Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 20 Issue 2 Version 1.0 Year 2020
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 2249-4596 & Print ISSN: 0975-5861

Optimized Load Centroid and Rabin Onion Secured Routing in Wireless Sensor Network for IoT

By Renuka Mohanraj
Maharishi International University

Abstract- Advances in wireless communication have geared up extensive insights wherein the sensors can themselves communicate with other sensors that form significant parts of the Internet of Things (IoT). However, the large-scale acceptance of WSN for IoT is still surfacing threats and controversies that apprehend the security aspects. There are a lot of attacks that can manipulate the routein WSN for IoT. In this work, an Optimized Load Centroid and Rabin Onion Routing (OLC-ROR) method are designed to improve the throughput rate with minimum routing overhead and latency. The proposed method is based on a Centroid and Rabin Signature, a Digital Signature technique. First, the optimal route is identified by considering both the load and residual energy using Load Centroid function. Then onion routing is used for selecting secured route amongst the optimality. Besides, the node genuineness is checked by applying the Rabin Signature.

Keywords: wireless sensor network, internet of things, security, load centroid, rabin signature, onion routing.

GJCST-E Classification: C.2.1

Strictly as per the compliance and regulations of:

Optimized Load Centroid and Rabin Onion Secured Routing in Wireless Sensor Network for IoT

Renuka Mohanraj

Abstract- Advances in wireless communication have geared up extensive insights wherein the sensors can themselves communicate with other sensors that form significant parts of the Internet of Things (IoT). However, the large-scale acceptance of WSN for IoT is still surfacing threats and controversies that apprehend the security aspects. There are a lot of attacks that can manipulate the routein WSN for IoT. In this work, an Optimized Load Centroid and Rabin Onion Routing (OLC-ROR) method are designed to improve the throughput rate with minimum routing overhead and latency. The proposed method is based on a Centroid and Rabin Signature, a Digital Signature technique. First, the optimal route is identified by considering both the load and residual energy using Load Centroid function. Then onion routing is used for selecting secured route amongst the optimality. Besides, the node genuineness is checked by applying the Rabin Signature. Each node uses a special data structure (i.e. onion routers) to store routing information. The main objective of this algorithm is to improve security and efficiency for WSN in IoT. The performance of the proposed Optimized Load Centroid and Rabin Onion Secured Routing method is compared with different state-of-the-art methods using the NS-2 simulator. Extensive simulation scenarios are considered, and final results show that the proposed method has higher throughput with minimum routing overhead and route acquisition latency, which makes it more efficient in WSN for IoT.

Keywords: wireless sensor network, internet of things, security, load centroid, rabin signature, onion routing.

I. Introduction

The Internet of Things (IoT), where several devices are associated to share the data in different domains such as home automation, patient monitoring, industrial device monitoring, smart cities, and so on. Wireless Sensor Networks (WSNs), due to its ubiquitous devices, has been in use in recent years in many IoT applications. However, researchers have not complicatedly addressed the issue part during routing. A significant amount of research work in the domains of security, topology, and energy consumption in WSN for IoT has been managed in the recent past.

Given view of the essential qualities of the sensor nodes in WSN, the constrained computing capability, and energy requirements, a Sector-based Random Routing (SRR) method was presented in [1] to address the Source Location Privacy (SLP) issues and therefore minimizing the energy consumption. With this objective, in SRR, the data packets were sent to random phantom sources that were situated in several sensors. These were then disseminated via all routes to arrive promptly at the sink node. Besides, the notion of a hop threshold was also included to manage the routing strategies and minimize energy consumption.

Despite improvement observed in the energy consumption with minimum delay, the routing overhead was not considered. To minimize the routing overhead, the Load Centroid Optimal Route Identification model is applied to the WSN network that considers both load and residual energy to identify optimal routes.

An Anchor-based Routing method was designed in [2] with constrained flooding and dynamic clustering. A novel type of event-based clustering model along with a novel clustering mechanism to be included dynamically. With the design of these models, energy consumption was said to be reduced with higher number of packets processed successfully by the sink. Data collection performed at the mobile sink was then said to be shared to the contended users via IoT infrastructure.

Despite the improvement observed in the throughput rate, the security aspect was not covered. To improve the security with minimum latency and higher throughput, in this work, a Rabin Onion Secured Routing algorithm is designed. This algorithm not only identifies the secured route using Onion Routing but also ensures that the node with which the routing is carried out is also authenticated node or in other words, the genuineness of the node is checked via Rabin Signature.

In this paper, we propose an optimal and secured routing to be followed in WSN for IoT, called Optimized Load Centroid and Rabin Onion Routing (OLC-ROR). OLC-ROR method aims at ensuring the routing overhead for IoT-based applications, i.e., for a smart city. To improve the efficiency of the throughput rate, the OLC-ROR method analyzes onion routes for obtaining secured routing and builds an Onion-based Route in WSN for IoT. Also, in contrast to existing anchor-based routing, OLC-ROR method leverages a Rabin Onion Secured Routing algorithm to ensure route

Author: Department of Computer Science, Maharishi International University, Fairfield, Iowa, USA. e-mail: rmohanraj@miu.edu

acquisition latency. Our selection secured routing algorithm is performed based on the Rabin signatures with minimum load and residual energy and, can reduce the routing overhead of the entire smart city network.

The main contributions of the proposed work are summarized as follows:

- We design a Load Centroid function that is exploited as the basis of constructing an optimal routing model to reduce the routing overhead.
- We identify serious security threats to the optimal routing in WSNs for IoT. Subsequently, a Rabin Onion Secured Routing algorithm is introduced to obtain secure routes with minimum route acquisition latency.
- A Rabin Signature is exclusively proposed to verify the genuineness of the node with which secured routing is said to be established, at the same time it also significantly improves the throughput rate incur by the secured routing.
- Theoretical analysis and empirical validations are done to show the significance of OLC-ROR method. It reduces the routing overhead and route acquisition latency with higher throughput rate.

The paper is prearranged in the following sections. Section 2 describes the work related to security aspects in WSN for IoT. Section 3portrays the method of secure routing, Optimized Load Centroid and Rabin Onion Routing (OLC-ROR). The simulation setup, along with the results, is depicted in Section 4 and Section 5, respectively. Finally, the concluding remarks are shown in Section 6.

II. Related Works

Adding the distinctiveness and the extent of the routing path can significantly improve the network safety time. But, the constrained energy consumption has to be also considered. In [3], a source location privacy protection scheme based on ring-loop routing (SLPRR) in WSNs for IoT was presented to solve the issues related to energy consumption. Three types of routing were first considered, followed by which the distinctiveness and routing extent were said to be enhanced. Finally, rings were formed in the non-hotspot area, therefore reducing energy consumption.

With new improvements in IoT technology, authorized users are said to access reliable sensor nodes. By accessing the reliable sensor nodes, data are said to be first obtained, and commands are also sent to the destined nodes. However, designing an effectively secured authentication and key agreement scheme is significant due to the resource constrained nodes. In [4], secure and lightweight authentication and key agreement scheme for IoT based WSNs were designed, contributing to the security aspect.

A survey on recent advancements in data trust, communication trust in WSN-assisted IoT was designed [5]. However, security for both data and route was not ensured. To address this issue, a cross-layer based adaptive secured routing and data transmission process was designed in [6] to ensure data security.

With the routing protocol susceptible to different types of attacks in WSN, which is an important network type of IoT. The correlation coefficient, and Kolmogorov-Smirnov (KS) test approaches were combined to measure the trustworthiness of the Intrinsic Mode Function (IMF) components and discard the false IMF components. Besides, Hilbert-Huang transformation and trust evaluation techniques [7] were also integrated to cover the security aspect.

However, with the IoT edge nodes being exposed to different types of attacks, in [8], the focus was made on developing a lightweight authentication model for constrained end-devices, therefore ensuring security. Yet another convolutional technique concentrating on security aspect was designed in [9] to prevent malicious node attacks.

A full evaluation of security attacks regarding WSNs and IoT, along with the methods to detect the types of attack, preventing the attacks, and mitigations of those attacks was presented in [10]. IoT is not only considered as the most favorable research topic but also considered as the blossoming industrial drift. The basic idea in the Internet is to bring objects; there are different methods because an IoT system is introduced in several applications. A WSN based IoT platform for wide-area and heterogeneous sensing applications was presented in [11].

A concept of combining fault tolerance and secured routing model in WSN called as the Fault Tolerant Secured Routing (FASR) that ensures secured routes between the source node and sink nodes under faulty node constraints was presented in [12]. Here, faulty nodes were first identified via battery power and interference models. Next, the trustworthy nodes between fault-free nodes were then obtained using agent-based trust model. Finally, the data was found to be secured routed via fault-free non-compromised nodes to sink. Yet another secured and effective access control mechanism for WSN in the cross-domain context of the IoT [13] that permits an Internet user in Certificate Less Cryptography (CLC) environment to communicate with a sensor node via an Identity-Based Cryptography (IBC) environment with different system parameters.

A secure routing and monitoring model via multiple variant tuples using the Two-Fish (TF) symmetric key approach to identify and discard the malicious nodes in the network was designed in [14] based on the Authentication and Encryption Model (ATE). With the aid of the Eligibility Weight Function (EWF), the sensor guard nodes were identified and were hidden using a symmetric key approach. However, challenges posing security for the smart city was less focused. In [15], a scalable framework for authentication

and hierarchical routing was designed to address the security issues. However, the energy efficiency of the node was not concentrated. In [16], presented an energy-aware and secure multi-hop routing protocol using a secret sharing scheme. So that reduces the energy consumption along with the network throughput and average end-to-end delay.

An enhancement of the reactive routing protocol, called constrained flooding and dynamic clustering, was presented in [17]. Here, a novel event-based clustering mechanism, in addition to the dynamic clustering technique, minimizing the energy consumption with higher data packets being processed successfully manner to the sink node.

In [18], the networking characteristics required for smart city applications, besides networking protocols utilized to engage different data traffic streams, were introduced. A secure 3-way routing protocol for routing using cryptographic techniques for providing a high degree of security was introduced in [19].

For the influence of constrained energy and networking attacks resulted from open transmission channels, a low-power and secure multi-hop routing technique based on the Markov state transition theory was presented in [20]. Here, with the random transmission route selection, typical attacks were said to be eliminated, thus resulting in secured data transmission with the reduced energy consumption.

All the existing methods are given above utilized random route selection and balanced load to secure data transfer. Random route selection is not an effective approach as it consumed more routing overhead and route acquisition latency to generate the route according to load factor. Each node entering the network is provided with these load factors; therefore, for large networks it becomes more complex and more storage space is required, which is limited. In the proposed method, an optimal routing model is used to select the optimal route using minimum load centroid and residual energy and hence minimizing the routing overhead. Next, a secure route is obtained via onion routers, and node authentication is also checked using Rabin signature.

III. Methodology

In this section, an optimal and secured routing method to be followed in WSN for IoT called Optimized Load Centroid and Rabin Onion Routing (OLC-ROR) is designed. Here, two different models are used. First, optimal route identification is made by applying the Load Centroid function. The objective behind the use of the Load Centroid function is that it assists in minimizing the routing overhead because of the consideration of both minimum load and residual energy while selecting the route. Next, amongst optimal routes being identified, secured routing is followed by applying the Rabin Onion Routing model. The purpose of using this routing model is that by using Onion routing, the route acquisition latency is reduced, and using Rabin Signature, verification is performed, therefore ensuring security with a higher throughput rate. First, a network model used for the design of OLC-ROR is presented, followed by which the elaborate description is provided.

a) Network model

Let us assume a multi-hop WSN that comprises a number of sensor nodes $N = N_1, N_2, \ldots, N_n$, and some sink nodes $S = S_1, S_2, \ldots\ldots, S_n$ is deployed for one application (i.e., for a smart city) of IoT. The sensor nodes deployed in WSN within the wireless transmission range ' R ' directly send data packets $DP = DP_1, DP_2, .., DP_n$ to each other following a specified type of routing. The multi-hop communication is said to be enabled when the distance is said to be greater than the transmission range with the assumption that the sensor node in the network is a dense network where each sensor node has several neighbor nodes.

Thus, this network is said to be defined by a graph $G(V, L)$. Here, V represents the set of sensor nodes and, L represents the set of links between the sensor nodes in the network. Besides, a link is represented by $link_{i,j} \in L$, if the distance between the sender nodes $i \in V$ and the receiver node $j \in V$ is smaller than the transmission range R. Figure 1, given below illustrates a sample IoT-based WSN.

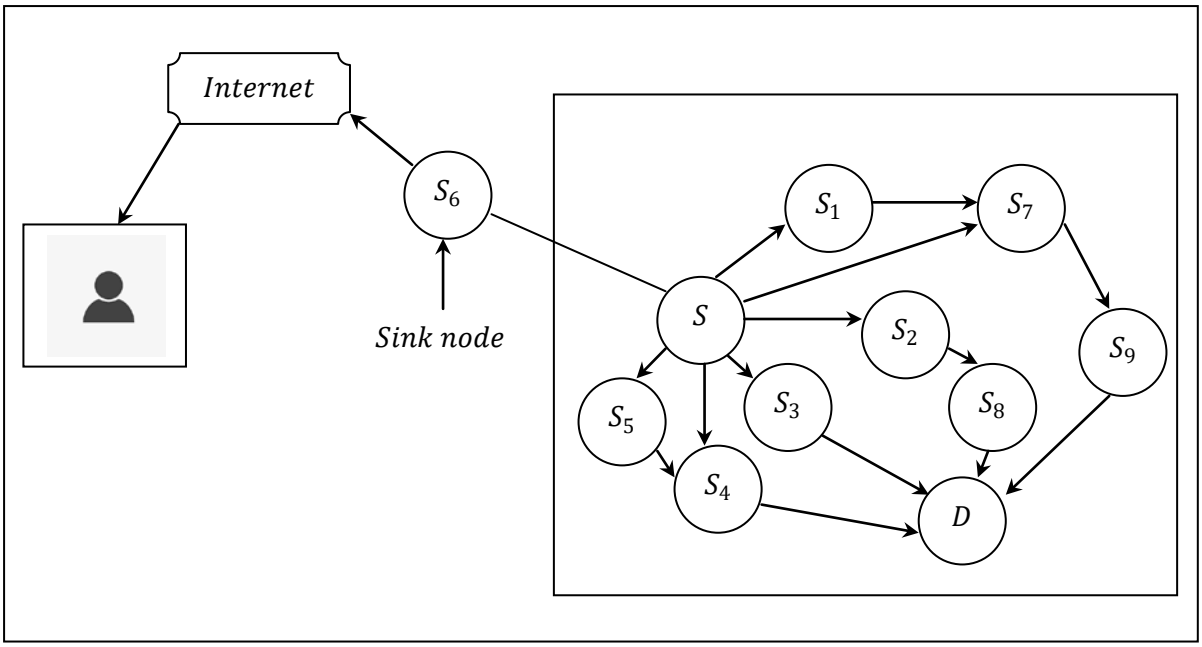

Figure 1: IoT-based WSN

Figure 1 given above depicts a scenario of WSN in IoT with a single source node S, single destination node D, with multiple sensor nodes 'S_1', 'S_2', 'S_3', 'S_4', 'S_5', 'S_7', 'S_8', 'S_9', one sink node 'S_6'respectively that also acts as the gateway node. Therefore, multiple sensor nodes join the internet through a gateway or sink node. In this work, an IoT-enabled WSN for a smart city is designed that uses different types of IoT sensors for route optimization and secured routing.

b) Load Centroid Optimal Route Identification

In an IoT-enabled WSN, different routes are said to exist with the advantages of following one route over another route. Therefore, multiple routes are said to exist for an IoT-enabled WSN. However, the optimal route has to be identified. In this section, Optimal Route Identification is said to be made using Load Centroid function. Table 1, given below shows the sample routes identified for figure 1.

Table 1: Sample Routes

Number of Routes identified	Routing Pattern
R_1	$S \rightarrow S_2 \rightarrow S_5 \rightarrow D$
R_2	$S \rightarrow S_4 \rightarrow D$
R_3	$S \rightarrow S_3 \rightarrow D$
R_4	$S \rightarrow S_7 \rightarrow S_9 \rightarrow D$
R_5	$S \rightarrow S_1 \rightarrow S_7 \rightarrow S_9 \rightarrow D$
R_6	$S \rightarrow S_5 \rightarrow S_4 \rightarrow D$

In the field of mathematics, centroid refers to the center of the load, the imaginary point of mass concentration.With the sample routes identified, in our study, the concept of Load Centroid is used to identify the optimal route. So, the route with minimal load and average residual energy is said to be an optimal route when compared to the other routes. Figure 2 shows the block diagram of the Load Centroid Optimal Route Identification model.

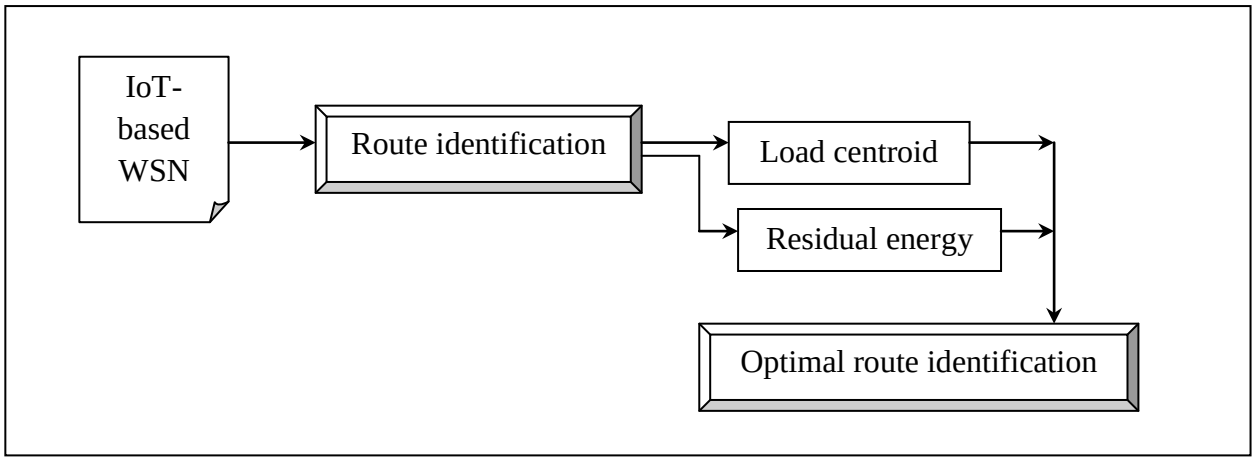

Figure 2: Block diagram of Load Centroid Optimal Route Identification

As depicted in the above figure 2, the first optimal route identification is performed by applying Load Centroid function along with the residual energy. The pseudo-code representation of load-balanced optimal route identification using Load and residual energy centroid function is given below.

Input: Sensor nodes '$S = S_1, S_2, \ldots, S_n$', Source node '$S$', Destination node '$D$'
Output: Load balanced optimal route identification '$R = R_1, R_2, \ldots, R_n$'
1: **Begin** 2: **For** each sensor nodes '$S = S_1, S_2, \ldots, S_n$' with source node '$S$', destination node '$D$' 3: Measure position of the load centroid with respect to 'P' axis using (1) 4: Measure position of the load centroid with respect to 'Q' axis using (2) 5: Measure residual energy centroid with respect to 'P' axis using (3) 6: Measure residual energy centroid with respect to 'Q' axis using (4) 7: Return (load balanced optimal route) 8: **End for** 9: **End**

Algorithm 1: Load Centroid Optimal Route Identification

As given in the above algorithm, for each sensor nodes with source node requesting to send the data packets, the position of load centroid, followed by residual energy centroid are measured. The equations (1) and (2) given below are utilized to measure the position of the load centroid and is formulated as given below.

$$P_{lc} = \frac{SM_q}{SM} = \frac{\int p * \alpha DL}{\int \alpha DL} \quad (1)$$

$$Q_{lc} = \frac{SM_p}{SM} = \frac{\int q * \alpha DL}{\int \alpha DL} \quad (2)$$

From the above equations (1) and (2), $P, Q,$ represents the coordinates of the node i, P_{lc} and Q_{lc} symbolizes the results of load coordinates with α representing the node density, SM_q, SM_p representing the static moment to the q axis and p axis for a differential of load DL respectively. Then, the residual energy centroid rec for two different axes P and Q is measured as given below.

$$P_{rec} = \frac{\sum_{i=0}^{n} \frac{E_{i\_re}}{E_{ie}} * P}{N} \quad (3)$$

$$Q_{rec} = \frac{\sum_{i=0}^{n} \frac{E_{i\_re}}{E_{ie}} * Q}{N} \quad (4)$$

From the above equations (3) and (4), E_{i_re}, represents the residual energy of node i with an initial energy of E_{ie} respectively. If the load of the sensor nodes is known and said to be distributed in an even fashion, then equations (3) and (4) are used to measure the position of the load centroid. However, for IoT-based WSN, the influence of node load in the network is not required for the network lifetime. Therefore, with the node load information and the residual energy, the equations (3) and (4) are used to measure the position of the residual energy centroid.

Therefore, the residual energy centroid has the influence of the energy distribution during the smooth operation of the network. Hence, in this work, both the load and residual energy centroid are considered in an integrated manner to select the optimal route. With this, the routing overhead incurred in identifying the optimal route is said to be reduced. Table2, given below shows the optimal routes identified after applying the load centroid function.

Table 2: Load Centroid Optimal Routes

Number of Routes identified	Routing Pattern
R_2	$S \rightarrow S_4 \rightarrow D$
R_3	$S \rightarrow S_3 \rightarrow D$

c) Rabin Onion Secured Routing

Smart security is an essential component of IoT-based WSN. Since IoT-based WSN uses the wireless medium, communication in a wireless network can arise from any direction and can target any node, therefore it ranges from different types of attacks, and securing smart cities for the future remains a key concern. There are a few solutions for securing routing protocols for IoT-based WSN as far as a smart city is concerned. But still due to security lapse while routing and detecting them is complicated in IoT-based WSN.

The goal here is to propose a model that performs point-to-point routing authentication with IoT-based WSN. There is another issue of plotting secure and efficient routing protocols that have both high network performance via route acquisition latency and security with a higher throughput rate. Although the researcher has outlined several security mechanisms for a few existing secured routing protocols. Yet, there is no standard secured routing model for IoT-based WSN that performs best regarding performance (i.e., minimum route acquisition latency) and performance (i.e. maximum throughput rate).

In this work, with the objective of securing both the route and the carrier node, a Rabin Onion Secured Routing algorithm is designed. The proposed routing algorithm is to select a secured route while considering the key when selecting the forwarding route. Also, carrier node genuineness is a key requirement for IoT-based WSN. Thus, we also propose a model to balance between throughput and route acquisition latency in our Rabin Onion Secured Routing model.

Rabin Onion Secured Routing ensures anonymous communication over a computer network, where the nodes are encapsulated in layers of encryption, related to the layers of an onion. The encrypted data is transmitted through a series of intermediate or relay nodes called onion routers, uncovering the data's next destination. When the final node is decrypted, the data packet arrives at its destination, ensuring both secured routing with the correctness of carrier node genuineness. The sender node is said to be anonymous because each intermediate node knows only the location of the immediately preceding and following nodes. Figure 3 shows the block diagram of Rabin Onion Secured Routing.

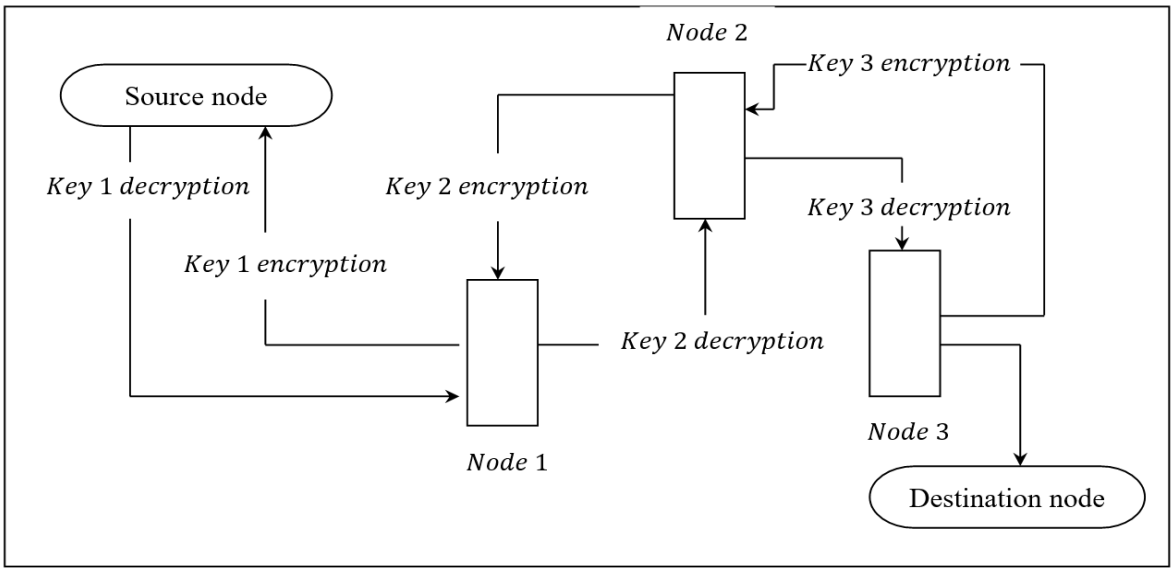

Figure 3: Rabin Onion Secured Routing

Figure 3 shows a Rabin Onion Secured Routing model followed for IoT-based WSN with a sample of three intermittent nodes between the source and destination node. This onion secured routing model is applied once the optimal routes are said to be identified. With the optimal routes, secured routing amongst them is identified by following onion routing. The source node with access to all the encryption keys, i.e., $K = K_1, K_2, \ldots, K_n$ encrypts the message wrapping it under three layers like an onion.

This triple encrypted layer message is then sent to the first intermediate node N_1. Here, N_1 only has the address of N_2 and K_1. Hence, it decrypts the message using K_1 and perceives that it does not make any sense since it still has two layers of encryption. So, it passes it on to N_2. Here, N_2 has K_2 and the addresses of the input & exit nodes. So, it decrypts the message using K_2 perceiving that it is still encrypted and passes it onto the exit node. Now, the N_3 peels of the last layer of encryption and pass it on to the destination node.

The destination node processes the request and serves up the desired source node as a response. The response passes through the same sensors in the opposite direction where each node puts on a layer of encryption using their specific key. It finally reaches the source node in the form of a triple encrypted response that is said to be decrypted as the source node has access to all the keys. The pseudo-code representation of Rabin Onion Secured Routing is given below.

Input: Optimal routes '$R = R_1, R_2, \ldots, R_n$', sensor nodes '$S = S_1, S_2, \ldots, S_n$', source node '$S$', destination node '$D$', encryption keys, '$K = K_1, K_2, \ldots, K_n$'

Output: Robust secured routing '$SR = SR_1, SR_2, \ldots, SR_n$'

1: **Begin**
2: For each Optimal routes 'R', with sensor nodes 'S' with encryption keys, 'K'
3: For each source node 'S' with destination node 'D'
4: Select public key and private key using (6) and (7)
5: Solve the rabin function using (9)
6: Measure the genuineness of intermediate node via
7: If '$x(x+u), mod\ f = (DP * RP\ mod\ f)$'
8: Node said to be genuine
9: Perform secured routing
10: **End if**
11: **If** '$x(x+u), mod\ f <> (DP * RP\ mod\ f)$'
12: Node said to be not genuine
13: Go to step 4
14: **End if**
15: **Return** (Robust secured routing 'SR')
16: **End for**
17: **End for**
18: **End**

Algorithm 2: Rabin Onion Secured Routing

As given in the above algorithm, for each Optimal route$R$, with source node S destination node D, the source node S selects primes a, b and measures the product as given below.

$$f = a * b \tag{5}$$

With the measured product, the source node S, then chooses a random u in $\{1,2, \ldots, f\}$ with public key PB_{Key} and private key PR_{Key} as given below.

$$PB_{Key} \rightarrow (f, u) \tag{6}$$

$$PR_{Key} \rightarrow (a, b) \tag{7}$$

To send a data packet DP, the source node S picks random padding $RP$and is written as given below.

$$fun = DP * RP\ mod\ f \tag{8}$$

Then, the source node solves the Rabin Signature written as given below.

$$RS = x(x+u), mod\ f = (DP * RP\ mod\ f) \tag{9}$$

The signature on DP is the pair (RP, x). Finally, authentication of the sensor is performed via verifying the genuineness of the node. Given a data packet DP, and a signature (RP, x), the verifier calculates $x(x+u), mod\ f$ and $(DP * RP\ mod\ f)$ and verifies that they are equal. Hence, by applying Rabin Onion Secured Routing, both the secured routes obtained via Onion Routing, and the genuineness of the selected routing node is verified using Rabin Signature. Therefore, both the route acquisition latency is said to be reduced and throughput rate is improved, ensuring secured routing.

IV. Simulation Setup

The performance of the Optimized Load Centroid and Rabin Onion Routing (OLC-ROR) method is evaluated in this section. Simulations were carried out to compare the performance of the OLC-ROR method. The following results compare the performance characteristics of Sector-based Random Routing (SRR) [1] method, Anchor-based Routing [2] method with proposed OLC-ROR method in a simulated environment. In our implementation, sensor nodes are placed randomly in the network of 1000m * 1000m. Each simulation result is based on ten iterations. The practical networks include a notable number of malicious nodes, and their consequences have to be circumvented. The results are summarized in Table. The version of NS-2 used in our simulation is NS-2.35.

Table 3: NS-2 Simulation parameters

Parameters	Description
Network size	1000m * 1000m
Total number of nodes	50, 100, 150, 200, 250, 300, 350, 400, 450, 500
Simulation time	100s
Max node speed	20 km/hr
Initial energy	2J
Traffic source	Constant Bit Rate
Packet size	512 bytes
Radio range	250m
Mobility	Random way point
Node's transmission range	25m

In the network scenario, 500 sensor nodes were deployed of homogeneous characteristics. Initially, all nodes have 2J energy levels, whereas the transmission power for each node is fixed to 25m. The proposed method is compared with [1] and [2], and the performance is evaluated in terms of routing overhead, route acquisition latency, and throughput.

V. Discussion

This section presents the performance evaluation of the Optimized Load Centroid and Rabin Onion Routing (OLC-ROR) method. Its effectiveness is analyzed for secured routing in WSN for IoT that represents a dense IoT routing with sensor networks. Here, we show how with the aid of OLC-ROR method can follow optimal routing where there are several sensors. Furthermore, we compared the OLC-ROR method with that of SRR [1] and Anchor-based Routing [2] for ensuring secured routing for IoT once all the three methods have a common goal to detect optimal route and also we can show improvement from OLC-ROR compared to the previous work.

a) *Performance analysis of routing overhead*

The first metric considered for analysis is the routing overhead. Whenever an optimal route has to be found, a considerable amount of overhead is said to be incurred. Lower the routing overhead, more efficient and optimal the route is said to be and vice versa. The routing overhead is written as given below.

$$RO = \frac{DP_{tot} + CM_{tot}}{DP_{tot}} \quad (10)$$

From the above equation (10), the routing overhead RO refers to the ratio of summation of the total passed data packets DP_{tot} and the total control messages CM_{tot} to the total passed data packets DP_{tot} respectively. Let us consider 1000 data packets with different types of IoT sensors in a smart city environment, and let us assume the 100 control packet. Then, the routing overhead using the proposed OLC-ROR, SRR [1], and Anchor-based Routing [2] is measured as given below.

Sample calculation for routing overhead

- Proposed OLC-ROR: With 25 number of totals passed data packets and 20 number of total control messages, the routing overhead measured is given below.

$$RO = \frac{25 + 20}{25} = 1.8$$

- Existing SRR: With 25 number of totals passed data packets and 21 number of total control messages, the routing overhead measured is given below.

$$RO = \frac{25 + 21}{25} = 1.84$$

- Existing Anchor-based Routing: With 25 number of totals passed data packets and 22 number of total control messages, the routing overhead measured is given below.

$$RO = \frac{25 + 22}{25} = 1.88$$

Table 4, given below shows the tabulation results of routing overhead for variant number of packets considered in the range of 25 to 250 for three different methods, OLC-ROR, SRR [1], and Anchor-based Routing [2].

Table 4: Tabulation for routing overhead

Number of packets	Routing overhead (ratio)		
	OLC-ROR	SRR	Anchor-based Routing
25	1.8	1.84	1.88
50	2.1	2.3	3.1
75	2.4	2.7	3.3
100	2.5	3	3.8
125	2.8	3.3	4.1
150	3.1	3.8	4.5
175	3.3	4.1	5
200	3.5	4.5	5.3
225	4.1	5	5.5
250	4.5	5.3	5.9

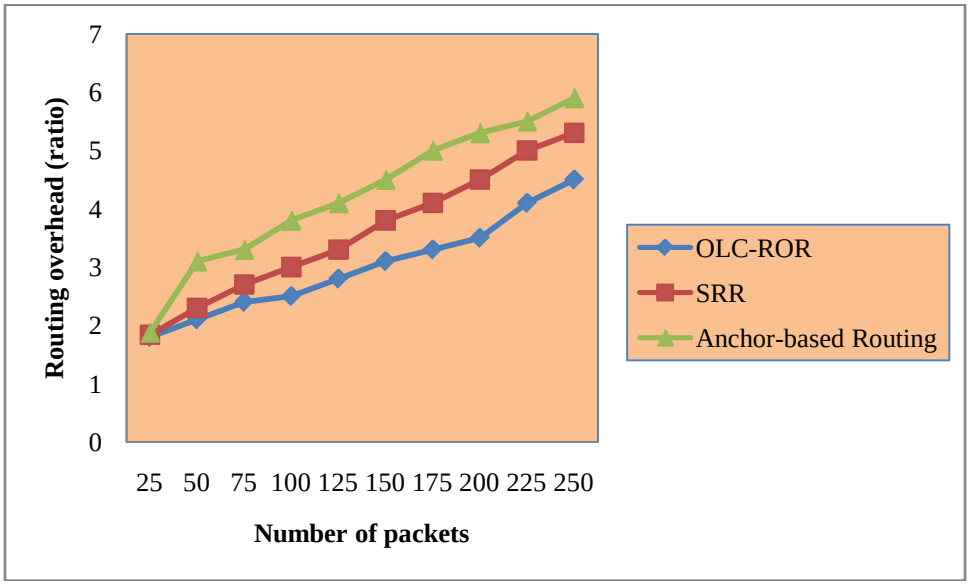

Figure 4: Measure of routing overhead over number of packets

The Figure given above shows the routing overhead for three different methods, OLC-ROR, SRR [1], and Anchor-based Routing [2]. The number of packets is varied in the range of 25 to 250 for ten different simulation runs with each packet varying in the size of 512 bytes. Routing overhead refers to the number of routing packets required for network communication. The proposed algorithms used for routing produces a considerable number of small-sized packets and are referred to as the routing packets. However, routing packets do not carry any application content, as in the case of the data packets. But routing packets and the data packets shares the same network bandwidth, and therefore routing packets are considered as an overhead in the WSN. This overhead is referred to as the routing overhead, lesser the routing overhead, efficient is the method said to be. Figure 4 shows the RO of the three methods. The RO is found to be reduced when applied with the OLC-ROR method when compared to [1] and [2]. The improvement or the minimization of routing overhead using the OLC-ROR method is due to the application of the Load Centroid Optimal Route Identification algorithm. By applying this algorithm, both position of the load centroid and residual energy centroid is considered while selecting the optimal route. Therefore, a route possessing minimal load and lesser residual energy is selected as an optimal route via load and residual energy centroid function. Proposed method minimizes the routing overhead by 15% when compared to [1] and 28% when compared to [2].

b) The Performance measure of routing acquisition latency

The second metric used while considering secured routing in WSN for IoT is the route acquisition

latency. It is measured in terms of milliseconds (ms). It refers to the average time consumed between the generation of a Rabin signature and the reception of the first valid route produced from an intermediary device. Route acquisition latency is calculated only for the Rabin signatures of data packets successfully received by the sink node. It is measured as given below.

$$RAL = \sum_{i \in N}(T_{i,res}) - (T_{i,req}) * N \quad (11)$$

From the above equation (11), the route acquisition latency RAL is measured based on the time at which a signature is generated to request a route for data packet $T_{i,req}$ and $T_{i,req}$ refers to the time at which the first valid route offer for data packet i is received by the source IoT device and N is the number of nodes in the network. The sample calculations for route acquisition latency using the proposed OLC-ROR, existing SRR [1], and existing Anchor-based Routing [2] is given below.

Sample calculations for route acquisition latency

- Proposed OLC-ROR: With 50 number of nodes considered for simulation and $0.035ms$ refers to the time between the request and response, the route acquisition latency is measured as given below.

$$RAL = 0.035ms * 50 = 1.75ms$$

- Existing SRR [1]: With 50 number of nodes considered for simulation and $0.055ms$ refers to the time between the request and response, the route acquisition latency is measured as given below.

$$RAL = 0.055ms * 50 = 2.75ms$$

- Existing Anchor-based Routing [2]: With 50 number of nodes considered for simulation and $0.075ms$ refers to the time between the request and response, the route acquisition latency is measured as given below.

$$RAL = 0.075ms * 50 = 3.75ms$$

Table 5 given below, shows the tabulation results of route acquisition latency for variant number nodes considered in the range of 50 to 500 for three different methods, OLC-ROR, SRR [1], and Anchor-based Routing [2].

Table 5: Tabulation for route acquisition latency

Number of nodes	Route acquisition latency (ms)		
	OLC-ROR	SRR	Anchor-based Routing
50	1.75	2.75	3.75
100	2.25	3.15	5.25
150	2.45	3.35	6.15
200	3.15	3.85	6.35
250	3.35	4.15	6.55
300	3.55	4.55	7.15
350	3.85	5.35	8.35
400	4.35	5.55	8.85
450	4.55	5.95	9.15
500	5.25	6.25	9.55

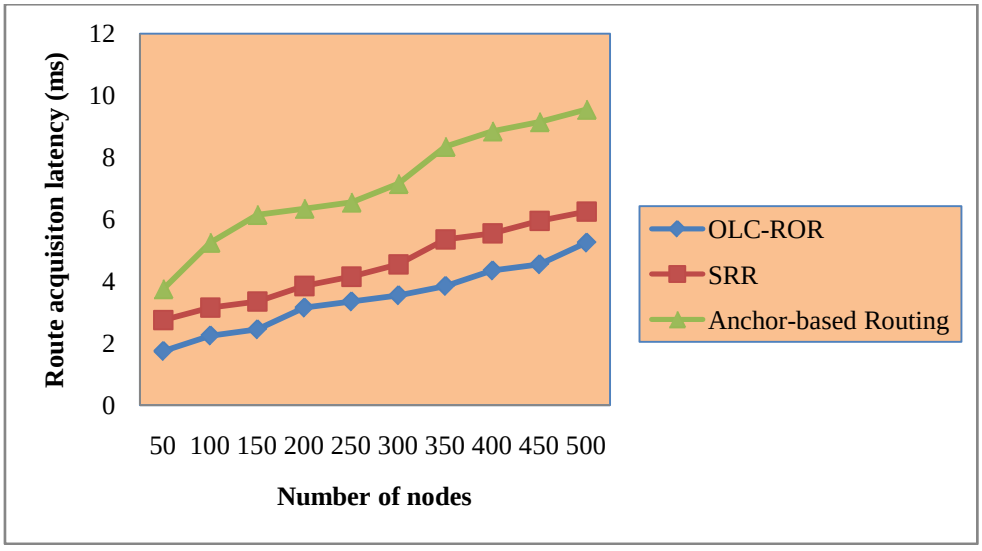

Figure 5: Measure of route acquisition latency over number of nodes

Figure 5 given above shows the performance evaluation of route acquisition latency over different numbers of nodes in the range of 50 to 500 for ten different simulation runs conducted at different time intervals over a wide area of network sizing 1000m*1000m. From the figure it is evident that, with increasing number of nodes, different numbers of optimal routes have to be identified and hence higher the route acquisition latency. From the simulations conducted for 50 numbers of sensor nodes, an optimal route to the sink node is identified within 1.75ms using the proposed OLC-ROR method, 2.75ms when applying with the SRR [1] method and Anchor-based Routing [2] method respectively. Route acquisition latency is said to be reduced using the OLC-ROR method when compared to [1] and [2]. By applying this algorithm, both the secured route and the genuineness of the node is identified. Here, a secured route is obtained via the onion route, and genuineness of the intermediate node is verified via the Rabin signature. Therefore, optimal and secured routes are obtained and with which the data packets are forwarded, minimizing the route acquisition latency using the OLC-ROR method by 24% compared to [1] and 52% compared to [2] respectively.

c) Performance measure of through put

Throughput refers to the average number of data packets successfully received per second to the number of data packets sent is given by

$$TP = \frac{DP_{rec}}{DPT_{sent}} \quad (12)$$

From the above equation (12), the throughput rate TP is measured based on the data packets successfully received DP_{rec} and the data packets sent DPT_{sent} . It is measured in terms of percentage (%). The sample calculations for throughput using the proposed OLC-ROR method, existing SRR [1], and anchor-based routing [2] are given below.

Sample calculation for throughput

- Proposed OLD-ROR: With 25 number of data packets to be sent and 22 number of data packets received at the sink node, the overall throughput rate is measured as given below.

$$TP = \frac{22}{25} * 100 = 88\%$$

- Existing SRR [1]: With 25 number of data packets to be sent and 21 number of data packets received at the sink node, the overall throughput rate is measured as given below.

$$TP = \frac{21}{25} * 100 = 84\%$$

- Existing anchor-based routing [2]: With 25 number of data packets to be sent and 20 number of data packets received at the sink node, the overall throughput rate is measured as given below.

$$TP = \frac{20}{25} * 100 = 80\%$$

Table 6, given below, shows the tabulation results of throughput for variant number packets considered in the range of 25 to 250 for three different methods, OLC-ROR, SRR [1], and Anchor-based Routing [2].

Table 6: Tabulation for throughput

Number of data packets	Throughput (kbps)		
	OLC-ROR	SRR	Anchor-based Routing
25	88	84	80
50	85.35	82.15	79.35
75	81.25	80.45	78.15
100	80.35	77.15	77.55
125	80.25	75.35	73.25
150	80.15	74.25	72.15
175	78.25	71.55	65.35
200	75.35	70.35	64.15
225	75.55	70.15	62.25
250	75.15	68.45	60.3

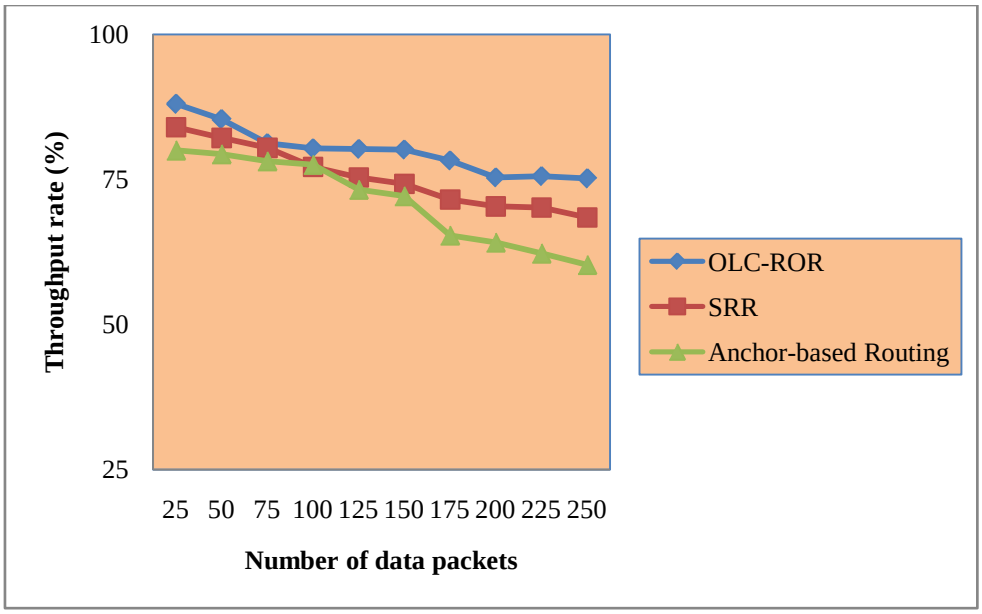

Figure 6: Measure of throughput over number of data packets

Figure 6, given above, shows the graphical representation of throughput rate. The figure x-axis refers to the number of data packets considered for experimentation, and the y-axis refers to the throughput rate. Here, the data packets considered for experimentation differ in the range of 25 to 250, with the packet size being 512 bytes for a maximum node speed of 20 km/hr spreading over a radio range of 250 m. From the figure, it is illustrative that the rate of throughput decreases with the increase in the number of data packets. As a result of that, with the increase in the number of data packets to be sent to the sink node specified for a stipulated destination node, the number of intermediate nodes in the network increases, and therefore the throughput rate reduces. However, from the simulation it is evident that with 25 number of data packets to be sent, the number of data packets received at the sink node using OLC-ROR method was found to be 22, 21 number of data packets received at the sink node using SRR [1] and 20 number of data packets received at the sink node using anchor-based routing [2]. From this, it is inferred that the throughput rate is found to be higher using the OLC-ROR method because of the application of Rabin signature and Onion routing. With this, anonymous communication over a computer network is said to be ensured. As a result of that, the nodes are encapsulated in layers, and the encrypted data is transmitted via a series of relay nodes called onion routers, uncovering the data's next destination. In this manner, security for the node carrying the data packets is said to be ensured. Besides, genuineness of the nodes in onion routers is established by applying the Rabin signature following random padding. In this way, throughput is said to be improved using the OLC-ROR method by 6% compared to [1] and 13% compared to [2], respectively.

VI. Conclusion

In this paper, we present a secured routing in Wireless Sensor Network (WSN) for the Internet of Things (IoT) using the Optimized Load Centroid and Rabin Onion Routing (OLC-ROR) method. The main aim is to improve the throughput rate and minimizes the routing overhead and route acquisition latency. Most of the optimal routing mechanisms focus on the energy consumption aspect and adopt the source location privacy and clustering for data routing. As a result, such solutions are non-feasible in dynamic scenarios where security plays a major role in routing. The proposed method designs a method that not only reduces the routing overhead and route acquisition latency but also improves the throughput rate, ensuring security in a significant manner. First, optimal route identification was made by determining the route possessing minimum load centroid and the residual energy, therefore reducing routing overhead. Next, the optimized secured routes were identified based on Onion routers using encapsulation, which reducing the route acquisition latency. Furthermore, the proposed method concentrated on the genuineness of the node that was ready to be routed using a Rabin signature, which ensured the throughput rate and therefore forming security. Simulation results have shown the OLC-ROR method effectiveness in securing the IoT network route as well as its low routing overhead and route acquisition latency with higher throughput.

References Références Referencias

1. Yu He, Guangjie Han, Hao Wanga, James Adu Ansere, Whenbo Zhang, "A sector-based random routing scheme for protecting the sourcelocation privacy in WSNs for the Internet of Things", Future

Generation Computer Systems, Elsevier, Feb 2019 [Sector-based Random Routing (SRR) method]
2. Catalina Aranzazu-Suescun and Mihaela Cardei, "Anchor-based routing protocol with dynamic clustering for Internet of Things WSNs", EURASIP Journal on Wireless Communications and Networking, Springer, Jul 2019
3. Hao Wang, Guangjie Han, Lina Zhou, James Adu Ansere, Wenbo Zhang, "A Source Location Privacy Protection Scheme Based on Ring-loop Routing for the IoT", Computer Networks, Elsevier, Nov 2018
4. Arezou Ostad-Sharif, Hamed Arshad, Morteza Nikooghadam, Dariush Abbasinezhad-Mood, "Three party secure data transmission in IoT networks through design of a lightweight authenticated key agreement scheme", Future Generation Computer Systems, Elsevier, May 2019
5. Ilhem Souissi, Nadia Ben Azzouna, Lamjed Ben Said, "A multi-level study of information trust models in WSN-assisted IoT", Computer Networks, Elsevier, Jul 2019.
6. Jai Kumar Vinayagam, C.H. Balaswamy, K. Soundararajan, "Cross-layered-based adaptive secured routing and data transmission in MANET", International Journal of Mobile Network Design and Innovation, Vol. 9, No. 1, 2019, Inderscience
7. Hongsong Chen, Caixia Meng, Zhiguang Shan, Zhongchuan Fu,Bharat K. Bhargava, "A Novel Low-Rate Denial of Service Attack Detection Approach in Zig Bee Wireless Sensor Network by Combining Hilbert-Huang Transformation and Trust Evaluation", Security and Privacy For Cloud and IoT, IEEE Access, Mar 2019.
8. Shiju Sathyadevan, Krishnashree Achuthan, Robin Doss, Lei PAN," Protean Authentication Scheme A Time-Bound Dynamic Key Gen Authentication Technique for IoT Edge Nodes in Outdoor Deployments", IEEE, Jul 2019.
9. Turki Ali Alghamdi, "Convolutional technique for enhancing security in wireless sensor networks against malicious nodes", Human-centric Computing and Information Sciences, Springer, Jul 2019.
10. Ismail Butun, Patrik O sterberg, Houbing Song, "Security of the Internet of Things: Vulnerabilities, Attacks and Countermeasures", IEEE Communications Surveys & Tutorials, Oct 2019.
11. Yaw-Wen Kuo, Cho-Long Li, Jheng-Han Jhang, and Sam Lin, "Design of a wireless sensor network based IoTplatform for wide area and hetero generous applications", IEEE Sensors Journal (Volume: 18, Issue: 12, June15, 15 2018).
12. Geetha D. Devanagavi, N. Nalini and Rajashekhar C. Biradar, "Secured routing in wireless sensor networks using fault-free and trusted nodes", International Journal of Communication Systems, Wiley Online Library, Oct 2014.
13. Ming Luo, Yi Luo, Yuwei Wan, and Ze Wang, "Secure and Efficient Access Control Scheme for Wireless Sensor Networks in the Cross-Domain Context of the IoT", Security and Communication Networks, Wiley, Feb 2018
14. Deebak B D, Fadi Al-Turjman, "A Hybrid Secure Routing and Monitoring Mechanism in IoT-based Wireless Sensor Networks", Ad Hoc Networks, Elsevier, Oct 2019
15. Travis Mick, Reza Tourani, Satyajayant Misra, "LASeR: Lightweight Authentication and Secured Routing for NDN IoT in Smart Cities", IEEE Internet of Things Journal (Volume: 5, Issue: 2, April 2018)
16. Khalid Haseeb, Naveed Islam, Ahmad Almogren, Ikram Ud Din, Hisham N. Almajed, Nadra Guizani, "Secret Sharing-Based Energy-Aware and Multi-Hop Routing Protocol for IoT Based WSNs", Mobile Edge Computing and Mobile Cloud Computing: Addressing Heterogeneity and Energy Issues of Compute and Network Resources, IEEE Access, May 2019
17. Catalina Aranzazu Suescun and Mihaela Cardei," Anchor-based routing protocol withdynamic clustering for Internet of Things WSNs", EURASIP Journal on Wireless Communications and Networking, Springer, Jul 2019
18. Imad Jawhar, Nader Mohamed, Jameela Al-Jaroodi, "Networking architectures and protocols for smart city systems", Journal of Internet Services and Applications, Springer, Jan 2018
19. Ramesh Sekaran and Ganesh Kumar Parasuraman, "A Secure 3-Way Routing Protocols for Intermittently Connected Mobile Ad Hoc Networks", Hindawi Publishing Corporation, The Scientific World Journal, Jul 2014
20. Songxiang Yang, Lin Ma, Shuang Jia, Danyang Qin, "A Novel Markov Model-Based Low-Power and Secure Multihop Routing Mechanism", Journal of Sensors, Hindawi, Oct 2019