ENHANCEMENT OF SECURITY AND PERFORMANCES OF BLOCKCHAIN BY UPDATING HASHING TECHNIQUES

Sangeeta, Dr. Banita
Research scholar, Associate Professor
Department of Computer Science and Engineering,
Baba Mastnath University, Rohtak,
Haryana , India
Email: sangeetaritu0@gmail.com, banita@bmu.ac.in

Abstract:
The Mobile Ad hoc Network (MANET) is a different wireless network architecture that is increasingly being used in commercial, disaster management, law enforcement, and military applications. MANETs are peer-to-peer networks where mobile devices can connect with one another without the use of any external infrastructure by routing messages that are outside of their communication range. Thus, in addition to serving as end devices, nodes also serve as routers. The network's topology is constantly changing as a result of the nodes' mobility and open architecture, which allows them to join or leave the network at any time. In these situations, routing becomes a difficult operation because it must take into account the resource limitations of mobile devices. Despite maintaining a route to every destination and having minimal latency, proactive routing techniques, according to an examination of these protocols, suffer from substantial routing overheads and are unable to keep up with the dynamic topology in a large-scale network. Comparatively speaking, reactive routing technologies offer lower routing costs, better throughput, and higher packet delivery rates. In comparison to proactive routing protocols, reactive routing techniques are appropriate for the majority of applications. Reactive routing protocols with a large user base include the Ad hoc On-demand Distance Vector (AODV) protocol and the Destination Sequence Routing (DSR) protocol. A node is labeled a malicious node and is not allowed to participate in the routing process if its trust value is below the threshold. Although this method uses fewer resources, it is time-consuming, difficult to define the threshold value, and less dependable. The employment of cryptographic methods involving symmetric and asymmetric cryptography is the second strategy for protecting the routing protocol. Although cryptographic techniques offer improved security, they need a lot of processing resources.

Keywords: Routing, Link State Routing, MANET Issues, Path Selection

I. INTRODUCTION

Routing is defined as the method to select the network path. It is used for various types for communication which includes wired communication, E- networks. The packet switching network will send packets to the other packets as per their source to their final address via nodes (intermediate) known as routers. The routing is generally used to send or forward based on routing tables which helps in maintaining a record of the routes among several communication destinations [1]. Hence maintaining is important for making routing effective. Many algorithms access via single path at a given instance of time but in case of multipath routing an algorithm accessed through their respective substitute paths.
Routing is further defined in a precise manner in such a way that all the network addresses are specified in a structured form with respect to their nearby addresses due to which data transfer from

one node to another node within a minimum instance of time.

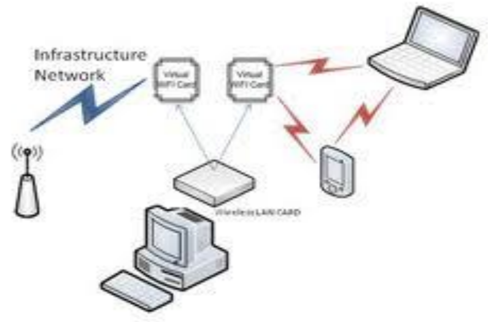

Fig. 1. MANET

Static routing which contains small networks may use physically configured routing tables. Longer networks have complex topologies that can change quickly, making the manual construction of routing tables unrealistic. Nevertheless, most of the public switched telephone network uses pre- computed routing tables, with fallback routes if the most direct route becomes blocked. Adaptive routing, or dynamic routing, attempts to solve this problem by constructing routing tables automatically, based on information carried by routing protocols, and allowing the network to act nearly autonomously in avoiding network failures and blockages[4].Examples of adaptive-routing algorithms are the Routing Information Protocol and the Open-Shortest-Path- First protocol. Adaptive routing dominates the Internet. However, the configuration of the routing protocols often requires a skilled touch; networking technology has not developed to the point of the complete automation of routing.

II. LITERATURE REVIEW ON MANET's

S.No.	Title/ Author	Objective	Methodology used	Result/ Conclusion
1	Scenario-Based Simulation Experiments and Metrics for Certificate-Based Authentication in MANETS P. Manoj Kumar et. al.	To examine the requirements and the characteristics of authentication systems for MANET's	Network Simulator-2	Data provided which may be utilized in NS-2 simulation
2	Configuration and Governance of Dynamic Secure SDN, Mohammed Alabbad et. al.	To identify an architecture which is suitable for dynamic networks	RNS Algorithm	Architecture 3 at data plane
3	A general framework of genetic multi-agent routing protocol for improving the performance of MANET environment, Mustafa Hamid Hassan et. al.	To integrate GA and MAS to improve QoS requirements	Genetic algorithm based multi-agent system	Presented new framework GMARP
4	Mathematical Modeling of Routes Maintenance and Recovery Procedure for MANETs,	To propose a novel formal model for route management	VDM-SL	VDM-SL specify mobility model.

	Zafar Iqbal et. al.			
5	Smart Pedestrian Crossing Management at Traffic Light Junctions through a Fuzzy-Based Approach, Giovanni Pau. Et. al.	To present description of fuzzy logic controller configuration	Fuzzy -Logic Controller	Depth analysis of FLV Configuration
6	Call Admission and Code Allocation Strategies for WCDMA Systems With Multirate Traffic, Felipe A. Cruz-Pérez et. al.	To propose call admission and code allocation	MLCR, OVSF	Code reservation is 6.8% capacity increased
7	MANET (MOBILE AD HOC NETWORK) – CHALLENGES, SECURITY AND PROTOCOLS Vikram m. Agrawal et. al.	To provide comprehensive idea in security field.	MAC Routing	Introduced protocols used for cryptography
8	Routing in Delay/Disruption Tolerant Networks: A Taxonomy, Survey and Challenges Yue Cao and Zhili Sun et. al.	To address multicasting issues in DTNs	Delay/Disruption Tolerant Networks,	Identified the challenges of routing in DTNs
9	Channel Aware Routing in MANETs with Route Handoff, Xiaoqin Chen et. al.	To provide diffrences in performance between CA-AOMDV and AOMDV	Channel adaptive routing	CA-AOMDV outperforms AOMD
10	ANALYZING THE MANET VARIATIONS, CHALLENGES, CAPACITY AND PROTOCOL ISSUES G. S. Mamatha et. al.	To analyse MANET environment	MANETs	MANETs are vulnerable to security threats than fixed networks.
11	Capacity, Bandwidth, and Available Bandwidth yin Wireless Ad Hoc Networks: Definitions and Estimations Marco A. Alzate et. al.	To present Capacity, bandwidth for wireless adhoc networks	Neuro-fuzzy system design	Evaluate performance of estimation methods of accuracy, time.
12	Agent based Bandwidth Reservation Routing Technique in Mobile Ad Hoc Networks, Vishnu Kumar Sharma et. al.	To propose an agent based bandwidth reservation for MANETs	EDCA, TXOP	Resource allocation reduces losses and improves network performance

III. Optimized Link State Routing algorithm

A link-state routing algorithm optimized for mobile ad-hoc networks is the Optimized Link State Routing Protocol [3]. Optimized Link State Routing Protocol is proactive; it uses Hello and Topology Control (TC) messages to discover and disseminate link state information through the mobile ad-hocnetwork. Using Hello messages, each node discovers 2-hop neighbor information and elects a set of multipoint relays. Multipoint relays distinguish Optimized Link State Routing Protocol from other link state routing protocols. An individual nodes use the topology information to compute next hop paths regard to all nodes in the network utilizing shortest hop forwarding paths. The Optimized Link State Routing Protocol is developed for mobile ad hoc networks. It operates as a table driven, proactive protocol, i.e., exchanges topology information with other nodes of the network regularly. Each node selects a set of its neighbor nodes as "multipoint relays". In Optimized Link State Routing, only nodes, selected as such multipoint relays, are responsible for forwarding control traffic, intended for diffusion into the entire network. MPRs provide an efficient mechanism for flooding control traffic by reducing the number of transmissions required. Nodes, selected as multipoint relays, also have a special responsibility when declaring link state information in the network. Indeed, the only requirement for Optimized Link State Routing to provide shortest path routes to all destinations is that multipoint relays nodes declare link-state information for their multipoint relays selectors. Additional available link-state information may be utilized, e.g., for redundancy. Nodes which have been selected as multipoint relays by some neighbor node(s) announce this information periodically in their control messages. Thereby a node announces to the network, that it has reachability to the nodes which have selected it as a multipoint relays. In route calculation, the multipoint relays are used to form the route from a given node to any destination in the network[11]. Furthermore, the protocol uses the multipoint relays to facilitate efficient flooding of control messages in the network. A node selects multipoint relays from among its one hop neighbors with "symmetric", i.e., bi-directional, linkages. Therefore, selecting the route through multipoint relays automatically avoids the problems associated with data packet transfer over unidirectional links (such as the problem of not getting link-layer acknowledgments for data packets at each hop, for link-layers employing this technique for unicast traffic). Optimized Link State Routing is developed to work independently from other protocols. Likewise, Optimized Link State Routing Protocol makes no assumptions about the underlying link- layer. Optimized Link State Routing inherits the concept of forwarding and relaying from HIPERLAN (a MAC layer protocol)which is standardized by ETSI [4].

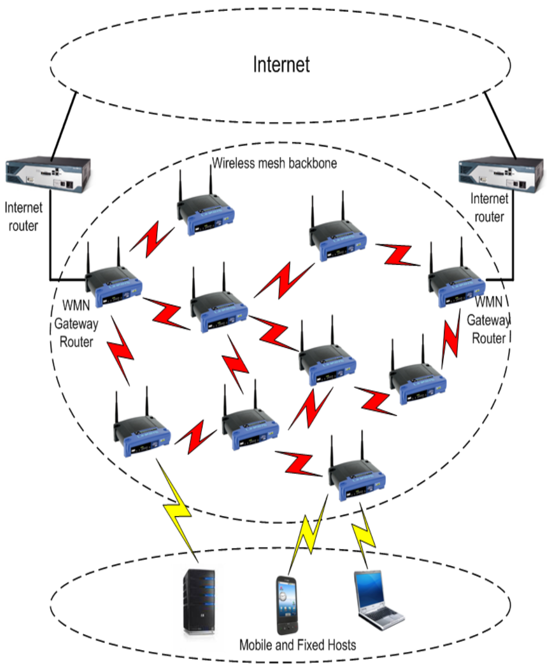

Fig.2: Use of MANET

Optimized Link State Routing is a proactive routing protocol for mobile ad hoc networks. The protocol inherits the stability of a link state algorithm and has the advantage of having routes immediately available when needed due to its proactive nature. Optimized Link State Routing is an optimization over the classical link state protocol, tailored for mobile ad hoc networks. Optimized Link State Routing Protocol minimizes the overhead from flooding of control traffic by using only selected nodes, called multipoint relays, to retransmit control messages. This technique significantly reduces the number of retransmissions required to flood a message to all nodes in the network. Secondly, Optimized Link State Routing requires only partial link state to be flooded in order to provide shortest path routes. The minimal set of link state information required is, that all nodes, selected as multipoint relays, MUST declare the links to their multipoint relay selectors. Additional topological information, if present, MAY be utilized e.g., for redundancy purposes. Optimized Link State Routing MAY optimize the reactivity to topological changes by reducing the maximum time interval for periodic control message transmission [12].Furthermore,as Optimized Link State Routingcontinuously maintains routes to all destinations in the network, the protocol is beneficial for traffic patterns where a large subset of nodes are communicating

with another large subset of nodes, and where the [source, destination] pairs are changing over time. The protocol is particularly suited for large and dense networks, as the optimization done using multipoint relays works well in this context. The larger and more dense a network, the more optimization can be achieved as compared to the classic link state algorithm. Optimized Link State Routing is designed to work in a completely distributed manner and does not depend on any central entity. The protocol does NOT REQUIRE reliable transmission of control messages: each node sends control messages periodically, and can therefore sustain a reasonable loss of some such messages. Such losses occur frequently in radio networks due to collisions or other transmission problems. Also, Optimized Link State Routing does not require sequenced delivery of messages. Each control message contains a sequence number which is incremented foreach message. Thus the recipient of a control message can, if required, easily identify which information is more recent - even if messages have been re-ordered while in transmission.

IV. ROUTING PATH SELECTION

Path selection involves applying a routing metric to multiple routes, in order to select (or predict) the best route. In the case of computer networking, the metric is computed by a routing algorithm, and can cover such informationas bandwidth, network delay, hop count, path cost, load, MTU, reliability, and communication cost. The routing table stores only the best possible routes, while link-state or topological databases may store all other information aswell. Since a routing metric is specific to a given routing protocol, multi- protocol routers must use some external heuristic in order to select between routes learned from different routing protocols. Cisco's routers, for example, attribute a value known as the administrative distance to each route, where smaller administrative distances indicate routes learned from a supposedly more reliable protocol. A local network administrator, in special cases, can set up host-specific routes to a particular machine which provides more control over network usage, permits testing and better overall security. This can come in handy when required to debug network connections or routing tables.

V. MANET Issues

If there are only two nodes that want to communicate with each other and are located very close to each other, then no specific routing protocols or routing decisions are necessary. On the other hand, if there are a number of mobile hosts wishing to communicate, then the routing protocols come into play. In this case, some critical decisions have to be made such as which is the optimalroute from the source to the destination, which is very important because often, the mobile nodes operate on some kind of battery power[20]. Thus it becomes necessary to transfer the data with minimal delay so as to waste less power. There may also be some kind of compression involved which could be provided by the protocol so as to waste less bandwidth. Further, there is also a need of some type of encryption so as to protect the data from prying eyes. In addition to this, Quality of Service support is also needed so that the least packet drop can be obtained.

If there are multiple nodes wishing to communicate with each other and one or more of them are beyond the vicinity of the node who wants to send data to them, then that node can send data to the nearest node who in turn can transfer to the next node and in this way, the data can be transferred.

Delay network (DTN) useful where delay factor is more important, in this dissertation aim to minimize the network delay with the help of congestion detection and prevention method. Delay of any network depends on network capacity, real time number of active connection, buffer size, channel capacity etc. In the dissertation proposed a network congestion detection and prevention (NCDP) in which use the concept of fuzzy logic based system to identify the congestion status and prevent it. In the prevention system use the data rate control mechanism and prevent the real time congestion. We also use the bundle based multicasting which minimize the network overload by destination number padding mechanism in packet. With the help of proposed NCDP system achieve the better throughput, packet delivery ratio, data receives and minimize the routing overhead, delay.

VI. CONCLUSION:

Study explains the characteristics of MANETs, the motivation for the research, the objectives of the research, the major contributions and finally presents the structure of the study.

REFERENCES

1) D. Pei, D. Massey, and L. Zhang, IEEE Global Communications Conference (Globecom) (December, 2003), "Detection of Invalid Routing Announcements in the RIP Protocol".
2) JonneZutt, Arjan J.C. van Gemund, Mathijs M. de Weerdt, and CeesWitteveen(2010). Dealing with Uncertainty in Operational Transport Planning. In R.R. Negenborn and Z.

Lukszo and H. Hellendoorn (Eds.)Intelligent Infrastructures, Ch. 14, pp. 355-382. Springer.

3) Robotics.eecs.berkeley.edu/~wlr/Tutorials/nets_files/Page674.htm.

4) Matthew Caesar and Jennifer Rexford (Nov/Dec 2005),BGP routing policies in ISP networks. IEEE Network Magazine, special issue on Interdomain Routing.

5) R. Kravets and P. Krishnan(October 1998), Power Management Techniques for Mobile Communication, Proc. of MobiCom'98, Dallas,TX.

6) P. J. Wan, G. Calinescu, X.Y. Li and O. Frieder (2001), Minimum energy broadcast routing in static ad-hoc wireless networks, Proc. of IEEE Conference on Computer Communications (INFOCOM), pp. 1162-1171

[7] Tony Larsson and Nicklas Hedman (1998), Routing pro to cols in

Wireless adhoc networks - A simulation study, Master's thesis in computer

science and engineering, pp. 9.

[8] Tony Larsson and Nisklas Hedman. "Routing Protocols in Wireless Ad- hoc Networks: A Simulation Study".

[9] Zeinalipour-Yazti Demetrios; Department of Computer Science,

University of California – Riverside; "A Glance at Quality of Services in

Mobile Ad Hoc Networks".

[10] RatulMahajan, David Wetherall, and Thomas Anderson (2007), Mutually

Controlled Routing with Independent ISPs. Proc. NSDI.

[11]Zeinalipour-YaztiDemetrios; Department of Computer Science,

University of California – Riverside; "A Glance at Quality of Services in

Mobile Ad Hoc Networks".

[12] S. Corson, and J. Macker (October 1998), Mobile Ad hoc Networking

(MANET): Routing Protocol Performance Issues and Evaluation

Considerations, IETF RFC 2501, x.

[13] K. Brown and S. Singh (1997),M-TCP: TCP for Mobile cellular

Networks, Proc. of ACM SIGCOMM Computer Communication Review,

pp. 19–43.

14) Neil Spring, Ratul Mahajan, and Thomas Anderson (2003), Quantifying the Causes of Path Inflation. Proc. SIGCOMM.

Ratul Mahajan, David Wetherall, and Thomas Anderson (2005), Negotiation-Based Routing Between Neigh boring ISPs. Proc. NSDI.

15) J. Broch, D.A. Maltz, D.B. Johnson, Y.C. Hu, and J. Jetcheva (October 1998.), A Performance Comparison of Multi-Hop Wireless Ad-Hoc Network Routing Protocols, Proc. of ACM/IEEE International Conference on Mobile Computing and Networking MOBICOM '98, pp.85-97.

[16] S.K. Sarkar, T.G. Basawaraju and C Pu6tamadappa (2008), Ad-hoc

Mobile Wireless Networks: Principles, Protocols and Applications,

Auerbach Publications, pp. 1.

[17] Steve Wisniewski, —Wireless and Cellular networks, Prentice Hall, 2004.

[18] C.K. Toh, —Ad-Hoc Mobile Wireless Networks: Protocols and Systems,

Prentice Hall PTR, 2002.

[19] Andrea Goldsmith (2005), Wireless Communications, Cambridge

University Press.

[20] Bing Lin and I. Chlamtac (2000), Wireless and Mobile Network

Architectures, Wiley.

[21] C. E. Perkins (Ed.), ―Ad-Hoc Networking, Addison-Wesley Longman,

2001.

[22]Wireless_technologies_advantage_from2008)http://www.kimaldi.com/kimaldi_eng/area_de_conocimiento/tecnologia_wireless/ ventajas_tecnologia_wireless.

22)J. Broch, D.A. Maltz, D.B. Johnson, Y.C. Hu, and J. Jetcheva (October 1998), A Performance Comparison of Multi-Hop Wireless Ad-Hoc

23)Network Routing Protocols, Proc. of ACM/IEEE International Conference on Mobile Computing and Networking M)OBICOM '98, pp.85-97.

24) S. Corson, and J. Macker (January 1999), Mobile Ad-hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations, IETF RFC 2501.

25) V Amato, Ph.D, Series Editor ―Cisco Networking Academy Program: Second – year Companion Guide, Primera Edicion, Cisco Systems Inc., pp. 73-104.