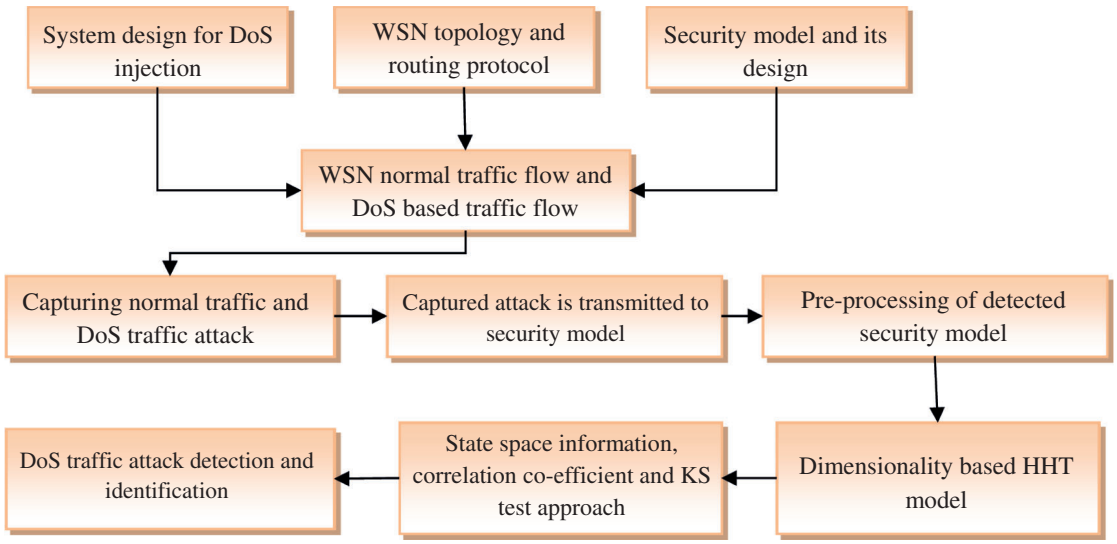

Figure 2: Flow of DoS attack identification

$$y_i(s) = C_i x(s) + v_i(s) \tag{4}$$

where, i = 1, 2, 3, ….L

Where $A \in C^{s*s}$ and $C_i \in Cq^{i*n}$. $w(s) \in C^s$ are uncorrelated zero-mean Gaussian noise satisfying as in Eq. (5).

$$E\left\{[w^T(s)v_i^T(s)^T[w^T(s_1)v_j^T(s_1)]\right\} = \delta_{s,s_1} diagonal\ \{Q_w,\ \delta_{i,j}Q_{vi}\} \tag{5}$$

This model is extensively utilized for determining the dynamic state-space of power systems, constructing automation systems and smart grid infrastructures and so on. With respect to the measurements $\{y_i(1), \ldots, y_i(s)\}$, local optimal estimator at i^{th} sink node is provided as in Eq. (6).

$$\begin{cases} x_i(s) = \varnothing\, k_i(s)\widehat{(s-1)} + k_i(s)y + y_i\,(s)\, k_i(s) \\ \quad = p_{ii}^*(s)C_i^T\,[c_i p + P_{ii}^*\,(s)C_i^T + Q_{vi}]^{-1} \end{cases} \tag{6}$$

where $G_{ki}(s) \triangleq I_n - k_i(s)C_i$, $\varnothing_{ki}(t) \triangleq G_{ki}(s)A$ and local optimal estimation error covariance matrix $P_{ii}(s)$ is evaluated using Eq. (7).

$$\{p_{ii}(s) = G_{ki}\,(s)p_{ii}^*(s), \qquad \{p_{ii}^*(s) = AP_{ii}(s-1)A^T + Q_w \tag{7}$$

The one-step prediction error covariance matrix is denoted by $p_{ii}^*(s)$. However, it facilitates that from estimation error cross-covariance matrix $p_{ii}^*(s)$ is computed as in Eq. (8).

$$p_{ij}(s) = G_{ki}(s)[AP_{ij}(s-1)A^T + Q_w]G_k j^T(t) \tag{8}$$

A communication channel is used to send an ideal fusion estimator design for each local estimate xi(t) to FC, as shown in Fig. 2. However, the state variable x(t) dimension in (6) is higher, any communication channel carries finite information per unit of time. Here it is impractical to expect the sink to transfer all of the data on xi(t) to FC. Only ri ($1 \le ri < n$) components of ith local estimate $\hat{x}i(t)$ are broadcast to FC at a given time to reduce communication traffic, similar to DR reduction procedures in [22] and [23]. Based on DR strategy, allowed sending components (ASCs) of $\hat{x}i(t)$ has _i possible cases, where _i is taken as.

As depicted in Fig. 3, to model an effectual node fusion estimator based local estimation has to transmit data to sink for the communication channel. However, the state variable dimension is higher in a larger number of nodes. Communication channels carry finite information per unit of time as well Here, it is unrealistic that a sink can transmit data to a fusion estimator. To diminish communication traffic, dimensionality reduction concept based component of i^{th} local estimators are selected and broadcasted to the fusion estimator at a specific time. In accordance with the dimensionality reduction scheme, the corresponding components for transmission are provided as in Eq. (9).

$$\Delta_i = C_n^{ri} = \frac{n!}{r_i!(n-r_i)!} \tag{9}$$

After that, in a specific time, only one vector signal is considered for one group, where Δ_i is selected and transmitted to the fusion estimator. When every sink node transmits data o a remote fusion estimator through the communication channel, an adversary may induce congestion between the communication channels and sink nodes, thereby launches DoS. It specifies that the estimator cannot receive the data at a specific time 't'. In addition, the attacker has a limited energy budget and must decide whether or not to congest the communication channel at each sample time. However, owing to limited energy constraint and spatial distribution of sink nodes, an adversary launches attack κ ($1 \le \kappa < L$) communication channel 'L' can

be congested, thus packets are dropped. To formulate an attack strategy, consider $\eta(t) \in \{0, 1\}$ which specifies that the adversary launches an attack and not in time 't'. Also, specify $\eta_i(t) = 1$ *or* $\eta_i(t) = 0$ as function indicator whether i^{th} the communication channel is jammed by attackers in time 't', and $\eta_i(t)$ should be satisfied as in Eq. (10).

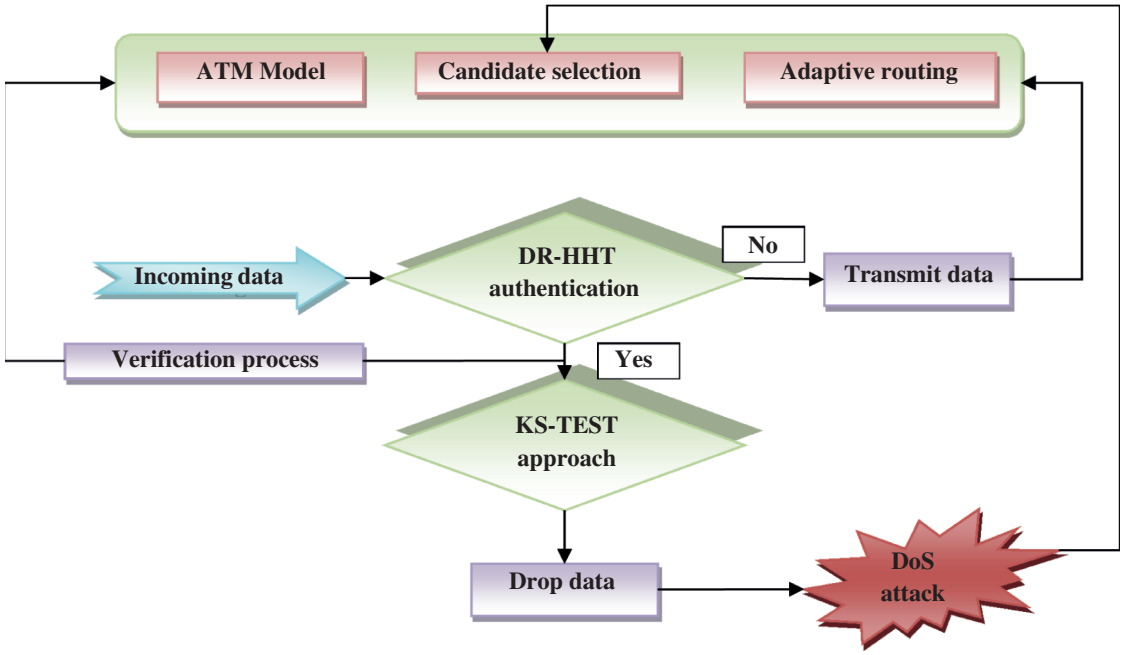

Figure 3: DoS attack detection and prevention using ATM

$$\sum_{i=1}^{L} \eta_i(t) = k(1 \leq k < L) \tag{10}$$

where η_i (t) = k(1 ≤ k < L) is intended to improve performance deterioration while the attacker launches a DoS assault at the time 't'. It is measured that η(t) is Bernoulli's theorem variable $E\{\eta(t)\} = \eta$ where 'η' is termed as attack rate.

Let $\widehat{x_{si}(t)}$ specify local estimation of the received signal. Then, in DoS attack, every $X_{si}(t)$ is designed by Eq. (11).

$$\widehat{x_{si}(t)} = [1 - \eta(t)\eta_i(t)]\, x_{si}(t) \tag{11}$$

This specifies that when $\eta(t) = 0$ *or* $\eta(t) = 1$, $\eta i(t) = 0$, i^{th} the channel is not congested due to DoS attack during the time 't'. The performance of a distributed fusion estimator is decreased once it is developed based on the signal. To eliminate performance degradation, state-space estimation is essential and provided in Eqs. (12)–(14):

$$\begin{aligned} x_i(t) &= (1 - \eta(t)\eta_i(t))\, [H_i(t)x_i(t) + (I_n - H_i(t) \\ &Ax_i(t-1)] + \eta(t)\eta_i(t)Ax_i(t-1) \end{aligned} \tag{12}$$

where $H_i(t)$ specifies compression operator, and

$$H_i(t) = diag\ (\gamma_{i1}(t),\ r_{i2}(t) \ldots \gamma_{in}(t)\} \tag{13}$$

With $\gamma_{in}(t) \in \{0, 1\}$. While there is no attack at time 't', $\gamma_{in}(t)$ specifies that j^{th} component of $x_i(t)$ is transmitted to fusion estimator or not.

$$\sum_{j=1}^{n} \gamma_{ij}(t) = r_i(i\epsilon\{1,\ \ldots,\ L\}) \tag{14}$$

where r_i specifies bandwidth constraint.

Certain components of (x_i (t)) are facilitated to be broadcast to the fusion estimator due to bandwidth constraints. Compression matrix is $H_i(t) = diag\{\gamma_{i1}(t), \gamma_{i2}(t), \gamma_{i3}(t)\}$, where $\gamma_{ij}(t) \in \{0, 1\}(j = 1, 2, 3)$ and $\gamma_{i1}(t) + \gamma_{i2}(t) + \gamma_{i3}(t) = 2$.

Now, DR problem based on DoS attacks has been presented. Following are the two cases of effectual transmission,

1) If $\eta(t)\eta_i(t) = 0$, the dimensionality reduction model with bernoulli's theorem reduces $x_i(t) = (1 - \eta(t)\eta_i(t))\ [H_i(t)\ x_i(t) + (I_n - H_i(t)\ Ax_i(t-1)]$, which specifies that chosen value is transmitted successfully to the fusion estimator, the un-transmitted data packets are compensated.
2) If $\eta(t)\eta_i(t) = 1$, the proposed dimensionality reduction model specifies the i^{th} communication channel which is jammed due to DoS attack at time interval 't'.

3.5 Dimensionality Reduction Based Hilbert-Huang Transform (DR-HHT)

In this investigation, Hilbert-Huang Transform is extensively utilized to examine non-stationary signals, like financial applications, biomedical applications, image processing, health monitoring, ocean engineering, and network abnormal traffic detection. It is anticipated to identify a small signal generated using routing layer based DoS attack in WSN. Empirical Mode Decomposition (EMD) is an adaptive data analysis technique that decomposes data signals into intrinsic mode function (IMFs) component sets that extract the significant instantaneous frequency and amplitude information using the Hilbert transform. Here, Kolmogorov-smirnov is used to compute trust evaluation with IMF component, missing detection and error detection with time-frequency analysis. This is a non-parametric test that is used to compute data from a known distribution or a set of data from the same distribution. KS is utilized to compute similarity among IMF components and original traffic data, therefore similarity is utilized as IMF component evidence for trust computation. Fig. 2 shows the flow of DoS attack identification.

The process of IMF component extraction is determined as follows:

1) Recognize local extreme in data signal;
2) Connect local maxima with an upper envelope of cubic spline line;
3) Connect local minima with a lower envelope of cubic spline line;
4) Attain mean curve value amongst lower and upper envelope.

Lower and upper envelopes have to determine all data. The average envelope value is m_1. The difference amongst original data $X(t)$ and m_1 is primary component h_1, as in Eq. (15).

$$h_1 - m_{11} = h_{11} \tag{15}$$

After the worst round for calculation, the peak is turned to be the local maximum. In the subsequent stage, h_1 specifies proto-IMF, as h_1 does not belong to stationary data series, the average value m_{11} is computed on h_1 as a similar technique. Subsequently, h_1 is evaluated as follows in Eq. (16).

$$h_1 - m_{11} = h_{11} \tag{16}$$

After repeated evaluation of k times, h_{1k} becomes an IMF that is given below in Eq. (17).

$$h_{1(k-1)} - m_{1k} = h_{1k} \tag{17}$$

Therefore, h_{1k} is the first IMF component, indicating the greatest frequency component, with the standard deviation serving as the halting condition. In this work, the SD stoppage criteria value is between 0.2 and 0.3. It is given as below in Eq. (18).

$$SD = \left[\sum_{t=0}^{T} \frac{|h_{1(k-1)}(t) - h_{1k}(t)|^2}{h_{1(k-1)}^2(t)}\right] \tag{18}$$

When stopping criteria is fulfilled, data ranges from [0.2, 0.3], can be attained with the first IMF component. Subsequently, IMF components are computed as a similar strategy. From a real signal x (t), an analytic signal z (t) is calculated, and Hilbert transforms y(t) are given below in Eqs. (19) and (20).

$$y(t) = \frac{1}{\pi} p \propto \frac{x(\tau)}{t-\tau} d\tau \tag{19}$$

$$z(t) = x(t) + jy(t) \tag{20}$$

where P specifies the principal value of singular integral, y(t) is a Hilbert transformation of $x(t)$ real part.

3.6 Authentication Trust Model Evaluation Using Kolmogorov-Smirnov Test

After the computation of HHT, a correlation co-efficient approach is utilized to examine the trust value model of IMF components, missing detection or error detection that occurs in dimensionality reduction based HHT time-frequency analysis.

Therefore, the trust evaluation Kolmogorov-Smirnov approach is integrated with DR-HHT to examine the data built from known distribution i.e., one or two sample data, which is, built from the same distribution.

Two samples are generally a non-parametric approach to evaluate sample distribution similarity, as it is sensitive to the shape of CDF of two samples. Test samples are utilized to compute IMF components similarity and original data traffic, therefore, the similarity is utilized as proof of IMF trust component evaluation. Fig. 3 shows the DoS attack detection and prevention using ATM.

The CDF (Cumulative Distribution Function) supporting two-time series is f(x) and r(x), and the maximum absolute difference of the two CDFs is represented by D, as shown in formula (20).

As CDF (cumulative distribution function) is made up of two-time series, f(x) and g(x), the biggest difference between them is given as D in Eq. (21):

$$D = |f(x) - g(x)| \tag{21}$$

The probability of similarity between two samples is given as in Eqs. (22) and (23):

$$probability\ (D) = Q_{ks}\left[\left(\sqrt{N_e + 0.12 + \frac{0.11}{\sqrt{N_e}}}\right)D\right] \tag{22}$$

$$N_e = \frac{N_1 N_2}{N_1 + N_2} \tag{23}$$

From the above Eq. (22), N_1 and N_2 specifies sample amount of time series. Q_{ks} is provided as probability distribution function in Eq. (24):

$$Q_{ks}\ (\lambda) = 2 \sum_{j=1}^{\infty} (-1)^{j-1}\ e^{-2j^2\lambda^2} \tag{24}$$

Therefore, CDF is the same, their probability is nearer to 1, similarity provides higher IMF components trust degree; else its probability is nearer to 0, which is irrelevance amongst them. The lower IMF trust component is utilized to examine IMF trust value. Therefore, CC and Kolmogorov-smirnov approach is used to resolve the trust-based problem.

4 Numerical Results and Discussions

In this investigation, network topology and routing was constructed for building routing during DoS attack, security detection is based on the need of security requirement. Normal traffic is constructed in accordance with network configuration. Then, captured routing traffic has to be provided for security analysis by periodically USB protocol.

Packets attained is in Packet sniffer format which is used to convert captured file format into traffic format in security level based server, then message number is abridged at the pre-processing stage. Therefore, pre-processed static traffic data is analyzed using DR-HHT approach. DR-HHT analysis process as in Fig. 4 is used to examine pre-processed statistical data and identify DoS attacks. To resolve inference of false IMF component crisis, CC and KS approaches are used to examine and identify trust IMF components to enhance DoS accuracy to detect the attack. While the DoS traffic attack is detected, a node that generates DoS attack traffic is recognized as a DoS attack node. Tab. 1 shows the simulation setup of the proposed work.

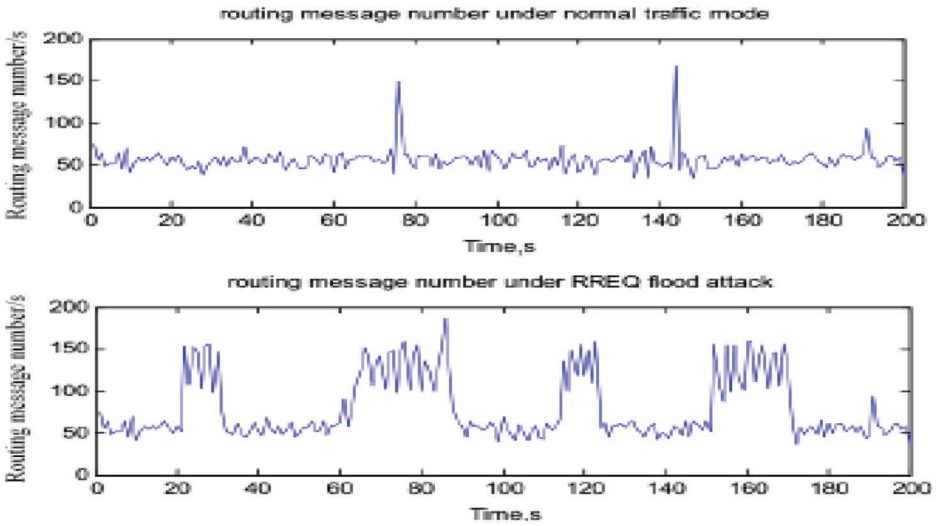

Figure 4: Sample IMF component outcome

Table 1: Simulation setup

Parameter	Value
Simulation time	200 s
Wireless node type	CC2530
Total nodes	5
Total attack nodes	1
Total sniffer node	1
Attack node ID	2
Protocol	Zigbee
Routing protocol	AODV
MAC layer protocol	IEEE 802.15.4
Attack	DoS
Duration	20–30 s

The maximum amount of messages in DoS is nearer to usual traffic. It is complex to identify traffic using the conventional detection method. Moreover, performance will be influenced, PDR as in Fig. 5 has been raised from 0.1%–0.35% in DoS attack. If DoS is not identified effectively, performance is affected due to DoS attacks simultaneously.

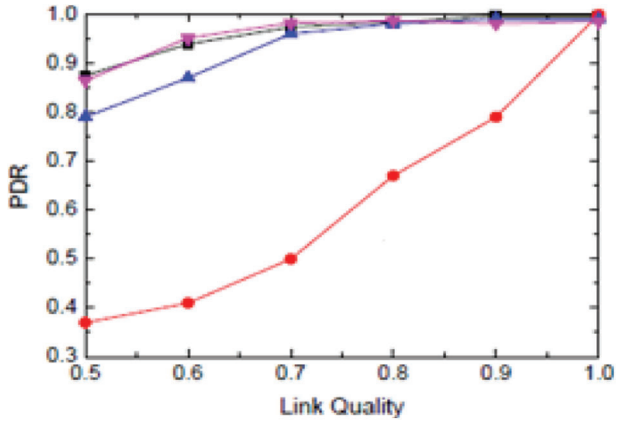

Figure 5: PDR with ATM

In accordance with the algorithm, correlation coefficient values of the first IMF components are more than 0.3 as in Tab. 3, that of other IMF components. Therefore, the first IMF component is a trust value-based component, whereas other IMF components are false IMF components. The Trust evaluation as in Tab. 2 outcomes are based on IMF components similarity value relative to original DoS attack. Tab. 3 shows the ATM performance.

Table 2: Component analysis

Components	Correlation coefficient value
IMF component 1	0.4550
IMF component 2	0.2037
IMF component 3	0.1370
IMF component 4	0.3470
IMF component 5	0.2820

Table 3: ATM performance

ATM condition	ATM value	ATM degree	ATM usage
Fulfils two condition	2	Higher IMF component	Detect DoS attack
Fulfils one condition	1	Lower IMF component	Moderate assistance to DoS attack
Does not fulfils condition	0	False IMF component	Does not detect DoS attack

Fig. 7 shows the transmission overhead. The below-given performance metrics are evaluated using DR-HHT in WSNs:

1) PDR: is distinct as a proportion of total packets attained to total packets transmitted from source nodes.
2) Verification process: total verification carried out by nodes during simulation, shows the influences of computational cost and energy consumption.
3) Invalid packet-based Hop count: computed as regular hop count of invalid packets broadcasted.
4) Invalid packets based transmission overhead: In a network, the total number of packets (bits) sent is different from the total number of packets (bits) sent.
5) E2E delay: average packet delivery time from the source to the sinks, comprising together invalid and legal packets (sec) as in Fig. 5.
6) Invalid packets ratio (IPR): IPR is defined as the ratio of the number of invalid packets obtained by sinks to the total number of packets acquired by sinks as in Fig. 6.
7) Overhead in the control packet, there are total packets for delivery in time (bits/s), a packet of warning push, and a packet of verification notice in Fig. 8.

Fig. 9 shows the control packet overhead. This work examines the authentication performance under various scenarios of wireless links. Here, DR-HHT is compared with other approaches of four solutions under topologies with various attack rates of DoS attackers. Fig. 10 shows the invalid packet data. These solutions are summarized in Tab. 4:

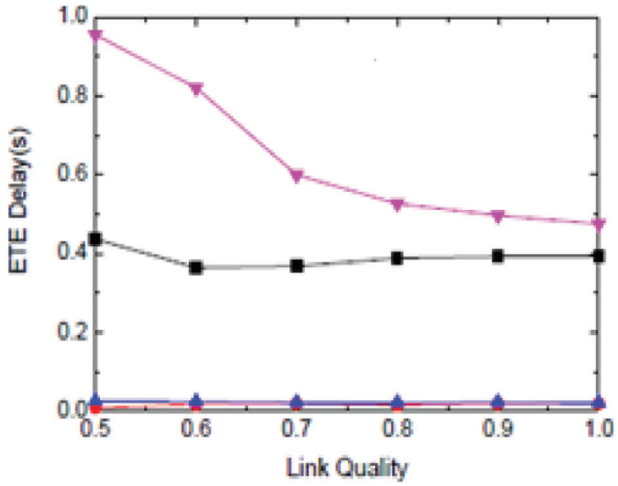

Figure 6: E2E delay with ATM

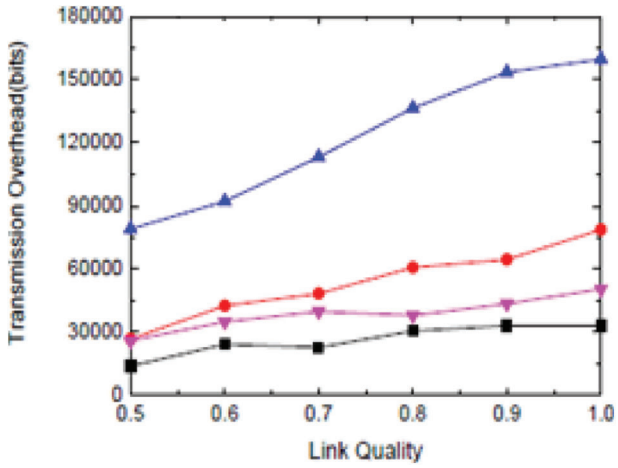

Figure 7: Transmission overhead

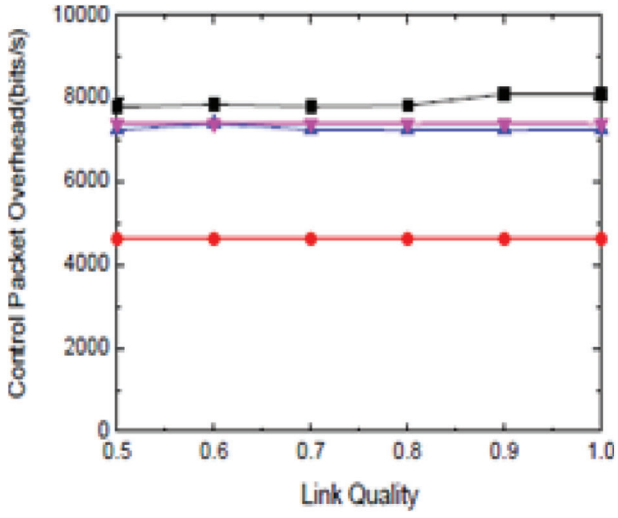

Figure 8: Control packet overhead

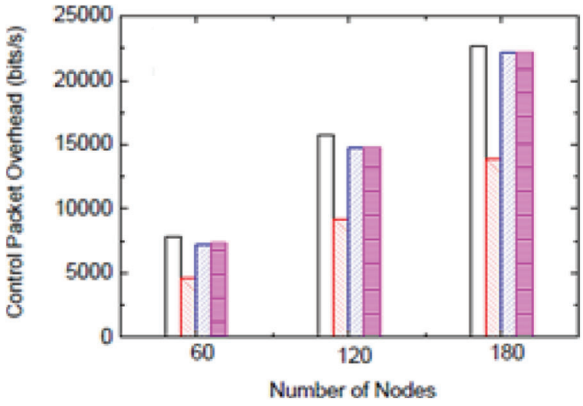

Figure 9: Control packet overhead

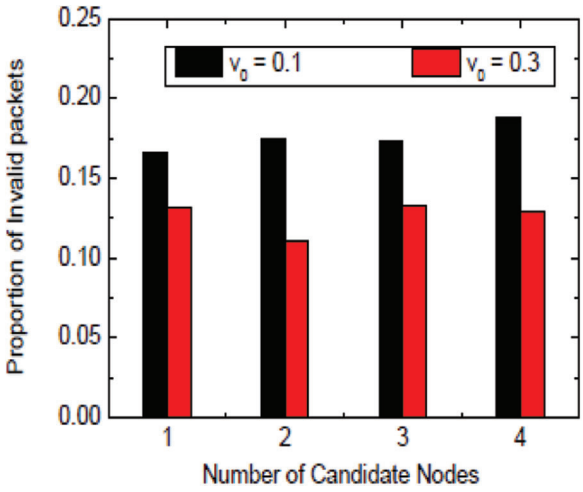

Figure 10: Invalid packet data

Table 4: Comparison with existing models

Methods	Geographic	Opportunistic	No authentication	All authentication	Selective authentication	Cooperative verification
SelGOR	✓	✓			✓	✓
No verify	✓	✓	✓			
Verify all	✓	✓		✓		
GPSR Sel	✓	✓			✓	
GOR sel	✓				✓	
DR-HHT	✓	✓		✓	✓	✓

1) No-verify is defined as a primary geographic opportunistic routing approach that is not based on authentication.
2) Verify All is an approach where sensor nodes validate every received packet of data.
3) GPSR is a generalized unicast routing protocol that allows sensor nodes to evaluate data packets selectively.
4) GOR-sell utilizes a selective authentication algorithm devoid of cooperative verification strategies.

As depicted in Tab. 5, five different factors are utilized to evaluate various attack detection approaches in WSN. They are attack detection, time-frequency analysis, trust evaluation, WSN attack detection and scalability in the WSN environment. All these items are considered in this model, where only certain items are supported by prevailing approaches. The anticipated DR-HHT model is easily scalable in the WSN environment. Overall performance of the anticipated model is superior to prevailing approaches.

Table 5: Comparison with attack parameters

Methods	Time-frequency	Attack detection	Trust evaluation	WSN attack	Scalability
SelGOR	Supportive	Abnormal traffic detection	NA	NA	Complex
GPSR sel	NA	DoS detection	NA	Supportive	Moderate
GOR sel	NA	DDoS detection	Supportive	Supportive	Moderate
DR-HHT	Supportive	LDoS detection	Supportive	Supportive	Easier

5 Conclusion

DoS attack recognition is a huge confrontation with recent IDS in WSN. Here, a DoS attack identification scheme with a Dimensionality reduction based HHT and authentication trust model is anticipated. There exist three significant contributions in this investigation:

1) Stabilized DoS attack identification model with the merits of WSN and IoT.
2) A novel adaptive authentication method is designed by combining dimensionality reduction based Hilbert-Huang Transformation (DR-HHT) to monitor the traffic and to record the congestion that is caused in the network.
3) KS test and correlation component are used to examine the trust model of WSN with IMF modules, therefore the accurateness of detecting DoS attack is enhanced using the DR-HHT modelFalse IMF components will be removed and not taken into account. The trust-based component is utilized to identify DoS attacks.

For further research direction, DoS based attack detection for both IoT and WSN architecture is carried out by combining cloud computing and Fog computing. This model is an effective model to analyze and detect attacks in WSN. This approach promotes that DR based HHT and the authentication based Trust model (DR-HHT and ATM) for IoT application is highly effective.

Acknowledgement: We show gratitude to anonymous referees for their useful ideas.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] L. Atzori, A. Iera and G. Morabito, "The internet of things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[2] L. Da Xu, W. He and S. Li, "Internet of things in industries: A survey," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 4, pp. 2233–2243, 2014.

[3] J. N. Al-Karaki and A. E. Kamal, "Routing techniques in wireless sensor networks: A survey," *IEEE Wireless Communications*, vol. 11, no. 6, pp. 6–28, 2004.

[4] S. Li, R. K. Neelisetti, C. Liu and A. Lim, "Efficient multi-path protocol for wireless sensor networks," *International Journal of Wireless and Mobile Networks*, vol. 2, no. 1, pp. 110–130, 2010.

[5] G. Schaefer, F. Ingelrest and M. Vetterli, "Potentials of opportunistic routing in energy-constrained wireless sensor networks," in *European Conf. on Wireless Sensor Networks*, Berlin, Heidelberg, pp. 118–133, 2009.

[6] J. Luo, J. Hu, D. Wu and R. Li, "Opportunistic routing algorithm for relay node selection in wireless sensor networks," *IEEE Transactions on Industrial Informatics*, vol. 11, no. 1, pp. 112–121, 2014.

[7] K. Zeng, Z. Yang and W. Lou, "Location-aided opportunistic forwarding in multirate and multihop wireless networks," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 6, pp. 3032–3040, 2008.

[8] L. Cheng, J. Niu, J. Cao, S. K. Das and Y. Gu, "QoS aware geographic opportunistic routing in wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 7, pp. 1864–1875, 2013.

[9] P. Ning, A. Liu and W. Du, "Mitigating DoS attacks against broadcast authentication in wireless sensor networks," *ACM Transactions on Sensor Networks (TOSN)*, vol. 4, no. 1, pp. 1–35, 2008.

[10] M. Naghshvar and T. Javidi, 2010, "Opportunistic routing with congestion diversity in wireless multi-hop networks," in *Proc. IEEE INFOCOM*, San Diego, CA, USA pp. 1–5, 2010.

[11] L. Cheng, J. Niu, Y. Gu, T. He and Q. Zhang, "Energy-efficient statistical delay guarantee for duty-cycled wireless sensor networks," in *Annual IEEE Int. Conf. on Sensing, Communication, and Networking (SECON)*, Seattle, WA, USA, pp. 46–54, 2015.

[12] X. Tang, J. Zhou, S. Xiong, J. Wang and K. Zhou, "Geographic segmented opportunistic routing in cognitive radio ad hoc networks using network coding," *IEEE Access*, vol. 6, no. 11, pp. 62766–62783, 2018.

[13] M. Salehi and A. Boukerche, "A novel packet salvaging model to improve the security of opportunistic routing protocols," *Computer Networks*, vol. 122, no. 4, pp. 163–178, 2017.

[14] C. Lyu, D. Gu, X. Zhang, S. Sun, Y. Zhang *et al.,* "SGOR: Secure and scalable geographic opportunistic routing with received signal strength in WSNs," *Computer Communications*, vol. 59, pp. 37–51, 2015.

[15] M. Roopak, G. Y. Tian, and J. Chambers, "Multi-objective-based feature selection for DDoS attack detection in IoT networks," *IET Networks*, vol. 9, no. 3, pp. 120–127, 2020.

[16] A. Chonka, Y. Xiang, W. Zhou and A. Bonti, "Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks," *Journal of Network and Computer Applications*, vol. 34, no. 4, pp. 1097–1107, 2011.

[17] N. Ravi and S. M. Shalinie, "Learning-driven detection and mitigation of DDoS attack in IoT via SDN-cloud architecture," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3559–3570, 2020.

[18] B. Rakesh and H. Parveen Sultana, "Novel authentication and secure trust-based RPL routing in mobile sink supported internet of things," *Cyber-Physical Systems*, vol. 14, pp. 1–34, 2020.

[19] S. Patel and A. Sharma, "The low-rate denial of service attack based comparative study of active queue management scheme," in *Tenth Int. Conf. on Contemporary Computing (IC3)*, Noida, India, pp. 1–3, 2017.

[20] R. Nagarathna and S. Mercy Shalinie, "Learning-driven detection and mitigation of DDoS attack in IoT via SDN-cloud architecture," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3559–3570, 2020.

[21] N. Singh, S. Chaudhary, K. K. Verma and A. K. Vatsa, "Explicit query-based detection and prevention techniques for DDoS in MANET," *International Journal of Computer Applications*, vol. 53, no. 2, pp. 19–24, 2012.

[22] D. Yin, L. Zhang and K. Yang, "A DDoS attack detection and mitigation with software-defined internet of things framework," *IEEE Access*, vol. 6, no. 4, pp. 24694–24705, 2018.

[23] A. K. Nain, J. Bandaru, M. A. Zubair and R. Pachamuthu, "A secure phase-encrypted IEEE 802.15. 4 transceiver design," *IEEE Transactions on Computers*, vol. 66, no. 8, pp. 1421–1427, 2017.

[24] Y. Cao, Y. Gao, R. Tan, Q. Han and Z. Liu, "Understanding internet DDoS mitigation from academic and industrial perspectives," *IEEE Access*, vol. 6, no. 11, pp. 66641–66648, 2018.

[25] Z. Tan, A. Jamdagni, X. He, P. Nanda, R. P. Liu *et al.,* "Detection of denial-of-service attacks based on computer vision techniques," *IEEE Transactions on Computers*, vol. 64, no. 9, pp. 2519–2533, 2014.

[26] S. Nithya, P. Sundara Vadivel, D. Yuvaraj and M. Sivaram, "Intelligent based IoT smart city on a traffic control system using raspberry Pi and robust waste management," *Journal of Advanced Research in Dynamical and Control Systems*, vol. 10, no. 14, pp. 765–770, 2018.

[27] D. Yuvaraj, M. Sivaram, A. M. U. Ahamed and S. Nageswari, "An efficient lion optimization-based cluster formation and energy management in WSN based IoT," in *Int. Conf. on Intelligent Computing & Optimization*, Thailand, pp. 591–607, 2019.

[28] A. M. U. Ahamed and D. Yuvaraj, A. Jayanthiladevi, E. Balamurugan and R. Tamaraiselvi, "Smart connected digital products and IoT platform with the digital twin," *Research Advancements in Smart Technology, Optimization, and Renewable Energy*, vol. 16, pp. 330–350, 2021.

[29] K. Manikandan and D. Yuvaraj, "An energy-efficient EDM-RAEED protocol for IoT based wireless sensor networks," *Journal of Advanced Research in Dynamical & Control Systems*, vol. 10, no. 14, pp. 1978–9191, 2018.

[30] V. Porkodi, S. Amin and D. Yuvaraj, "Prolong the network lifespan of wireless sensor network," *Journal of Advanced Research in Dynamical & Control Systems*, vol. 10, no. 14, pp. 2034–2038, 2018.

[31] V. Porkodi and D. Yuvaraj, "A survey on various machine learning models in IoT applications," in *Conf. on Computing and Information Technology (ICCIT-1441)*, Saudi Arabia, pp. 1–4, 2020.