IJAREEIE

e-ISSN: 2278-8875
p-ISSN: 2320-3765

International Journal of Advanced Research

in Electrical, Electronics and Instrumentation Engineering

Volume 11, Issue 5, May 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.18

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (IJAREEIE)

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.18|

||Volume 11, Issue 5, May 2022||

|DOI:10.15662/IJAREEIE.2022.1105029 |

Secure Confusion based Bidirectional Routing for Internet of Things

Sandeep Krishna K

Lecturer, Dept. of Electronics Engineering, Sree Narayana Polytechnic College, Kottiyam, India

ABSTRACT: Mobile services in Internet of things (IoT) play an important part in our day-to-day activities. In the field of mobile service computing, the routing of IoT has an eminent role. In the resource constrained IoT network, geometric routing is an efficient routing scheme for mobile services. Unfortunately, the protection of secret data is not guaranteed in geometric routing. So, privacy protection is an important problem for mobile service in IoTs. As the resources are constrained in IoT, the encryption or hashing techniques is not a solution in geometric routing. In this paper, we propose a secure confusion based bidirectional routing (SCBR) to protect the private data attached to the corresponding node. A coordinate confusion mechanism is adopted in the proposed routing scheme that attributes each node, an anonymous coordinate and hence the private data is protected. A bidirectional routing scheme is used for data transmission with anonymous coordinate. The simulation results prove that the proposed routing method guarantees anonymity, efficiency and scalability.

KEYWORDS:Internet of things (IoT), privacy, geometric routing, coordinate confusion mechanism, bidirectional routing

I. INTRODUCTION

In our daily life, Internet of things plays a main role. In IoT, different devices are connected to the internet to exchange data.In the field of mobile service computing the routing of IoT is given priority. In IoT, as the devices are smart, the resources are constrained. Geometric routing is an efficient solution for the resource constraint IoT. Geometric routing is a coordinate-based routing and it consists of greedy embedding and greedy forwarding. A virtual coordinate is attributed to every node in geometric routing. In greedy forwarding every node selects a nearby node that is closer to the target node. In geometric routing, every node keeps the coordinates of the neighbours only and in greedy forwarding the shortcuts [1] of the network topology is being used. So geometric routing ensures efficiency and scalability. In certain schemes of geometric routing, for example; practical isometric embedding [2], prefix embedding [3], [4], simple and succinct coordinate structure offers lightweight calculations. In addition to that, mobility is also offered. So geometric routing is the best choice for mobile services in IoT.

All other IoT routing schemes face the privacy issue. Similarly geometric routing also faces this issue. In geometric routing the node coordinate discloses topology information. So, it becomes easy for the network attackers to reconstruct the embedded topology thereby obtaining the relation between any two nodes in the topology. The location is also revealed to the network attacker. This enables the attacker to obtain the secret data.Encryption and hashing are the two major approaches to solve the privacy issues. But these approaches are not effective in geometric routing because it causes more consumption of resources. Some of the privacy protection approaches do not depend on hashing or encryption. The private data is valuable only when it is associated with the corresponding node i.e., the health data of a person is valuable only when he owns the wearable device. When we detach the device from that person the health data becomes meaningless. Similarly, when the private data is detached from the corresponding node, it becomes meaningless and it remains useless to the network attackers.

This paper proposes a secure confusion based bidirectional routing (SCBR) scheme that provides an anonymous routing in the resource constraint IoT networks. The proposed routing uses a coordinate confusion mechanism in order to secure the private data. Thus, the network attacker is unable to identify the communicating nodes. By using bidirectional routing scheme, the private data can be passed over from the initial node to the target node via the shortest path, in the presence of confusion node or anonymous agent.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.18|

||Volume 11, Issue 5, May 2022||

|DOI:10.15662/IJAREEIE.2022.1105029 |

II. RELATED WORK

Today we all live in a smart world. In such a world mobile service in IoTs have great importance. Lots of technologies are being used in mobile services for effective transmission and management. The main problem faced by IoT is the security issue.This research paper aims on privacy protection. The privacy protection mainly targets on data and location of a sensor node. The process of encryption ensures the data security when it is transferred over the network. The location of IoT device is protected by location privacy protection.

Earlier geometric routing schemes [5], [6], use nodes location (physical positions) as coordinate for greedy routing. But these schemes face three issues. First issue is the local minimal i.e., when the forwarding node approaches the destination node than its neighbours, the packet gets stuck there. Second issue is the non-practice i.e., it is not easy to find the physical location for each node. The third one is the inefficiency i.e.,the physical coordinate discloses geographical information. The issue of non-practice is solved by selecting virtual coordinates by certain routing schemes [7], [9]. The virtual coordinate is obtained by the technique of embedding in metric spaces. But these embedding schemes does not ensure theoretical guarantee.

Kleinberg [8] put forth that greedy algorithm is the most suitable approach for arbitrary graphs and asserted that each graph has a greedy embedding technique in hyperbolic space. He investigated that in the graph, the minimum spanning tree can be used for greedy hyperbolic embedding.Julien Herzen et al. [2] proposed a distributed protocol that results in greedy embedding. He proved that so called PIE is more efficient routing scheme that can achieve better results by often finding the shortest path. In internet like graphs this scheme works very well. He found that this scheme offers polylogarithmic scalability. Hofer et al. [3] put forth a darknet routing scheme that focuses on the prefix embedding. In this scheme address representations are precisely used to offer success to the embedding. Thus, shortest paths are achieved in this scheme. This embedding scheme is more effective than other heuristic embedding.

Yanbin sun et al. [4] proposed a bit-string oriented prefix embedding scheme and also focused on succinct prefix embedding schemes in geometric routing. Greediness is guaranteed by the above embedding schemes. Even though these two schemes don't ensure the privacy of the geometric based routing, SPrefix–B can guarantee greediness, succinctness and low path stretch.X Yao et al. [10] investigated a lightweight no-pairing ECC-oriented ABE scheme to address secure communication and cipher-text access control in the resource constraint IoT networks. The proposed scheme achieved both lightweight and ABE. The comparison of KP-ABE schemes and CP-ABE schemes are done to show us that the above-mentioned scheme is a lightweight one. It has low overhead communication and low computation overhead. Here the scheme is a KP-ABE scheme and it is well suited for resource constraint IoT networks.

S Singh et al. [11] analysed several lightweight cryptographic algorithms that is based on the key size, number of rounds, block size and structures. This paper discussed a security architecture in IoT for resource constraint background. Low resource devices do calculations in an IoT scenario but these devices are primitive in memory, power consumption, battery life and computations. These algorithms are suitable to handle software and hardware implementations. This paper focused on a scheme that is applicable to the smart home environment.

B Muthusenthil et al. [12] focused on preservation of privacy of a geographic routing that is cluster based in MANET. Selection of the cluster head is based on the node value which in turn is based on the mobility of the node, degree difference and residual energy. For anonymity a group signature scheme is used by the cluster head. The proposed scheme improves the delivery ratio and results in low computation overhead and energy consumption. Here the routing packets are protected by encryption.

III. SECURE CONFUSION BASED BIDIRECTIONAL ROUTING

The main objective of SCBR is to provide an anonymous routing in such a way that the private data is protected from the network attackers and the attackers cannot find the particular node to which the data belongs to. In this session we discuss about Wireless Sensor Network Initialization, greedy embedding, coordinate confusion mechanism and bidirectional routing.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.18|

||Volume 11, Issue 5, May 2022||

|DOI:10.15662/IJAREEIE.2022.1105029 |

A. ***WIRELESS SENSOR NETWORK INITIALIZATION:***

Wireless Sensor Network (WSN) and IoT have got great importance in the modern world of wireless communication. Wireless sensor network can be described as a network of devices that can communicate through wireless links. They can also monitor physical or environmental conditions i.e., pressure, temperature, sound etc. A WSN comprises of thousands of sensor nodes. WSN necessitate the security mechanism which appropriately works with high protection methods which provide the authorization of nodes in the network to stay away from malicious activities and offer the better performance.In this module, a network model is created with number of nodes. The random x and y position of each node is assigned then the coverage area of sensor node is set. Each node is assigned 1millijoule energy.

B. ***GREEDY EMBEDDING:***

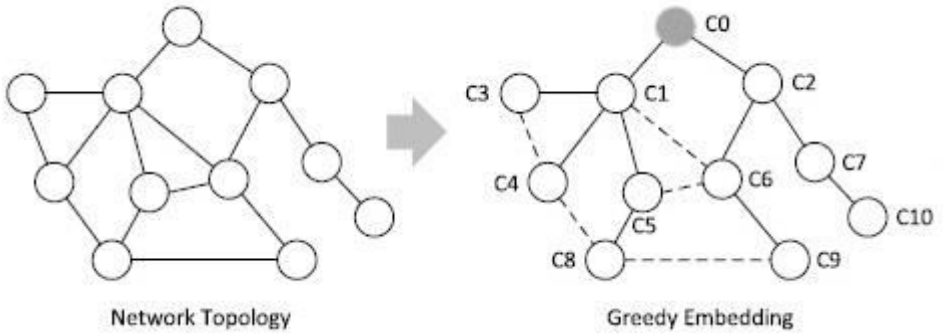


Fig 1. Process of greedy embedding

Greedy embedding is an effective technique in which the network topology is embedded into the metric space and a virtual coordinate is assigned to each node. Firstly, the greedy embedding is explained in detail and the analysis of the embedding process is done. Lastly, the scheme of embedding in SCBR is presented. The greedy embedding process is defined here. In a graph G (V, E) for a metric space (X, d), embedding from G to X is indicated by a function f: V → X, where V is called the node set of G, E is called the edge set of G and d is the metric of X. For ∀v, u ∈ G, ∃w ∈ Nv (Nv is the neighbor set of v) and w ≠ u, such that: d(f(v), f(u)) > d(f(w), f(u)). The greedy embedding guarantees complete routing success according to this definition.

There are two steps in greedy embedding. First, the spanning tree is derived from network topology. Spanning tree extraction is done by using various distributed protocols. Then the spanning tree is greedily embedded into the metric space. An initial coordinate is given to the root node and each node derives its coordinate on the basis of its parent coordinate, the edge weight, and additional information. Several embedding methods are adopted by SCBR. Here we use a Prefix-B method.

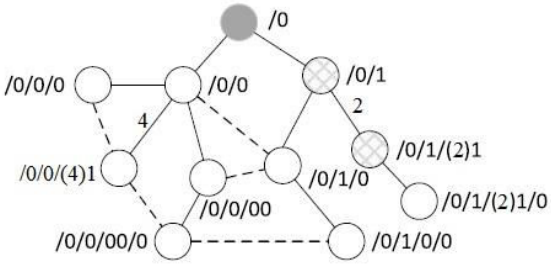


Fig 2. Bit-string prefix embedding

As shown in figure 2, Prefix-B method assigns a coordinate of prefix tree to each node. An initial coordinate /0 is given to the root node. A bit-string is assigned to every non-root node by their parent nodes. The coordinate is

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.18|

||Volume 11, Issue 5, May 2022||

|DOI:10.15662/IJAREEIE.2022.1105029 |

attained by attaching the bit-string to the parent coordinate. If there is weight on the edge, the bit-string is also assigned that weight. Given example, a parent node with bit string coordinate /0/0 assigns its one of the child nodes a bit-string 1. The edge weight between parent node and that child node is 4 so the coordinate of that child node will be /0/0/(4)1.

C. ***COORDINATE CONFUSION MECHANISM:***

In this mechanism, an anonymous coordinate is assigned to each node that is related to virtual node. The real node, to which the virtual node directly or indirectly connects to, is the anonymous agent or confusion node. In the routing of SCBR, the anonymous coordinate is used and hence the network attacker is unable to find the real coordinate of destination node. Even though the topology information is inherent in the anonymous coordinate; the anonymity of SCBR is guaranteed. A tree structure can be inferred for the anonymous coordinate rather than the entire topology. The network attacker cannot find the actual coordinate in the presence of a secret coordinate because the secret coordinate is unable to reveal the nontree edge. In the topology, even though the two corresponding nodes are very near, the distance from the actual coordinate to the secret coordinate is very large. Two steps are there in the process of coordinate confusion mechanism. Firstly, an anonymous agent is determined by each node and then it attains an anonymous coordinate from anonymous agent. An anonymous agent is selected on the basis of levels that are selected by the number of hops.

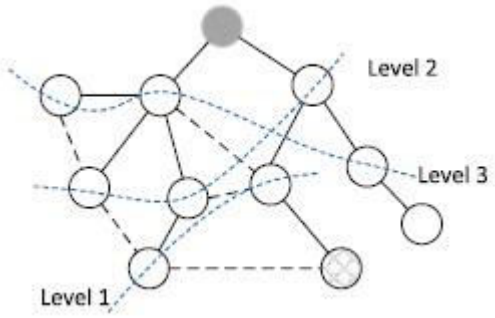


Fig 3. Levels of confusion node

In figure 3, even though a node belongs to various levels, the following two selection methods can handle the situation easily. Two selection strategies are used for finding the anonymous agent i.e., Random Selection (RS) and Distance based Selection (DS). In both these strategies, the request node is sent a request packet. The request packet contains a number i and other related information. The level on which the anonymous agent is selected, is indicated by the number i. The information contained in the request is used for constructing the anonymous coordinate. In the request packet, the routing path is recorded by each forwarded node. The source routing path is attained by the confusion node.

The flow chart of Random based selection strategy is detailed in figure 4, when a request packet p is received by a node u.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.18|

||Volume 11, Issue 5, May 2022||

|DOI:10.15662/IJAREEIE.2022.1105029 |

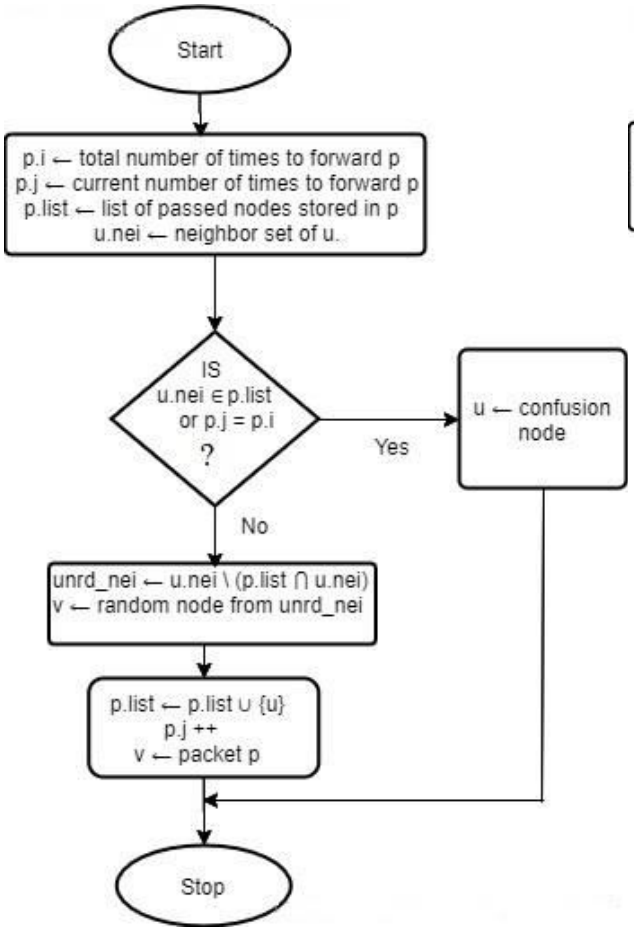


Fig. 4. Random based selection strategy

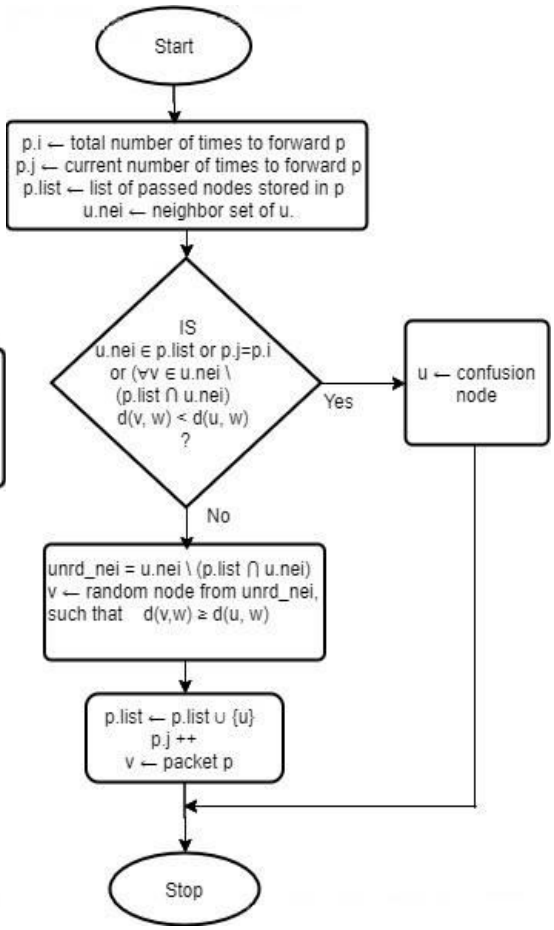


Fig 5. Distance based selection strategy

In Random selection method, a neighbor is randomly selected by the request node and the request packet is forwarded to a neighbor. Anonymous agent is found after forwarding i number of times. In the request packet, the passed node is recorded in order to avoid request from entering the loop. When packet enters a node that has j hops ($i \geq j$) with no unrecorded neighbor, the process of forwarding ends and that node is the confusion node or anonymous agent. In Distance based selection method, a neighbor is selected by the request node that is far away from the node corresponding to its coordinate distance. In certain cases, the distance is equal from the neighbors to the node. In such cases it randomly selects the neighbors. Then the neighbor is forwarded the request packet. In forwarding, every time the next hop will be far away from the request node corresponding to its coordinate distance. The anonymous agent can be obtained after i times of forwarding. Figure 5 shows the flow chart of distance based selection strategy, where u denotes node, d denotes coordinate distance and w denotes request node.

When the anonymous agent is determined by the request node, a virtual node is produced by it. Then the coordinate of the virtual node is sent back to its request node. The hop number from anonymous agent to virtual node determines the anonymous coordinate. According to the number of hops, the request node can change the anonymous coordinate. This hop number is present in the request packet. Then the anonymous agent will randomly produce the bit-string allotted to the virtual node.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.18|

||Volume 11, Issue 5, May 2022||

|DOI:10.15662/IJAREEIE.2022.1105029 |

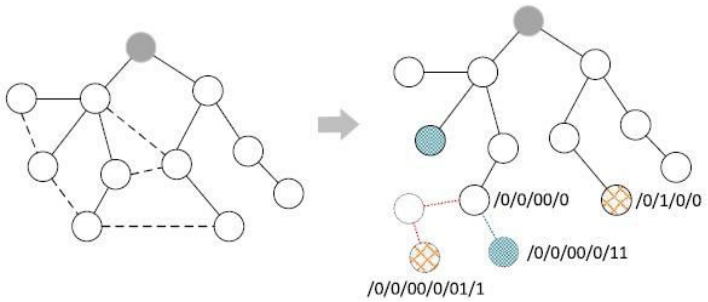


Fig 6. Coordinate confusion example

The coordinate confusion in two nodes (solid lines of blue and red node) is shown in figure 6. The anonymous agent has the coordinate /0/0/00/0 at level 1. The anonymous coordinate of solid lined red node is the coordinate /0/0/00/0/01/1 of the dash lined red node. The coordinate distance between two nodes in red is 8 hops but on the whole topology the distance is 3 hops only. As the difference between the two distances is larger, the coordinate confusion mechanism will be better.

D. ***BIDIRECTIONAL ROUTING SCHEME:***

In existing hybrid routing, when the network grows, more number of nodes are required for routing. Hence the routing path length also increases. This results in worst efficiency and high routing cost. In order to overcome this problem, SCBR adopts a bidirectional routing scheme. In this scheme, bidirectional search [13] applied using Dijkstra's algorithm [14] and the search started independently from the source node and destination node simultaneously. In the middle of the path the search stopped. Thus, the shortest path can be found with minimum cost. Dijkstra algorithm will provide some distance values initially and this will be modified in the further steps. The node from which we start can be called the initial node. Initial node is given a tentative distance value zero and the other nodes is given infinity. All the nodes are marked unvisited, the initial node is the current node. An unvisited set is formed by using all the unvisited nodes except current node. The tentative distances of all the unvisited neighbor of the current node are calculated. For example, a tentative distance of 7 is given to the current node A, and the edge to which it is connected to the neighbor B has a length of 2, then 7+2=9 will be the distance to B through A. Initially we have assigned a tentative distance of B. If the calculated distance (9) is less than this tentative distance, then overwrite that distance. Even if we find a neighbor, it is not marked as visited and it exists in unvisited set. When we stop considering all the neighbors of current node, it is marked as visited and hence removed from unvisited set. A visited node is not checked again and the distance calculated is final. When the destination node is visited, the algorithm is stopped. In bidirectional routing scheme, each node uses an anonymous coordinate for the process of routing. So, the terminus of routing is the virtual node from the view point of network attackers. In bidirectional routing scheme, the shortest path is always found and the packets are forwarded from the initial node to the real target node in the presence of confusion node. Here the confusion node only knows the real destination node because it contains source routing information

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.18|

||Volume 11, Issue 5, May 2022||

|DOI:10.15662/IJAREEIE.2022.1105029 |

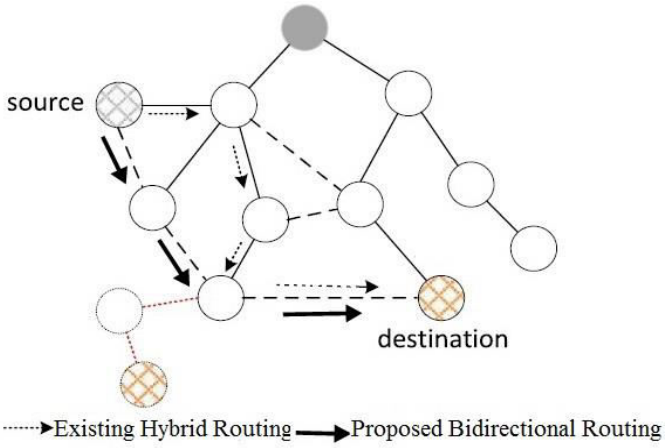


Fig 7. Hybrid Routing and Bidirectional Routing

Fig. 7 shows the existing hybrid routing and proposed bidirectional routing. The existing hybrid routing comprises of greedy routing and source routing. This type of routing requires more number of nodes and the routing path will also be longer. This in turn will affect the efficiency of the routing scheme. In the proposed bidirectional routing, the routing is done by the shortest path and it requires less number of nodes.

IV.RESULTS AND DISCUSSION

Our scheme is evaluated from two aspects: the anonymity and the efficiency by using MAT LAB simulation software.

ANONYMITY

The confusion distance can be defined as the coordinate distance from virtual node to real node. This distance measures the anonymity. As confusion distance is larger, it will be difficult for the network attackers to find the real destination node. Fig. 8 shows that the confusion distance when network grows. In the proposed routing, when the number of nodes increases the confusion distance also increases. So, the anonymity is guaranteed.

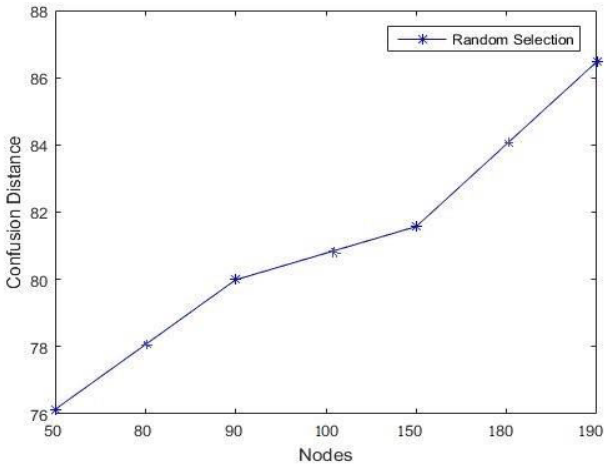


Fig 8. Confusion distance

EFFICIENCY

Efficiency of SCBR is determined on the basis of two aspects; one is path stretch and the other is path length. The path stretch can be defined as the ratio between routing path length and shortest path length. When the path stretch is lower, the routing scheme will be efficient.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.18|

||Volume 11, Issue 5, May 2022||

|DOI:10.15662/IJAREEIE.2022.1105029 |

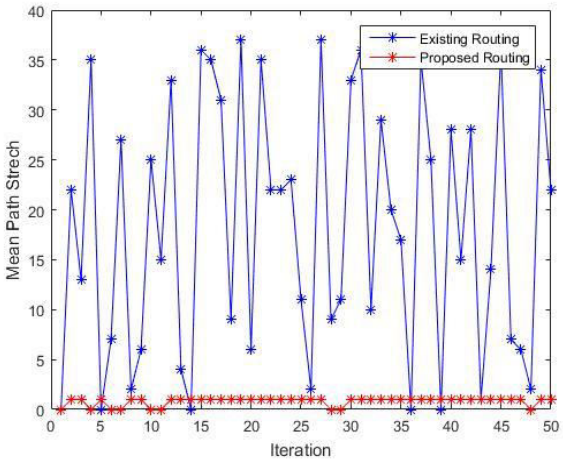


Fig 9. Mean path stretch for different test cases

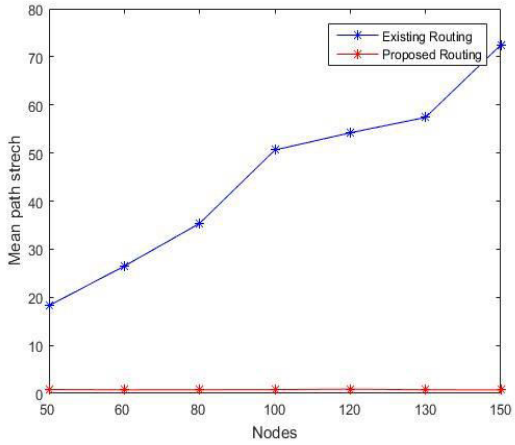


Fig 10. Comparison of Mean path stretch

Fig. 9 shows mean path stretch of existing and proposed routing for different test cases. In the existing routing the path stretch is higher and it is indicated in blue colour. The lower path stretch of the proposed routing is indicated in red colour.

TABLE I
COMPARISON OF MEAN PATH STRETCH

N	50	60	80	100	120	130	150
Existing Mean Pathstretch	18.26	26.48	35.36	50.62	54.20	57.40	72.48
Proposed Mean Pathstretch	0.82	0.74	0.76	0.80	0.90	0.76	0.72

Fig. 10 shows the mean path stretch as the network grows. As detailed in table 1, in existing routing, an increase in the number of nodes results in an increase in path stretch and causes worst efficiency. But in the proposed routing the path stretch is low hence the overall efficiency increases.

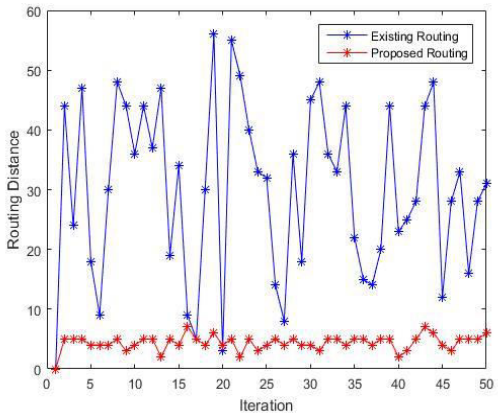


Fig 11. Routing distance for different test cases

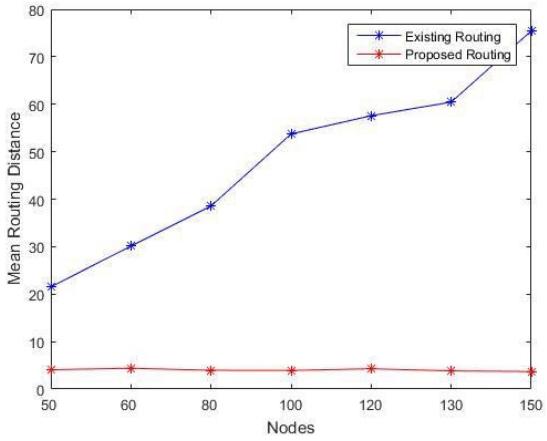


Fig 12. Comparison of Mean Routing distance

Fig. 11 shows the routing distance of the existing and proposed routing for different test cases. In the existing routing the routing distance is longer and it is indicated in blue colour. The shorter routing distance of the proposed routing is indicated in red colour.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 8.18|

||Volume 11, Issue 5, May 2022||

|DOI:10.15662/IJAREEIE.2022.1105029 |

TABLE II
COMPARISON OF MEAN ROUTING DISTANCE

N	50	60	80	100	120	130	150
Existing Mean Routing distance	21.52	30.12	38.56	53.74	57.58	60.46	75.46
Proposed Mean Routing distance	4.08	4.38	3.96	3.92	4.28	3.82	3.70

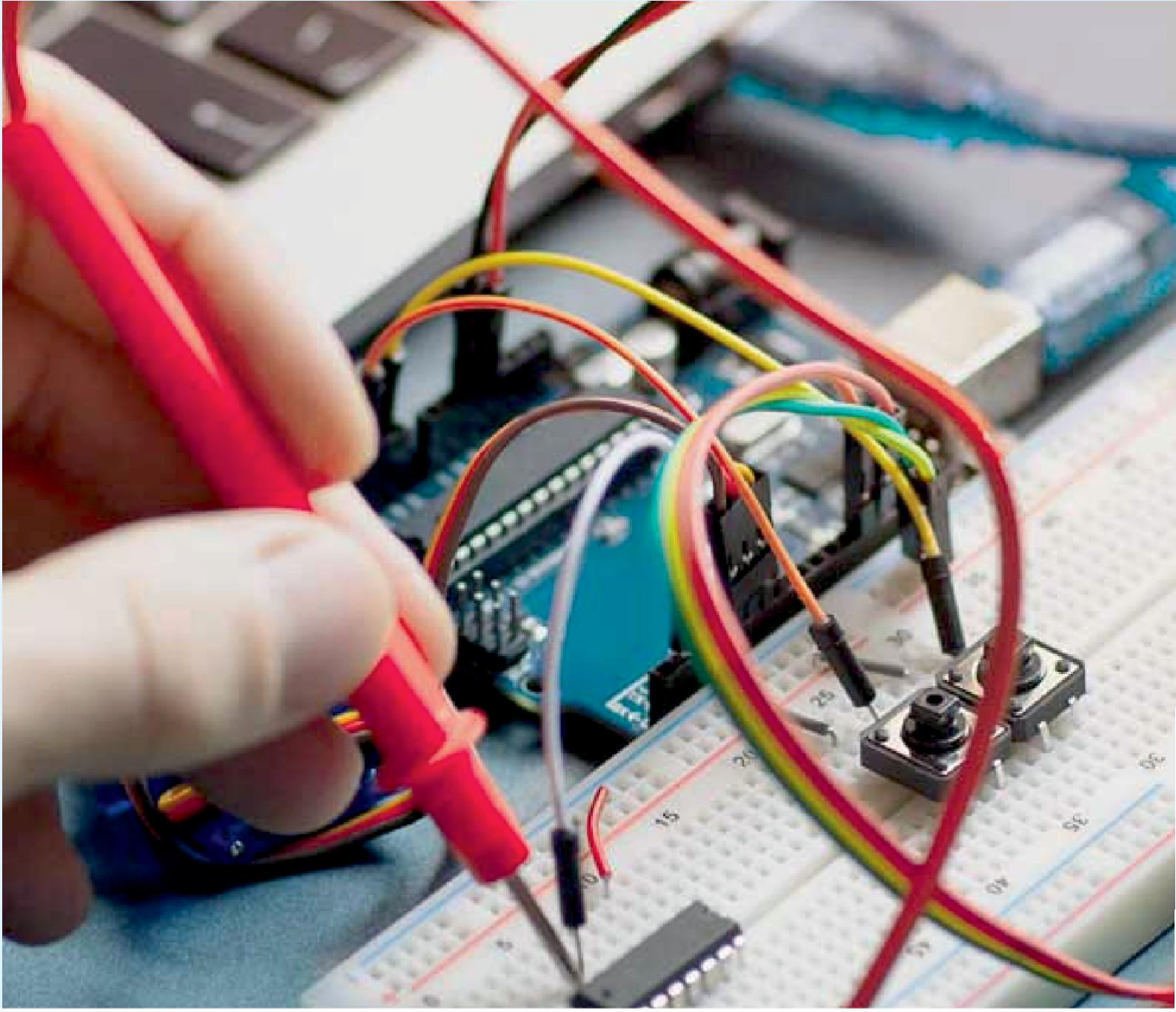
Fig. 12 shows mean routing distance as the network grows. As detailed in table 2, in existing routing, an increase in the number of nodes causes an increase in the mean routingdistance and hence the overall efficiency becomes worst. But in the proposed routing, as the number of nodes increases the mean routing distance remains stable and hence the efficiency will be improved.

V. CONCLUSION

The important goal of this paper is privacy protection of geometric routing in the field of mobile service computing in resource constraint internet of things. This paper proposes a secure confusion based bidirectional routing (SCBR) with a view to secure the private data related to the node from leaking. Most commonly encryption and hashing approaches are being used but SCBR follows a confusion mechanism to decouple the data and the corresponding node coordinate. The proposed routing follows a bidirectional routing scheme that improves the efficiency of routing. The network attacker being unaware of the fact that there is no attack effect on the corresponding node attains the private data. SCBR is a lightweight approach and is adaptable to all geometric based routing schemes. Anonymity, scalability and efficiency are guaranteed through SCBR. The simulation results show that SCBR offers real anonymity at the cost of acceptable efficiency and scalability.

REFERENCES

1. S. Sahhaf, W. Tavernier, D. Colle, M. Pickavet, and P. Demeester, “Efficient geometric routing in large-scale complex networks with lowcost node design,” IEICE Trans. Commun., vol. 99, no. 3, pp. 666–674, 2016.
2. J. Herzen, C. Westphal, and P. Thiran, “Scalable routing easy as PIE: A practical isometric embedding protocol,” in Proc. 19th IEEE Int. Conf. Netw. Protocols (ICNP), Oct. 2011, pp. 49–58.
3. A. Hofer, S. Roos, and T. Strufe, “Greedy embedding, routing and content addressing for darknets,” in Proc. Conf. Netw. Syst. (NetSys), Mar. 2013, pp. 43–50.
4. Y. Sun, Y. Zhang, B. Fang, and H. Zhang, “Succinct and practical greedy embedding for geometric routing,” Comput. Commun., vol. 141, pp. 51–61, Dec. 2017.
5. B. Karp and H.-T. Kung, “GPSR: Greedy perimeter stateless routing for wireless networks,” in Proc. 6th Annu. Int. Conf. Mobile Comput. Netw., 2000, pp. 243-254.
6. P. Bose, P. Morin, I. Stojmenovic, and J. Urrutia, “Routing with guaranteed delivery in ad hoc wireless networks,” Wireless Netw., vol. 7, no. 6, pp. 609-616, 2001.
7. A. Rao, S. Ratnasamy, C. Papadimitriou, S. Shenker, and I. Stoica, “Geographic routing without location information,” in Proc. 9th Annu. Int. Conf.MobileComput. Netw., 2003, pp. 96-108.
8. R. Kleinberg, “Geographic routing using hyperbolic space,” in Proc.26th IEEE Int. Conf. Comput. Commun. (INFOCOM), May 2007,pp. 1902- 1909.
9. A. Caruso, S. Chessa, S. De, and A. Urpi, “GPS free coordinate assignment and routing in wireless sensor networks,” in Proc. 24th IEEE Int. Conf.Comput. Commun. (INFOCOM), Mar. 2005, pp. 150-160.
10. S. Singh, P. K. Sharma, S. Y. Moon, and J. H. Park, “Advanced lightweight encryption algorithms for IoT devices: Survey, challenges and solutions,” J. Ambient Intell. Hum. Comput., vol. 2017, pp. 1-18, May 2017.doi: 10.1007/s12652-017-0494-4.
11. X. Yao, Z. Chen, and Y. Tian, “A lightweight attribute-based encryption scheme for the Internet of Things” Future Gener. Comput. Syst., vol. 49, pp. 104-112, Aug. 2015.
12. B. Muthusenthil and S. Murugavalli, “Privacy preservation and protection for cluster based geographic routing protocol in MANET” WirelessNetw., vol. 23, no. 1, pp. 79-87, 2017.
13. Mariusz Dramski, “Bi-directional search in route planning in navigation” Scientific Journals., 2014, 39(111) pp. 57–62.
14. DIJKSTRA E.W.: A note on two problems in connexion with graphs. NumerischeMathematik 1, 1959, 269–271



INNO SPACE
SJIF Scientific Journal Impact Factor

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

Impact Factor: 8.18

International Journal of Advanced Research

in Electrical, Electronics and Instrumentation Engineering

9940 572 462 6381 907 438 ijareeie@gmail.com

www.ijareeie.com

Scan to save the contact details