SURVEY: Topology Hiding In Multipath Routing Protocol In MANET

Akshay Suhas Phalke[1], Prof. M.S.Chaudhari[2],

[1] *Student, Department of Computer Engineering, Sinhgad Institute Of Technology,Lonavala, Maharashtra, India*

[2] *Asst. Prof., Department of Computer Engineering, Sinhgad Institute Of Technology,Lonavala, Maharashtra, India*

ABSTRACT

In this paper we have discussed the multipath routing with its variants. Our purpose is to discuss the different types of the multipath routing mechanism. Here we also put the taxonomy of the multipath routing. Multipath routing is used for the alternate path routing, reliable transmission of data and for better utilization of network resources. We also discussed the multipath routing for topology hiding such as TOHIP.

In multipath routing different parameters such as energy efficiency, packet delivery ratio, shortest path routing, fault tolerance plays an important role. We have discussed number of multipath routing protocol based on different parameters lastly.

Keyword - *Key word1 Multi-path routing, WSN, Topology, Fault Detection, Trust*

1. INTRODUCTION

A wireless sensor network is set of sensor nodes with limited battery supply and limited computational capability. Wireless nodes have limited range and densely deployment in network, which makes it to perform the multi-path routing in wireless network. In WSN data transmission is usually performed in multi-hop manner. To improve the network performance now a day's multipath routing plays an important role in multi-hop wireless sensor network. Current advances in wireless technologies and the manufacture of inexpensive wireless devices have introduced a low-power wireless sensor networks. Because of the low expensive WSN, there use is increased in large areas such as healthcare, target tracking, and environment monitoring.

The main aim of the wireless sensor network is to sense the data and transmit it to the sink node for further processing. Limitations resources of the sensor nodes and unreliability of low-power wireless links with various performance demands of many applications raises many challenges in designing efficient communication protocols for WSN.

Most of the routing protocols are based on the single path routing strategy without considering the effects of traffic load. In single path routing each node selects the path to satisfy the needs of the intended application. In single path routing network throughput cannot be achieved even though there is low computational cost.

When intermediate node or link fails, finding an alternative path to send data to the sink node causes the extra overhead and causes the delay in packet delivery. Because of the constrained resources and unreliable links single path routing cannot guarantee the performance requirements of the various applications. To cope with the limitations of the single path routing another type of routing called multipath routing becomes the promising technique in wireless ad-hoc network.

2. RELATED WORK

[1] Yujun Zhang, Guiling Wang, Qi Hu introduced another type of routing called a geographic routing, which specified that every node keeps the information of the location through the services of the locations.
[2] C. K. Toh, A. N. Le, et al mentioned that to fight attacks numerous secure multipath routing protocols have been proposed, these protocols usually foused on one or a portion of the five security Requirements: confidentiality, integrity, availability, authentication and non-reputation, instead of hiding topology.
[3] M. K. Marina, and S. R. Das mentioned
reliable and energy-aware multipath routing protocol designed to make the energy efficient for WSN, which would provide trustworthy data transmission throughout the network model, but didn't specify that security regarding the introduction of the malicious node in the topology.
[4] L. Abusalah, A. Khokhar, et al. proposed a mechanism that to make an alternative arrangement of the routing techniques.
Which specified that existing Multipath routing can be used to support trustworthy communication over untrustworthy low-power wireless links using data at the state during the data transmission process, but didn't proposed that security over the multipath routing
[5] wangBo et. al. discussed the concept of trust for the selection of trustworthy candidate for routing packet to the destination. An idea of trust is used for detection of faulty nodes in the network. The paper discussed the security of the packet being forwarded to the destination.

3. PROTOCOL DESIGN

There are three steps for designing THMR: (1) The information of connection of link is hidden as much as possible in route messages, due to which the malicious nodes cannot deduce network topology; (2) Even with previous condition of hiding topology, THMR can find as many node-disjoint routes as possible such that both, the load balancing and the reliable packet delivery can be achieved (3) THMR can exclude malicious nodes from routes and the routes which are unreliable can be detected before packet transmitting.

Overview:

TOHIP: a topology-hiding multipath routing protocol in mobile ad hoc networks

Most of the existing multipath routing protocols in MANET ignore the topology-exposure problem. TOHIP protocol doesn't allow packet to carry the routing information to avoid the attack from the malicious nodes [7]. Malicious nodes in the network grab the packet carrying routing information perform the attack. TOHIP can establish multiple node-disjoint routes and exclude untrustworthy routes before transmitting packets. TOHIP is a loop-free and does not expose network topology. The protocol is able to resist the different types of attack effectively. TOHIP has capability of finding routes and can increase the packet delivery ratio in the scenarios where there are malicious nodes at the cost of low routing overhead [7].

Fault-tolerant multipath routing scheme (FTMRS) for energy efficient wireless sensor networks

FTMRS is an energy efficient node fault diagnosis and recovery protocol for wireless sensor networks. FTMRS is based on multipath data routing scheme. One main path is used for data routing and other two backup paths are used as alternate path in faulty network to handle the overloaded traffic on main channel. Minimum energy consumption is ensured using shortest path routing [8]. FTMRS routing technique recovers node fault and transmission fault to transmit data in energy efficient manner. FTMRS posses the high fault tolerance as compared to other technique. Data routing time in FTMRS is a very fast and energy conscious even at high percentage of nodes fault [8].

Systematic review for network survivability analysis in MANET

In traditional MANET network survivability was hardly discussed, as there was no critical network system that depends on wireless networks. Authors given the systematic literature review of the state of the art approach in the network survivability in MANET [9].Authors used studies from a number of related article sources. From survey authors found that the existing of analysis method focus on individual node where node is treated as separate event. The analysis reveals the less popular methods in analyzing network survivability are with statistical methods such as regression analysis and survival analysis [9].

Directed diffusion:

DIRECTED DIFFUSION is a query-based multipath routing protocol to provide path failure protection. Routing operation is initialized by the sink node through flooding *interest* messages throughout the network [1]. Interest message contains the information required for the node to perform a task. In this phase the nodes cache the interest message for further use after reception of an *interest*
Message the receiver node creates a gradient towards the node from which this message has been Received [1].

In this stage several paths can be discovered between each pair of source-sink nodes.when a source node detects an event matched with the existing information in its interest table, source forwards its data packets towards the sink node through all the constructed path. The sink node receives requested data through several paths with a low-data rate [2].

After failure of the active path data will be forwarded using the available alternative path, which also provide the fault tolerant routing.

Braided multipath routing protocol: BMRP is routing protocol proposed to provide fault-tolerant routing in wireless sensor networks. BMRP protocol uses a similar approach as Directed diffusion to construct several partially disjoint paths. P*rimary path reinforcement* message is used for path construction by the sink. When an intermediate node receives a *primary path reinforcement* message, it forwards this message to its best next-hop neighboring node towards the source node [2]. Above process is continued till the *primary path reinforcement* message reaches the source node. Along with main path all nodes on the path construct the alternate path around the neighbor nodes. This alternative path uses the neighboring node, which is not present in the primary path [2].

This process terminates upon reception of this message by one of the nodes along the primary path.

Reliable and energy-aware multipath routing: this protocol is designed to mitigate the energy efficiency requirement of WSN. This protocol provides reliable data transmission through Using a backup path from each source to sink. As like above protocol in this protocol path construction is initiated by the sink node [1]. When the sink node receives an *interest* message from a source node and if there is no active path towards the source node, then it initiates a *service-path* discovery process by flooding a *service-path request* message [3].

Upon reception of the *service-path request* message at the corresponding source node, the receiver node transmits a *service-path reservation* message towards the sink node to confirm the discovered path. The *service-path* construction process ends with reception of *service-path reservation* message at the sink node. After path reservation source node can transmit its data packets towards the sink node through the constructed path [3].
Once the service path is constructed sink node initiate the path discovery process to build the backup path. In discovery of backup path the intermediate nodes which are not a member of the discovered *service-path are considered in the backup path [3]*.

Multipath routing protocols for reliable data transmission

Alternative routing techniques is one of the multipath routing mechanism. Existing Multipath routing can be used to support trustworthy communication over untrustworthy low-power wireless links using data at the state during the data transmission process [4].

Reliable information forwarding (reinform) using multiple paths in sensor networks **Rein form** uses the packet duplication technique which is used to provide a long data transmission trustworthy for each application. In this approach depending upon the applications need the reliability is determined using collected data [5]. When source has packet to send, it first determines the required data transmission reliability based on the importance of the collected data after getting reliability source node a Directed diffusions some information as dynamic packet state fields to the data packets and then sends multiple copies of the generated data packets over multipath paths [4].

The Dynamic Packet State fields of the data packets are used to determines the required number of paths to fulfill the trustworthy demands of the collected information. The Dynamic Packet State fields in the received data packets used to determine the number of copies that should be handover to their next-hop neighboring nodes [5].

According to the main operation of this protocol, reinform tries to improve data transmission Reliability through utilizing the packet duplication technique at all the involved sensor nodes in the data transmission process [5].

N-to-1 multipath routing protocol

This protocol is proposed according to converge cast traffic pattern of wireless sensor networks.
This protocol aims at the finding the multiple node-disjoint path from all sensor nodes to the single sink. During data transmission phase the intermediate nodes utilize a property of saving packet technique at each hop for the improvement of data transmission and reliability. The flooding mechanism is used for routing operation in n-to-1 multipath routing [6].

The sink node starts the first stage of the route discovery process through broadcasting a *route update* message. This phase *branch-aware flooding*, uses benefit of a simple flooding technique to construct a spanning tree which discovers several paths from sensor nodes towards a single sink node [6].

Taxonomy of the existing multipath routing protocols:

Figure shows the classification of the multipath routing protocols proposed for WSN. The suggested taxonomy classifies the existing multipath routing protocols into three important categories based on the path selection and traffic distribution mechanisms.

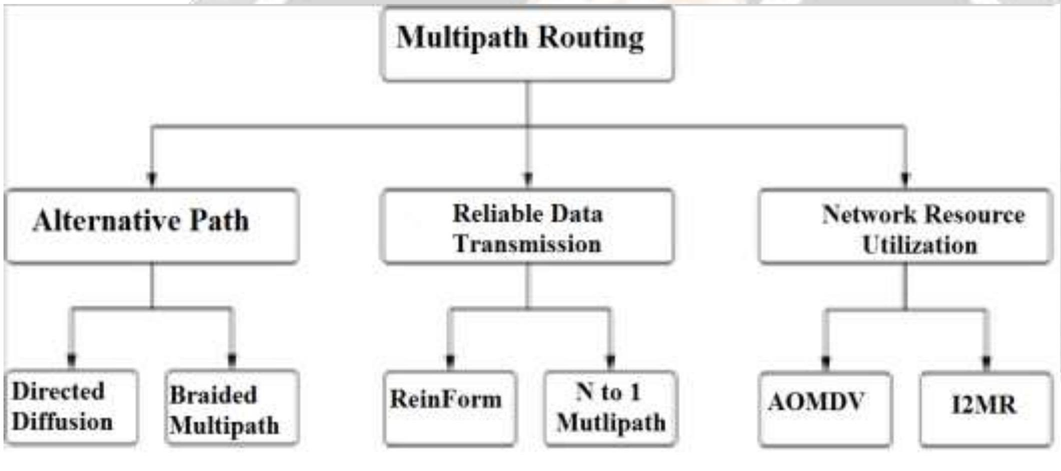


Fig 1. Taxonomy

Benefits of multipath routing

1. **Reliability and fault-tolerance:** the multipath routing in WSN is used to provide path resilience and reliable data transmission. In the fault tolerance domain a sensor node cannot forward its data packets towards the sink. Reliability in packet transmission using alternative path.

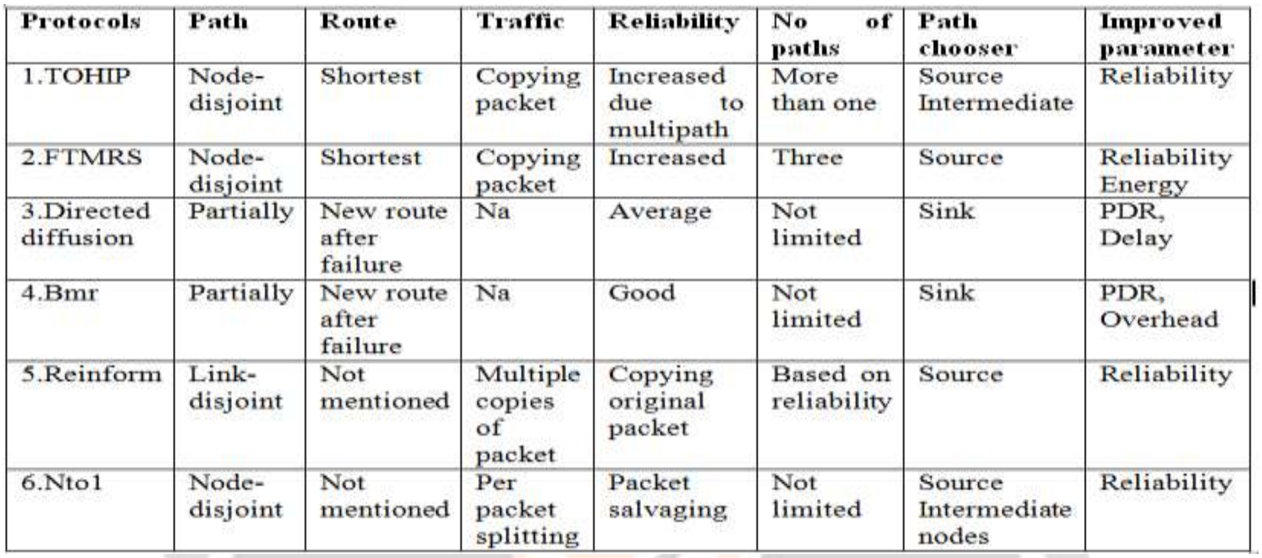
2. **Load balancing:** as traffic distribution is not equal in all links in the network, distributing the traffic along multiple routes can avoid congestion and bottlenecks in links.

3. **Quality Of Service improvement:** Quality Of Service can be achieved using network throughput, end-to-end delay and packet delivery ratio. Quality Of Service is an important objective in designing multipath routing protocols for different types of networks.

4. **Reduced delay:** backup routes are used to minimize delay in multipath routing in wireless network. This is Quality Of Service objective which plays an important role in routing protocol design.

5. **Bandwidth aggregation:** splitting data to the same destination into multiple streams and routed through a different path. This strategy is particularly beneficial when a node has multiple low bandwidth links but it requires a bandwidth that is greater than the one which an individual link can provide.

Comparison:



Protocols	Path	Route	Traffic	Reliability	No of paths	Path chooser	Improved parameter
1.TOHIP	Node-disjoint	Shortest	Copying packet	Increased due to multipath	More than one	Source Intermediate	Reliability
2.FTMRS	Node-disjoint	Shortest	Copying packet	Increased	Three	Source	Reliability Energy
3.Directed diffusion	Partially	New route after failure	Na	Average	Not limited	Sink	PDR, Delay
4.Bmr	Partially	New route after failure	Na	Good	Not limited	Sink	PDR, Overhead
5.Reinform	Link-disjoint	Not mentioned	Multiple copies of packet	Copying original packet	Based on reliability	Source	Reliability
6.Nto1	Node-disjoint	Not mentioned	Per packet splitting	Packet salvaging	Not limited	Source Intermediate nodes	Reliability

Table 1

6. PROBLEM STATEMENT:

After analyzing the paper's, we came to a point that even though if the packet is lost in between the node, then that particular packet broadcast the lost message to all the nodes which are present in the topology, which indicates that it fails to hide the topology structure when the packet is lost. In our project work we are implementing modified version of THMR. THMR gives better performance if there is no attack in the network. In attack scenario it has maintained the constant routing overhead but has reduced performance. In our work we are implementing data transmission strategy with fault detection mechanism. Finally we will compare performance of proposed work with existing system using PDR, PLR, Routing Overhead and delay.

4. CONCLUSIONS

In this paper we have studied the different routing protocols with different routing schemes. Our survey is limited to the multipath routing in wireless sensor network. We have studied the taxonomy of multipath routing protocols. Lastly we have discussed the multipath routing with different parameters.

5. REFERENCES

[1] [1]. Yujun Zhang, Guiling Wang, Qi Hu,"Design and Performance Study of a Topology-Hiding Multipath routing Protocol for Mobile Ad Hoc networks" IEEE 2012.

[2] C. K. Toh, A. N. Le, et al. Load balanced routing protocols for ad hoc mobile wireless networks. *IEEE Communications Magazine*, 47(8):78–84, 2009.

[3] M. K. Marina, and S. R. Das. Ad Hoc On-demand Multipath Distance Vector Routing. *Wiley Wireless Communications and Mobile Computing*, 6(7):969–988, 2006.

[4] L. Abusalah, A. Khokhar, et al. A Survey of Secure Mobile Ad Hoc Routing Protocols. *IEEE Communications Surveys and Tutorials*, 10(4):78–93, 2008.

[5] E. Gerhards-Padilla, N. Aschenbruck, et al. Detecting Black Hole Attacks in Tactical MANETs Using Topology Graphs. *IEEE Conference on Local Computer Networks (LCN)*, pages 1043–1052, 2007.

[6] VVangBo, HuangChuanhe ,YangVVenzhong, VVangTong,"Trust Opportunistic Routing Protocol in Multi-hop Wireless Networks " 2010 IEEE.

[7] F. N. Abdesselam, B. Bensaou, et al. Detecting and avoiding wormhole attacks in wireless ad hoc networks. *IEEE Communications Magazine*, 46(4):127–133, 2008.

[8] W. Galuba, P. Papadimitratos, et al. Castor: Scalable Secure Routing for Ad Hoc Networks. *IEEE conference on computer communications(InfoCom)*, 2010.

[9] Y. C. Hu, A. Perrig, et al. Rushing Attacks and Defense in Wireless Ad Hoc Routing Protocols. *ACM workshop on Wireless Security (WiSe)*, pages 30–40, 2003.

[10] J. R. Douceur. The Sybil Attack. *International Workshop on Peer-to-Peer Systems (IPTPS)*, pages 251–260, 2002.

[11] D. Johnson, Y. Hu, et al. The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4. *IETF RFC 4728*, 2007.

[12] C. Perkins, E. Belding-Royer, et al. Ad hoc On-Demand Distance Vector (AODV) Routing. *IETF RFC 3561*, 2003.

[13] S. Adibi, and G. B. Agnew. Multilayer Flavoured Dynamic Source Routing In Mobile Ad Hoc Netwo rks. *IET Communications*, 2(5), 2008.

[14] F. Kuhn, R. Wattenhofer, et al. Worst-Case Optimal and Average-Case Efficient Geometric Ad Hoc Routing. *ACM International Symposium onMobile Ad Hoc Networking and Computing (MobiHoc)*, pages 267–278,2003.

[15] V. Loscri, and S. Marano. A New Geographic Multipath Protocol for Ad hoc Networks to Reduce the Route Coupling Phenomenon. *IEEE Vehicular Technology Conference (VTC)*, pages 1102–1106, 2006.