2016 International Conference on Internet of Things and Applications (IOTA)
Maharashtra Institute of Technology, Pune, India 22 Jan - 24 Jan, 2016

Enhanced Location Privacy Algorithm for Wireless Sensor Network in Internet of Things

J. Sathishkumar
NIT Surat, India
ds14co001@coed.svnit.ac.in

Dhiren R. Patel
NIT Surat, India
dhiren29p@gmail.com

***Abstract*— Internet of Things is about IP enabled devices connecting and communicating over the globe. Wireless sensor network is one of the important enabling technology of Internet of Things. The accessibility of private information as a part of communication, raise serious concerns over personal privacy. In this context, we present location privacy of sensor network in IoT and related issues.**

Keywords*— Internet of Things; Location Privacy; Wireless Sensor Network.

I. INTRODUCTION

Recently, Internet of things (IoT) has acquired substantial attention owing to the applications and the capabilities it offers. IoT allows people and things to be connected anytime, anyplace, with anything and by anyone, ideally using any path or network and using any service [1]. IoT works on the principle of connecting objects to humans and objects to other objects in various places, times and services together, so as to exchange meaningful information and thus provide wide array of facilities. The ultimate aim of IoT is to make an enhanced world for human beings, in such a way that the objects or things around us will come to know their needs, likes, dislikes and act accordingly, with minimum human intervention and without explicit instructions [2].

The mode of connection between objects and the Internet vary from sensors, RFID, laser scanners, infrared devices, global writing system and other information sensing equipment. Once connected, they can be controlled via Internet; supervised, tracked, and monitored for various information services and data exchange. The implementation of the privacy in such intelligent scenario is of utmost importance to fully utilize their features without causing undue harm and misuse.

Wireless sensor network(WSN) is a non-trivial integral part of IoT because, ample of applications are depending on the huge number of sensors deployed over the network, so that real-time monitoring and processing of data can be transmitted timely to sink. A typical presentation of IoT that addresses various application is shown in Fig 1 [3]. For instance, sensors may be deployed for sending messages to base station that might be in battlefield, to monitor enemys activity. Therefore, it is must and significant to provide confidentiality to the location of sensors source. In this paper, we discuss and explore solution directives for location privacy issues associated with sensors in IoT.

Fig 1. IoT Application [3]

Rest of the paper is organized as follows: Location privacy issues in the wireless sensor network of IoT are discussed in Section II. Further, the algorithm is detailed in section II. Simulation results for the algorithm is shown in section III. Section IV concludes with the references at the end.

II. LOCATION PRIVACY ISSUES IN WSN

In IoT, wireless sensor network is used extensively. Different type of sensors that gather various information might be private which contains the object's location, status, identity, or some other social, business or personal relevant data. For example, assume an object or an event detected by a sensor, it will transmit that information to base station or sink which includes the information related to the events happening within its network. If an intruder is also in the network, then he or she is able to tap and crack the message. This leads to exploitation of the personal sensitive information about when and where a particular concerned event has taken place. This further takes to an

978-1-5090-0044-9/16/$31.00 ©2016 IEEE

effect that the intruder might able to determine the precise object's location and can be able to demolish or control the object, which is a big threat to the entire network. Suppose, the intruder reveals or exposes the location privacy, the information related to identity will be disclosed because the real entities in the identity information has a inversely proportional relationship with virtual information [4].

In WSN, information about location frequently signifies the actual event's physical location, which is critical in the many applications [5]. If the intruder will be able to determine the location information which is sensitive and private that was collected by examining the message, eavesdropper might go to the exact physical location of the event and able to monitor the issues happening in the event. Even though for location privacy lot of approaches exists, they are not suitable to protect and preserve the location of a sensor source in a network that can be applied in scenarios of general network [6], [7].

Zhou et al. [8] have proposed Multi-Routing Random walk algorithm to achieve location privacy in sensor networks. Multi-routing Random Walk algorithm is focusing on protecting the sensors location by bringing the appropriate modifications to sensor routing in-order to make it hard for an intruder to determine the actual location. This strategy can reduce the opportunity of packets being observed by eavesdropper effectively. Fig 2 , represents the idea of Multi-routing Random Walk [8].

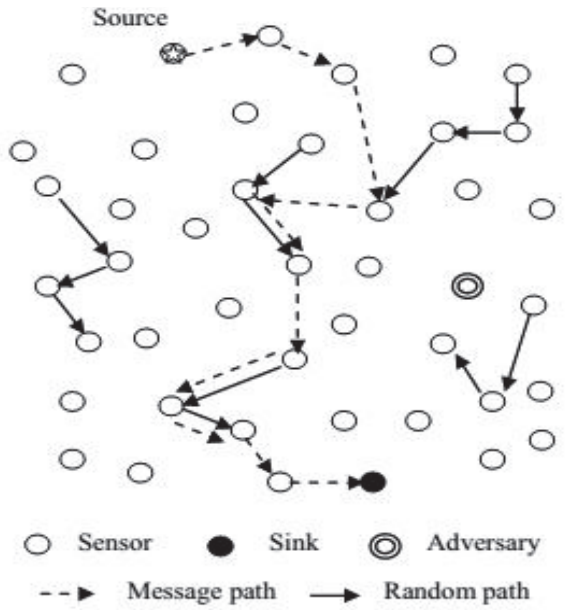

Fig. 2. Multi-routing randomly walk Algorithm [8].

In this algorithm, several random paths were initiated with an affordable number of hops. On each random path, sensors serve as receptors. From source, a packet is forwarded randomly to one of its neighbors. If neighbor is in the random path, then the packet is transmitted in the same path by a predefined direction till it reaches the end of this path. Otherwise, the packet is forwarded to one of its random neighbors. Likewise the packets are forwarded randomly again and again until they reach the sink. However, it is possible that a packet may be forwarded to one of its previous hop's neighbors. Under this circumstances, random walk does not progress and that the path will go in loop. To avoid such instances, Bloom filter can be used with the information of current neighbors and pre-established paths stored in that forwarding packet [9]. When the packet randomly chooses next hop in its neighbors, it should verify whether the neighbor has been already in the filter or not. The packet will be forwarded to a sensor which is not in the filter. Every node follows the same rule to send the packet till it reaches the sink. Even though an eavesdropper happens to detect a packet, the next packet is unlikely to follow the same path, thus rendering the previous observation useless.

However, a flaw is observed in a typical scenario that Multirouting random walk algorithm failed for certain instances. As shown in Fig 3, the path is stuck at node 25. This is due to the constraint of avoiding loops, the path cannot go to 23 and also no further neighbors. Therefore, the path is not able to reach the sink node 21 and hits the dead end.

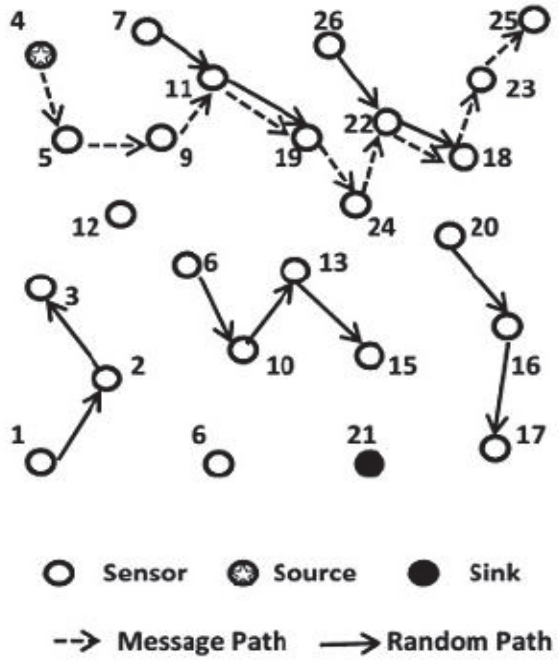

Fig. 3. Failed Case of Existing Algorithm.

To overcome such failures, we modified existing algorithmin such a way that the path will always reach to the sink by using the technique of back-tracking. If the path has no neighbors and it is not the destination node then we backtrack one step to the previous node and delete the current node to avoid revisiting the failure cases. As shown in Fig 4, from node 25, the path will backtrack to

23, and then to 18, from where it will pick up 20 and to destination sink 21.

Assume that the intruder is one of the node in the network and wants to know the origin of the message then two possible cases might arise. One is the actual path going through the intruder, in which case the chances of breaching the privacy of the source location is high. The other case is the actual path not going through the intruder. The more threatening and challenging case is the first case when compared to the second one because the intruder can easily trace back to previous nodes and can be determine the actual source node and related sensitive and important information. Our proposed algorithm assures complete privacy of the source node by taking into the consideration of such challenging scenarios,. For instance, in the first case, though the actual path goes through intruder node, due to the multiple random paths, while tracking back, the intruder will end up with several sources which makes difficult to determine the actual source and thus the privacy of the source is protected.

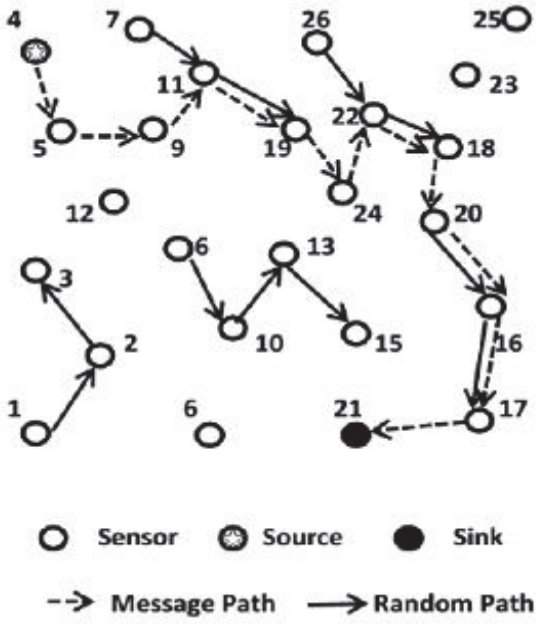

Fig. 4. Success Case of Updated Algorithm.

The novelty in our approach is, the modified algorithm assures that packets reaching to the sink with the promised level of privacy. This implies that our algorithm is efficient than the previous one in terms of utility and privacy. The backtracking approach will make sure that the packets will reach to destination and random paths assures the privacy. More the random paths, more the ambiguity of the source node location.

The proof of correctness of our proposed approach is determined by using probability of a tossing a coin [10]. Assuming the experiment of tossing a coin is conducted infinity times, the chances of getting head is 1 / 2 and tail is 1 / 2. Likewise, if the experiment of multi routing random walk algorithm was conducted infinity times, the chances of the packets reaching to the destination from source in order to assure the completeness of the algorithm is 1 / 2. This is because the path and packets might struck as shown in the above scenario in Fig 3. However, as shown in Fig 4, our proposed approach assures that the packets will reach to destination with probability 1. Therefore, our proposed updated multi routing random walk algorithm is more efficient than the already existing approach.

Algorithm 1: Updated Multi-routing Random Walk

```
Data: N, R where N is No. of Nodes, R is No. of
      Random paths
Result: Successful Packet Arriving at Sink
Curr_Loc=source;
Next_Loc=ChooseNeighbors(Curr_Loc);
Filter;
while (Next_Loc!=sink) do
    if !(Next_Loc in filter) then
        if (Next_Loc!=path) then
            MoveTo(Next_Loc);
        else
            FollowPath(Next_Loc);
        end
        Filter=StoreSensorsInfo(Curr_Loc);
    end
    Next_Loc=PickNeighbors(Curr_Loc);
    if (Next_Loc==null && Next_Loc!=sink) then
        Next_Loc=Backtrack to Previous_Loc(Curr_Loc);
        Filter=DeleteSensorsInfo(Curr_Loc);
    end
end
```

Let 'n' be the number of nodes deployed in the network and 'v' be the number of nodes takes part in the actual path. The time complexity of Multi routing random walk in worst case is O(n), because the path may visit all the nodes to reach sink from the source. O(v) on average case and O(1) in the best case, if sink is immediate next node of the source. The privacy of the source location is directly depends on the number of random paths because more the random paths, more the ambiguity because the chances for actual path togo through the random paths will be more such that it will
make the adversary to end multiple source locations.

TABLE I
COMPARATIVE TIME COMPLEXITY ANALYSIS

Algorithm	Best case	Avereage case	Worst case
Multi routing random walk strategy	O(1)	O(v)	O(n)
Modified Multi routing random walk strategy	O(1)	O(v+b)	O(n)

The time complexity of Modified Multi routing random walk is the same as Multi routing random walk strategy in best case O(1) and in worst case O(n). But, in the average case, the time complexity of the algorithm will be O (v+b), where 'b' is the number of nodes visited and backtracked i.e., visited but not counted in the actual path. Table I provides the information of the time complexity with respect to each algorithms. Although, our proposed algorithm takes more running time than the existing, our approach assures completely that the packets will reach to sink.

III. SIMULATION RESULTS

The algorithm is implemented in MATLAB [11]. We created a suitable scenario of randomly deployed nodes and applied both algorithms. Results are given for failed case of Multi-routing random walk in Fig 5 and the success case for Modified Multi-routing random walk algorithm in Fig 6.

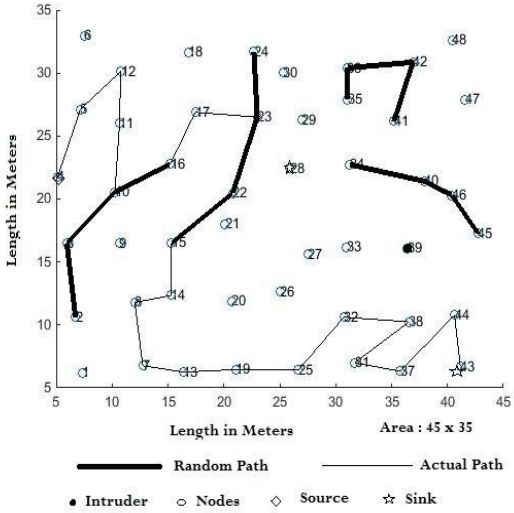

Fig. 5. Simulation results of failed case

The evaluation of this algorithm is carried out by two things. Firstly, the actual path i.e., light line starts from source node and must reach to destination node. Secondly, if intruder wants to trace back to find the source and the path, should lead to many sources results in more ambiguity and makes it difficult to determine the actual source. The results are shown in Fig 5 is the failed case where the actual path struck at node 43, with node 4 as source, node 28 as sink and 39 as intruder. The results of modified algorithm as shown in Fig 6 in which the total number of nodes are 100, with source node as 5, sink node as 35 and node 24 as intruder. The multiple sources are found as 12, 21, 44, 48, 54, 56, 75, 85 and 93.

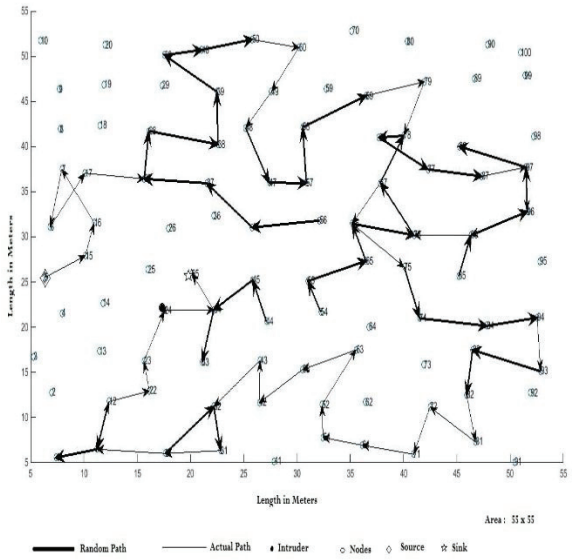

Fig. 6. Simulation Results of Modified Algorithm

IV. CONCLUSION

In this paper, the issues related to the privacy of the source location in wireless sensor network of IoT are investigated. We proposed a modified multi routing random walk algorithm by using back tracking technique which works well in all scenarios and promises with desired level of privacy. The algorithm has been implemented in suitable environment. Analysis and results help us to derive the conclusion that the proposed modified multi routing random walk algorithm works efficiently than the existing approaches.

REFERENCES

[1] G. M. Lee, N. Crespi, J. K. Choi, and M. Boussard, "Internet of things," Proceedings of Springer in *Evolution of Telecommunication Services*. 2013, pp. 257– 282.

[2] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Context aware computing for the internet of things: A survey," *IEEE Journalof Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 414–454,2014.

[3] (2014) The internet of things can drive innovation if you understand sensors. [Online]. Available:http://systemdesign.altera.com/the-internetof-things-can-drive-innovation-if-you-understand-sensors/.

[4] V. Oleshchuk, "Internet of things and privacy preserving technologies," in *in 1st International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace&Electronic Systems Technology*, 2009, pp. 336–340.

[5] Y. Xi, L. Schwiebert, and W. Shi, "Preserving source location privacy in monitoring-based wireless sensor networks," in *Proceedings of IEEE in20th International Symposium on Parallel and Distributed Processing. IPDPS*, 2006, pp. 1–8.

[6] D. Chaum, “Untraceable electronic mail, return addresses and digital pseudonyms,” Proceedings of Springer in *Secure electronic voting*. 2003, pp. 211– 219.

[7] M. G. Reed, P. F. Syverson, and D. M. Goldschlag, “Anonymous connections and onion routing,” *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 4, pp. 482–494, 1998.

[8] L. Zhou, Q. Wen, and H. Zhang, “Preserving sensor location privacy in internet of things,” in *Proceedings of IEEE at Fourth International Conference on Computational and Information Sciences (ICCIS)*, 2012, pp. 856–859.

[9] G. Park and M. Kwon, “An enhanced bloom filter for longest prefix matching,” in *Proceedings of IEEE /ACM at 21st International Symposium on Quality of Service (IWQoS)*. 2013, pp. 1–6.

[10] A. Papoulis and S. U. Pillai, *Probability, random variables, and stochastic processes*. Tata McGraw-Hill Education, 2002.

[11] B. R. Hunt, R. L. Lipsman, and J. M. Rosenberg, *A guide to MATLAB: for beginners and experienced users*. Cambridge University Press, 2014.