ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET) Vol. 7, Issue 9, September 2020

Secured Device to Device communication using Multipath Routing

Mr.S.Allwin Devaraj, S.Lakshmi, M.Mubeen, S.Preetha Elsie Yonggicho
Department of ECE, Francis Xavier Engineering College, Tirunelveli

Abstract: D2D communication refers to a type of technology that enables devices to communicate directly with each other. It does not use any communication infrastructure such as Access points (or) Base stations. Through the D2D communication the devices can communicate with each other without the cellular coverage. This technology is helpful when the devices are present outside the normal coverage. It provides a novel approach to solve poor coverage conditions. Device to Device communication provides the following advantages, it can increase the overall throughput, enhance the coverage, reduce the power consumption. Though the device to device communication effectively improves the network efficiency, it has some problems related to security. Security and privacy are the two important issues that has to be solved in the case of device to device communication. Our system proposes a Multipath Routing Algorithm solution to overcome the issues like eavesdropping in device to device communication.

I. INTRODUCTION

The cellular network we are using is four generations old. The cellular network journey is moving forward, so we need a fast multimedia rich data exchange .So,to boost data rates and reduce latency, there is a need for more efficient techniques. Here comes the device to device communication which allows users in close proximity to communicate directly without using a cellular coverage.

Device to Device communication will help the people who are within the poor coverage or outside the coverage area to communicate with each other directly.It allows the users who are in close proximity to communicate with each other directly.Though the device to device communication provides efficient network,security threat is an important problem.So our proposed system presents a approach which sends a data along multiple paths to prevent security threat especially eavesdropping.In this paper three different multipath routing algorithms are tested and compared for their resistance to eavesdropping.

This paper contains the following sections.Section II provides a review of eavesdropping, Section III provides Existing system,Section IV provides Proposed system,Section V provides Results, Section VI provides Conclusion.

II. REVIEW OF EAVESDROPPING

Eavesdropping can interfere the D2D links.The unauthorized interception of a private communication such as phone call,instant message etc is known as Eavesdropping.Here the transmission channels are used by source node,destination node and an eavesdropping node.The openness of wireless architecture is the one of the reasons for eavesdropping.

The eavesdropping are done as a passive attacks when the received signals cannot be intercepted directly due to encryption.Without finding the content of the signal,the information such as location and identity of communicating parties are intercepted by the eavesdropper by analyzing the pattern of the received signal.Eavesdropping can be manifest in different forms.A user's location can be tracked by the information on nodes that have joined recently a network.

III. EXISTING SYSTEM

As it is more difficult to listen to an encoded message, the most important protection against it is cryptography.In cryptography,the senders and receivers need to calculate the exchange keys.Cryptography is the technique for secured communication in the presence of third

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology
(IJARTET) Vol. 7, Issue 9, September 2020

parties.The principle of cryptography are Data Confidentiality,Data Integrity.Authentication and Non Repudiation.

In cryptography, Encryption and Decryption plays an important role. Encryption is the technique to provide confidentiality. It is the process of converting plaintext into Ciphertext. Decryption is the process of converting Ciphertext into Plaintext.Security of d2d networks include not only the confidentiality,integrity and authentication but also privacy,non-repudiation,revocability of access, and availability and dependability of the network.Though the cryptography act against eavesdropping,it has some limitations too.

A limitations of this approach are that it cannot provide different degree of security for different application.Also advances in quantum computing could make the decoding of encrypted message possible.

IV. PROPOSED SYSTEM

Though there exists many conventional approach such as encryption,it cannot provide the required security needs.So,in our proposed system,multipath routing techniques are used to prevent eavesdropping(a security attack) .

A.Multipath Routing

Multipath routing is a technique in which multiple alternative paths are used to route a information.If the duplicated data are sent via multiple paths,the reliability of data transmission can be improved.The attacker must target only one node,if the data is sent along the single path.Whereas, in case of multipath routing the data is sent along multiple path .So the attacker must target many nodes.

B.Metrics for Multipath Routing

Routing requirements for radio networks are different from that of the wired networks.The evaluation of different network routes can be determined by speed,reliability,secrecy or energy efficiency of the network.Nodes use bandwidth with their own transmission. Nodes interfere with the neighbour nodes.More information,memory and storage are required for multiple paths in routing tables.When choosing usable routes,interference must be taken into account.After choosing the path,the strategy for sending the data along that path must be determined.Then the different path sets must be evaluated.Because of complicated geometry of the path the evaluation of path sets is difficult.They use average distance between the nodes.

$$dpq = \frac{\sum n \in p \; dnq}{hops(p)}$$

C.Methodology

City Section mobility model incorporates the movement of nodes.In our simulation nodes are able to communicate with other nodes within a communication range.We distinguish the nodes as follows ,Source node where the message originates,Destination node where the message terminates . It can be obtained by finding the number of nodes that intercepts the entire message along both paths and dividing it by the total number of nodes with this ratio we are able to determine the effective algorithm against eavesdropping.

D. ALGORITHMS USED

Our simulations compare three different algorithms.

i. Least Interference Path

This algorithm is used to find two paths that have least interference.

According to a redesign of a Dijkstra's algorithm,the first path is selected.The degree of a node is determined by number of other nodes within its transmission range.A node which has a higher degree has greater potential to be eavesdropped.

A path which has fewest potential eavesdropping neighbours is picked up by the Dijkstra's shortest path algorithm.

From the first path the nodes are removed.

Second path is found by simple breadth first search.Second path is more direct than the first.

Dijkstra's shortest path algorithm:

1.All the nodes are marked unvisited.Create an unvisited set which is the set of all unvisited nodes.

2.Let the value of an initial node be zero and set it as current node.

3. Consider all the unvisited neighbour from the current node.From the current node calculate the

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology
(IJARTET) Vol. 7, Issue 9, September 2020

tentative distance.Compare the current value with the tentative value and assign the smaller one.
4.Now consider the current node as visited.This node will not be checked again.
5.When the destination node is marked visited or if there is no connection between initial node and unvisited node stop the algorithm.

ii. Mock Suurballe's algorithm

Step 1 : Dijkstra's algorithm is used to find a path from source to destination.
Step 2 : Nodes in the first path are removed from the graph.
Step 3 : A second path is chosen.
Step 4 : Message is sent over two paths.

iii. Random Direct Path Algorithm

This method finds a path based on the distance of a node to the destination.
Step 1: Nodes adjacent to the source node, shown in red, are evaluated according to their distance to the destination.
Step 2: A shortest-distance first path is chosen.
Step 3 : The first path nodes are removed, and a second path is chosen using the methodology of step 1.
Step 4: Message is sent over two paths.

V. RESULT

		Radius		
Algorithm	**Nodes**	**1500m**	**1000m**	**500m**
Least interference path	5000	0.34	0.21	0.12
	10000	0.19	0.34	0.19
	15000	0.28	0.15	0.11
Mock suurballe's	5000	0.46	0.44	0.38
	10000	0.42	0.41	0.29
	15000	0.45	0.43	0.44
Random direct path	5000	0.49	0.49	0.49
	10000	0.49	0.50	0.48
	15000	0.50	0.50	0.50

Table 1 Eavesdropping Rate

Table 1 shows the eavesdropping rates for each method with different radii

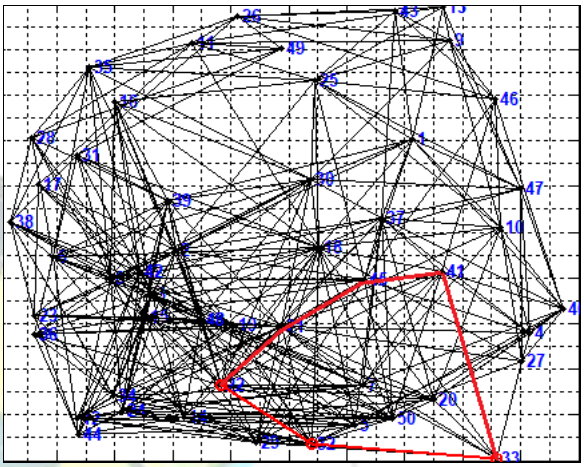

Fig 1 Two Shortest path between the source and destination node

The above figure shows the two shortest path between source and destination.

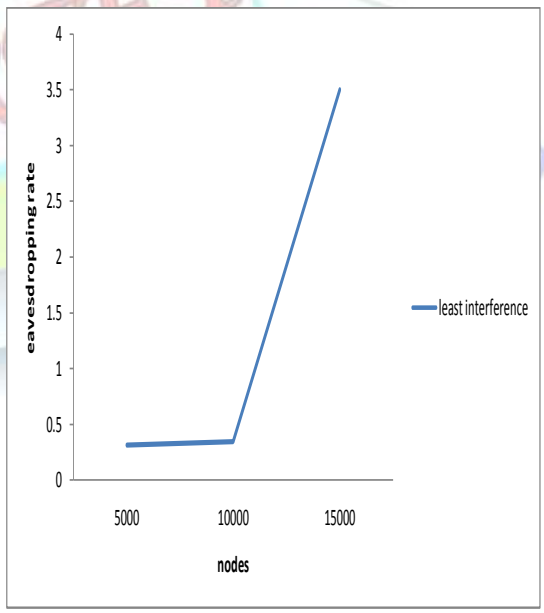

Fig 2 Least intereference path algorithm

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET) Vol. 7, Issue 9, September 2020

The above figure shoes the performance of least interference path algorithm in 5000,10000,15000 nodes.

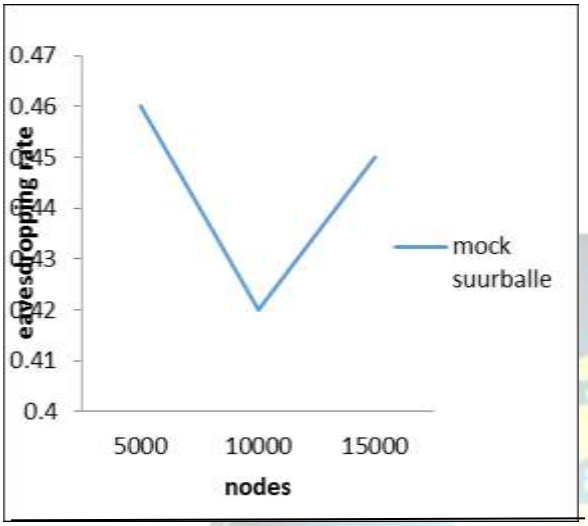

Fig 3 Mock Suurballe's algorithm

The above figure shows the performance of mock suurballe's algorithm in 5000,10000,15000 nodes.

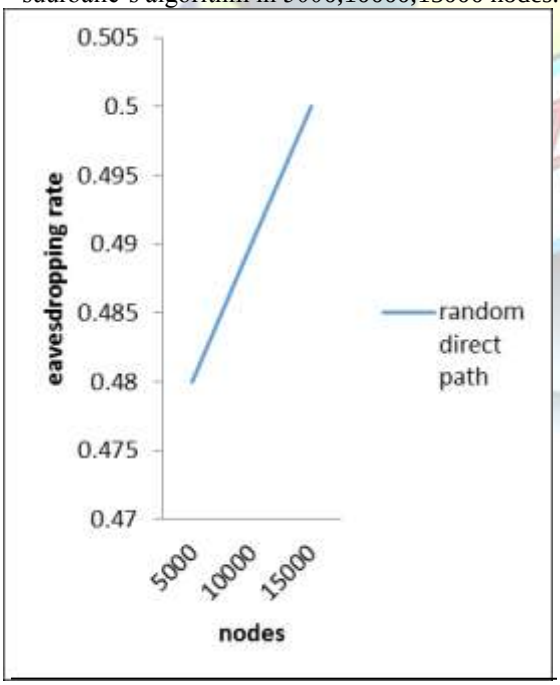

Fig 4 Random direct path algorithm

The above figure shows the performance of random direct path algorithm in 5000,10000,15000 nodes.

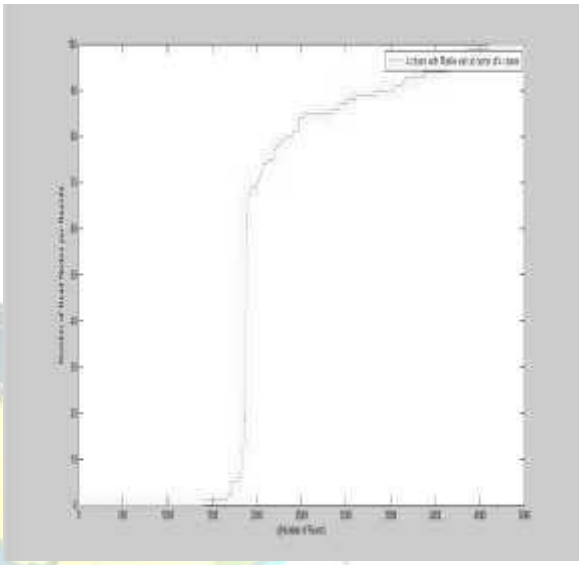

Fig 5 No.of dead nodes in 5000 nodes

The above figure shows the number of dead nodes in total of 5000 nodes.

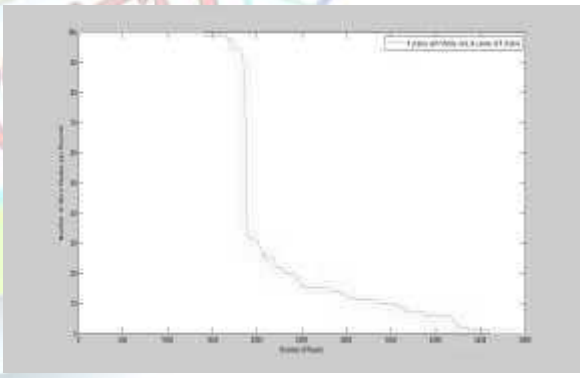

Fig 6 No.of alive nodes in 5000 nodes

The above figure shows the number of alive nodes in 5000 nodes.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET) Vol. 7, Issue 9, September 2020

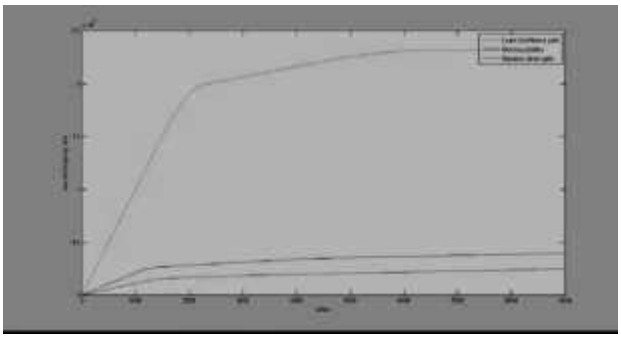

Fig 7 comparison result

Although the attack eavesdropping cannot be completely eliminated,Least interference path algorithm has the lowest eavesdropping rate,when compared to other two algorithms.From the above figure,it is also noted that the eavesdropping rate increases as the radius increases.It is also noted that in Least interference path the eavesdropping rate increases more slowly as the radius increases when compared to other methods.

VI. CONCLUSION

Security plays a vital role. We have presented a survey of the literature on the attack eavesdropping. Specifically,we have considered the defense strategy of multipath routing and the security implications related to eavesdropping. Related works on multipath routing were presented, along with a simulation that tested three different methods.It was found that least interference path algorithm effectively inhibits eavesdropping.It was also found that while increasing the broadcast radius of mobile devices,the eavesdropping rate was also increased.

REFERENCES

Abualhaol I, Muegge S (2016) Securing d2d wireless links by continuous authenticity with legitimacy patterns. In: 2016 49th Hawaii International Conference on System Sciences (HICSS). pp 5763–5771. https://doi.org/10.1109/HICSS.
2016.713

Bhattacharya A, Ghosh SC, Sinha K, Sinha BP (2018) Secure multipath routing for multimedia communication in cognitive radio networks. Int J Commun Netw Distrib Syst 21(1):26–55

han A, Javed Y, Abdullah J, Nazim J, Khan N (2017) Security issues in 5g device to device communication. IJCSNS 17(5):366

Kuperman G, Modiano E (2014) Disjoint path protection in multi-hop wireless networks with interference constraints. In: 2014 IEEE Global Communications Conference. pp 4472–4477. https://doi.org/10.1109/GLOCOM.2014.7037512

Le PH (2012) A performance evaluation of multi-path routing protocols for mobile ad hoc networks. In: 2012 IEEE 15th International Conference on Computational Science and Engineering. pp 484–491. https://doi.org/10.1109/ICCSE.
2012.73

Mavropodi R, Kotzanikolaou P, Douligeris C (2007) Secmr – a secure multipath routing protocol for ad hoc networks. Ad Hoc Networks 5(1):87–99. https://doi.org/10.1016/j.adhoc.2006.05.020. Security Issues in Sensor and Ad Hoc Networks

Mucchi L, Ronga L, Huang K, Chen Y, Wang R (2017) A new physical-layer security measure-secrecy pressure. In: GLOBECOM 2017-2017 IEEE Global Communications Conference. IEEE. pp 1–6. https://doi.org/10.1109/glocom.2017.
8254006

Mumtaz S, Huq KMS, Rodriguez J (2014) Direct mobile-to-mobile communication: Paradigm for 5g. IEEE Wirel Commun 21(5):14–23

Munir A, Qian Z, Shafiq Z, Liu A, Le F (2017) Multipath tcp traffic diversion attacks and countermeasures. In: 2017 IEEE 25th International Conference on Network Protocols (ICNP). IEEE. pp 1–10. https://doi.org/10.1109/icnp.2017.8117547