International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163
Volume 1 Issue 8 (September 2014) www.ijirae.com

Tree based routing method to reduce time complexity of routing in MANET

S.THABASU KANNAN
Dept of Comp Science, Anna University,

B.SUGUNA
Dept of Comp Science, Bharathiyar University,

Abstract - In this paper, we introduce a scalable and secure method for many-to-one symbol transmission that offers an optimal message length and is computationally simple. Here nodes can immediately check the correctness of received messages and detect data corruption without requiring any extra error tracing procedure. Previously message corruption was detected by the root of the tree communication model.

Keywords – Ad hoc network, Unlinkability, proactive, Eavesdropping, Tampering, topology

I. INTRODUCTION

In the last two decades great attention has been devoted to the ad hoc networking paradigm, which tries to enhance the feasibility of wireless networking by allowing multi-hop communications in absence of preexistent infrastructure or central administration, currently wireless networking is still limited to single-hop communications achieved via infrastructure-based topologies.
Ad hoc networks inherit all the traditional problems of wireless and mobile communications, such as bandwidth optimization, power control and transmission quality enhancement. In addition, the multihop nature and the lack of fixed infrastructure bring new issues such as network configuration, device discovery, topology maintenance and ad hoc addressing.
Its main aim is to enhance the path reliability and realize load balancing in mobile ad hoc networks.
Ad hoc networks are suited for use in situations where deploying an infrastructure is not cost effective or is not possible for any other reason. When the nodes of an ad hoc network are small mobile devices, such a network is called mobile ad hoc network.

II. INFORMATION SHARING IN MANETS

New-generation mobile devices (cell phones, PDAs, etc.,) are enabled with wireless communications technologies which paves the way to a broad range of services based on mobile ad hoc networks. Here nodes are constantly changing their location. This can cause any pair of nodes to be temporarily unconnected. Communication systems for adhoc networks should not depend on centralized authorities that need to be accessible all the time.

Information transmission between peers is a basic process in MANETs. Such networks rely on the data forwarding service to transmit data between users. It consists of correctly relaying the received packets from node to node until they reach their final destination. Some threads in adhoc networks are Eavesdropping, Tampering, Dropping data packets, Selfish behavior.

MANET applications may require the interaction between some devices may imply the disclosure of some information related to the involved users. Communication protocols for MANETs must be privacy-preserving, which includes anonymity and unlinkability. Anonymity means the requirement that a user should be able to participate in the network without revealing her identity. Unlinkability means that different interactions between a specific user and the network communication system can't be related to each other neither by the system nor by an external observer. If a system is anonymous but the different actions by the same user are linkable, the user's roaming pattern can be obtained from such linkage; this might suffice to infer the user's identity.

III. INFORMATION TRANSMISSION

The many-to-one scenario is obtained by intermediate routers combining received messages into a single message that is routed towards the base station. This process is called aggregation. Here intermediate nodes collect messages from their children, aggregate them and send a single aggregated message up to their parent. In this way, the base station receives a single message containing all the readings from the leaves. This solution is scalable (permitting an unlimited amount of senders) as long as aggregated data do not grow in size. Two scenarios are:

A. **Lossy aggregation**. Here, the message output by aggregation contains less information than the set of messages input to aggregation.

B. **Lossless aggregation** occurs when no information loss is affordable during aggregation. It happens in applications where the root multicasts a data request to the leaves and the leaves react by sending one. At the end of the process, the root knows which symbol was transmitted by each leaf. This implies that the actual informational content transmitted by leaves will be less than the bit-length of the messages they use.

IV. VARIOUS PROTOCOLS

A. Destination-Sequenced Distance Vector (DSDV): It belongs to the category of proactive protocol. Here each node in the network maintains an update route to each other node by exchanging both periodic and event-triggered routing updates (hello packets). The periodic updates occur at specific intervals, while the event-triggered ones are transmitted whenever a change in the topology occurs and, therefore, they introduce time-variable overhead.
It utilizes node sequence numbers for route selection and to pick up the most recent information. If a node learns two different paths to the same destination, it selects the one with the larger sequence number. If both have the same sequence number, the node picks up the one with the shortest hop count. If both the metrics are the same, the choice is arbitrary. DSDV contains two different types of updating: incremental and full. The first includes only the entries changed from the last full update. The second one requires the transmission of the whole routing table, when the number of changed entries exceeds the space available.

B. Ad Hoc on-Demand Distance Vector Routing (AODV): It belongs to the category of reactive protocol. Reactive routing gives up maintaining a route between all pairs of nodes and it discovers the routes when needed, commonly by flooding the network with a route request. AODV route discovery bases on a broadcast network search and a unicast reply containing the discovered path. AODV relies on node sequence numbers for loop avoidance and for selecting the most recent path. To route a packet, a node first checks if a route is available in the routing table. If so, that route can be used, otherwise the node has to start a route discovery procedure.

C. Dynamic Source Routing: Here each packet stores the whole path in the header allowing so a intervals, while the event-triggered ones are transmitted whenever a change in the topology occurs and, therefore, they introduce time-variable overhead. It utilizes node sequence numbers for route selection and to pick up the most recent information. If a node learns two different paths to the same destination, it selects the one with the larger sequence number. If both have the same sequence number, the node picks up the one with the shortest hop count. If both the metrics are the same, the choice is arbitrary. DSDV contains two different types of updating: incremental and full. The first includes only the entries changed from the last full update. The second one requires the transmission of the whole routing table, when the number of changed entries exceeds the space available.

D. Ad Hoc on-Demand Distance Vector Routing (AODV): It belongs to the category of reactive protocol. Reactive routing gives up maintaining a route between all pairs of nodes and it discovers the routes when needed, commonly by flooding the network with a route request. AODV route discovery bases on a broadcast network search and a unicast reply containing the discovered path. AODV relies on node sequence numbers for loop avoidance and for selecting the most recent path. To route a packet, a node first checks if a route is available in the routing table. If so, that route can be used, otherwise the node has to start a route discovery procedure.

E. Dynamic Source Routing: Here each packet stores the whole path in the header allowing so a simpler forwarding process with respect to the hop-by-hop forwarding exploited by AODV. Here each node maintains several routes toward the same destination which can be used in the case of link failures. DSR enables nodes to promiscuously listen to control packets not addressed to themselves. In such a way, nodes can utilize the source routes carried in both DSR control messages and data packets to gratuitously learn routing information for other network destinations.

V. PROPOSED TREE-BASED ROUTING

This routing method contains a distribute hash table and a location-based addressing schema for a scalable routing service. Here each node stores routes toward sets of nodes, and the cardinality of the sets depend on the overlay distance between the source and the destination addresses. It adopts a hierarchical approach, which allows one to reduce the routing state information stored by each node with respect to a flat approach from O(n) to O(log(n)), where n is the number of nodes in the network.

New routing method resorts to a multi-path strategy: the address space structure is augmented by storing multiple routes toward each set of nodes. With regards to the address space overlay, the multi-path approach improves the tolerance of the tree structure against mobility as well as channel impairments while, with reference to the packet forwarding, it improves the performance by means of route diversity.

A. Architecture of the proposed method

New routing method resorts to a network-layer architecture in which each node has a permanent unique id, to identify the node in the network, and a transient network address that reflects the node's topological location inside the network. Nodes acquire network addresses by listening for the routing update packets exchanged by neighbors.
In overlay network model is a tree-based structure offers simple and manageable procedures for address allocation. It contains low fault-tolerance as well as traffic congestion vulnerability since there exists only one path between any pair of nodes.

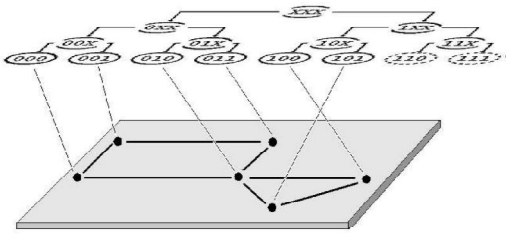

Fig 1: New routing method address space overlay

The address overlay embeds only a partial knowledge about the physical network topology, since only a subset of the available communication links is used for the routing. For such reasons, we propose to augment the tree structure by storing in the routing tables multiple next hops towards the same sibling.

New routing method is an iterative one through the address tree, based on a hierarchical form of multi-path proactive distance-vector routing. New routing method routing tables have n sections, one for each sibling. The k^{th} section stores the available routes (the next hops) towards a node belonging to the level-k sibling. The hierarchical feature of New routing method is based on the concept of sibling and it allows nodes to reduce the routing state information, and the routing update size. It assures that routes toward far nodes remain valid despite local topology changes occurred in the vicinity of these nodes. Since the routing process is based on the network addresses, they have to be efficiently distributed across the network.

B. Processes of new method

In the architecture, the address allocation process allows nodes to acquire a valid network address, while the route discovery process is responsible of both routing-table building and updating. The services provided by these processes are exploited by the packet forwarding process, which is in charge of both choosing the best route and forwarding the packets through. The address discovery process supplies the mapping between identifiers and network addresses, by resorting to the packet forwarding services. Finally, the link quality estimation process assesses the quality of the available links, supporting so the other processes.

[1] Address Allocation Process: New routing method exploits a stateful approach based on multiple disjoint allocation tables. When a new node joins the network, it listens for the hello packets exchanged by neighbors to acquire a valid and available address. It guarantees that nodes, which share the same address form a connected sub-graph in the network topology is known as the prefix constraint one. The detection of duplicate addresses resorts to the subtree identifier concept: we define as subtree id the lowest node id of all the nodes whose network addresses belong to that subtree. The subtree ids allow New routing method to detect the presence of the same address in two disconnected parts of the network.

[2] Link Quality Estimation Process: It allows the packet forwarding process to choose the routes assuring the highest throughput and enables the address allocation process to converge to a steady state. To estimate the link quality, New routing method resorts to the hello packets and to a moving average filtering. Each node locally broadcasts the hellos with an average period T. As mentioned before, the link quality is also used in the routing process to compute the path cost by means of the expected transmission count (ETX). This metric estimate the expected number of packet transmissions required to successfully deliver a packet to the ultimate destination.

[3] Path Discovery Process: It maintains a consistent routing state through the network by updating the routing tables with the information broadcasted by nodes with the hellos. A routing table is made up by L sections, where L is the network address length and the k^{th} section contains several routes. Each entry contains four fields: the network address of the next hop, the sibling id, the path cost and the route log. Differently, a routing update contains no more than L entries i.e one entry for each sibling, and each entry contains the sibling id, the path cost and the route log. If a node stores multiple routes toward the same sibling, it will only record in the routing update the information concerning the best route, according to the path cost. Every process requires a loop detection mechanism to avoid that the information stored in a route update visits the same node more times.

[4] Packet Forwarding Process: Here the route is singled out by taking into account the hierarchical feature of New routing method, by choosing, as next hop, the neighbor which shares the longest address prefix with the destination. If there are multiple neighbors sharing the longest address prefix, the node will select the one with the lowest route cost.

[5] Address Discovery Process: This supplies the mapping between node identifiers and network addresses resorting to a distributed hash table (DHT). It exploits the hierarchical nature of New routing method to address the challenges related to the design of both the two services provided by a DHT system, namely, association of information to peers and query forwarding to responsible peers. Since network addresses are assigned to nodes according to the network topology, there is no assurance that the peer location computed with the hash function is valid, i.e. it has been assigned to a node. To overcome such a drawback, we propose a distributed mechanism (indirect referencing), characterized by low communication overhead and absence of node coordination. Here the peer validation resorts only on the topological information stored in the routing table, without the need of explicit node coordination;

VI. PERFORMANCE EVALUATION

In this section, we present a numerical performance analysis of the proposed protocol by resorting to NS-2. At this end, for the sake of performance comparison, we consider three commonly adopted routing protocols, namely AODV, DSR and DSDV. We ran a large set of experiments to explore the impact of several workloads and environmental parameters on the protocol performances by adopting the following three metrics: Packet delivery ratio (PDR) means the ratio between the number of data packets successfully received, hop count means the number of hops a data packet took to reach its destination and routing overhead means the ratio between the number of generated data packets and the total number of generated routing packets; Each experiment ran ten times, and for each metric we estimated both its average value and the standard deviation.

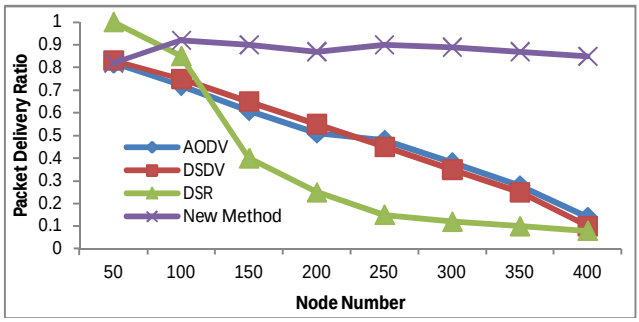

Fig 2: Packet delivery ratio vs node no

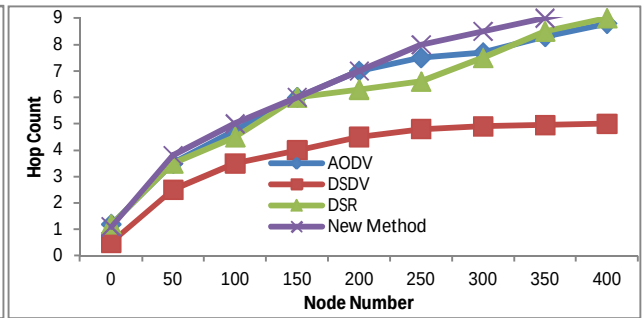

Fig 3: Hop count vs node no

In figure 2, New routing method remains largely unaffected as the number of nodes increases. On the other hand, DSDV and AODV performances decrease rough linearly with the number of nodes. Finally, DSR outperforms all the remaining protocols only for small networks whereas, as the number of nodes increases, its performances become the worst and, with reference to largest networks, nearly an order of magnitude separates them from those of new routing method.
In figure 3, new routing method has been designed to prefer reliable paths, despite of the hop number. Moreover, its hierarchical nature is a potential source of path length inefficiency. However, its performances are comparable with those of AODV and DSR, which experience a path stretch, defined as the ratio between the discovered path length and the shortest path length, of roughly two. DSDV is able to discovery routes very close to the shortest ones. Moreover, if we account for both the delivery ratio and the hop count performances, DSDV performs better than AODV since, by delivering the same number of packets on shorter routes, it uses more efficiently the network resources. The above figure shown that the aggregate data throughput delivered on TCP flows by both new routing method and AODV is unaffected by the number of nodes, whereas both DSDV and DSR performances decreases as the number of nodes grows. Moreover, TCP favors shorter connections, that is, it exhibits flow elasticity, as confirmed by the results in terms of hop number (all the protocols deliver packet on routes shorter than 3 hops in a network with 384 nodes).

The results show the presence of a saturation effect for both the scenarios, which assures that the overhead is bounded in terms of memory space. Such a behavior is due to the choice of adopting a threshold based on the link quality in order to accept the routing updates from neighbors.

The figure 4 shows that DSR outperforms all the other protocols in terms of routing overhead due to its aggressive route caching policy. Again, DSDV and AODV perform similarly in small networks but, when the number of nodes grows, AODV performs worst due to its reactive nature. In small networks, new routing method exhibits the highest overhead, since its routing update packets have fixed size, regardless of the node number. However, when the number of nodes grows, its behavior becomes comparable with those of the other proactive protocol, i.e. the DSDV.

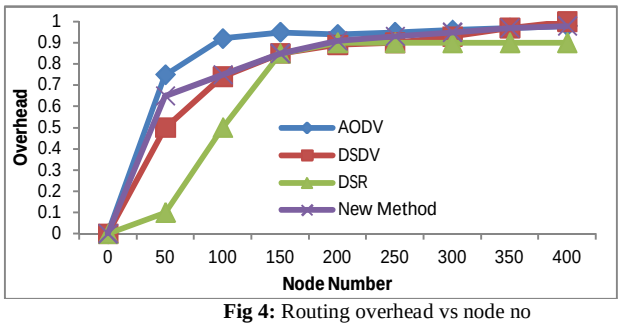

Fig 4: Routing overhead vs node no

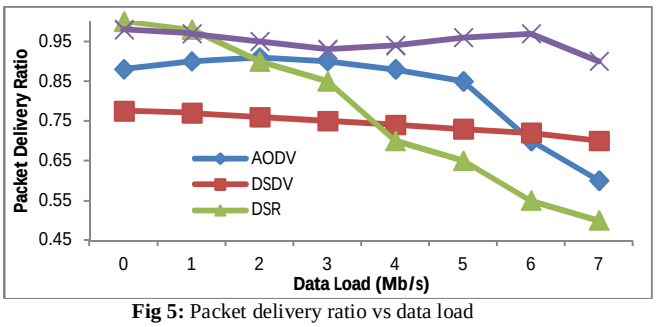

Fig 5: Packet delivery ratio vs data load

The figure 5 shows that the proactive protocols are able to scale well in terms of data load, whereas both DSR and AODV performances are affected by this parameter. Among all the protocols, new routing method outperforms for nearly each data load. Moreover numerical results, not here reported, show that new routing method outperforms all the other protocols in terms of delivery ratios for rough every data load when the number of nodes exceeds 64.

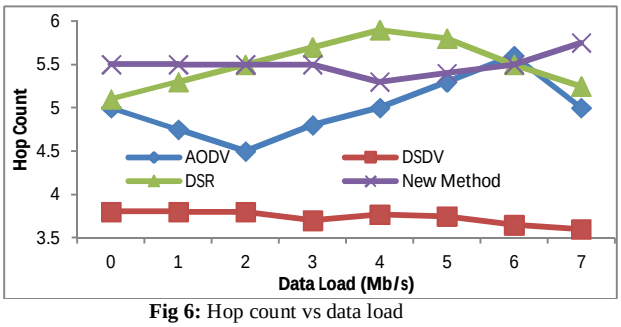

Fig 6: Hop count vs data load

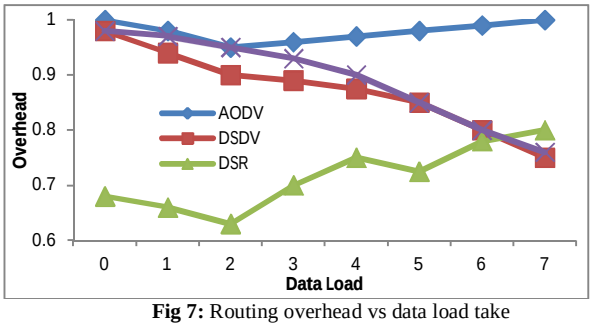

Fig 7: Routing overhead vs data load take

In the figure 6, the path lengths of proactive protocols are unaffected by the data load. DSDV routes have length closer to shortest ones. In the figure 7 the proactive routing traffic does not depend on the data load, since the routing overhead decreases linearly with the data load, whereas the reactive routing traffic increases linearly with the data load.

VII. CONCLUSION

In this paper, the adoption of a new hierarchical routing method to achieve a scalable network layer for ad hoc networks has been proposed. The main concept of hierarchical routing is to keep, at any node, complete routing information about nodes which are close to it and partial information about nodes located further away.

It has been shown that the overhead needed by current networking protocols for ad hoc networks increases so fast with the number of nodes that it eventually consumes all of the available bandwidth also in networks with moderate size. One of the main reasons for such a lack of scalability is that they have been proposed for wired networks and modified to cope with ad hoc scenarios. More specifically, they are based on the assumption that node identity equals routing address that is, they exploit static addressing which of course is not yet valid in ad hoc scenarios. Recently, some routing protocols have exploited the idea of decoupling identification from location, by resorting to distribute hash table services, which are used to distribute the node's location information throughout the network. In this paper, we give a contribution toward such an approach by focusing our attention on the problem of implementing a scalable network layer.

The new method is used to allow nodes to exploit hierarchical routing, limiting so the overhead introduced in the network and used to map the transient identifiers and node identities. Performance comparisons with three existing methods substantiate the effectiveness of the new proposed method for large ad-hoc networks operating in presence of channel hostility and moderate mobility. Since this new method adopts a multi-path strategy and the performances of these strategies are commonly evaluated by numerical simulations, an analytical framework to evaluate the performance gain achieved by multi-path routing has been proposed. By resorting to numerical simulations based on a widely adopted routing performance metric, packet delivery ratio, hop count and overhead, the proposed framework has been validated and the results show the effectiveness of new method.

BIBLIOGRAPHY

[1] A. Boldyreva, "Efficient threshold signatures, multisignatures and blind signatures based on the Gap-Diffie-Hellman-group signature scheme", *Lecture Notes in Computer Science*, vol. 2567, pp. 31–46, 2008.
[2] Leonard Kleinrock and Farouk Kamoun. Hierarchical routing for large networks; performance evaluation and optimization. *Computer Networks*, 1:155–174, 2009.
[3] X. Hong, K. Xu, and M. Gerla. Scalable routing protocols for mobile ad hoc networks. *IEEE Network*, 16(4):11–21, July 2007.
[4] Elizabeth Belding-Royer. Routing approaches in mobile ad hoc networks. In *Ad Hoc Networking*, pages 275–300. IEEE PressWiley, 2008.
[5] J. Broch, D.A.Maltz, D.B. Johnson, Y. Hu, and J.A. Jetcheva. A performance comparison of multi-hop wireless ad hoc network routing protocols. In *MobiCom '09: Proceedings of the 10th annual ACM/IEEE international conference on Mobile computing and networking*, pps 85–97, 2009.
[6] S. R. Das, R. Castaneda, and J. Yan. Comparative performance evaluation of routing protocols for mobile, ad hoc. In *IC3N '09: Proceedings of the International Conference on Computer Communications and Networks*, page 153, 2009.
[7] Elizabeth M. Royer and Chai-Keong Toh. A review of current routing protocols for ad hoc mobile wireless networks. *IEEE Personal Communications*, 6:46–55, 2009.
[8] Charles Perkins and Pravin Bhagwat. Highly dynamic destination sequenced distance-vector routing for mobile computers. In *SIGCOMM '09: ACM Conference on Communications Architectures, Protocols and Applications*, pages 234–244, 2009.
[9] S.R. Das, E.M. Royer. Performance comparison of two on-demand routing protocols for ad hoc networks. In *INFOCOM 2009. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, volume 1, pages 3–12, 2009.
[10] Sabyasachi Roy, Dimitrios Koutsonikolas, Saumitra Das, and Y. Charlie Hu. High-throughput multicast routing metrics in wireless mesh networks. *Ad Hoc Network*, 6(6):878–899, 2009.
[11] P.P. Pham and S. Perreau. Performance analysis of reactive shortest path and multipath routing mechanism with load balance. *INFOCOM 2003: Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies*, 1:251–259, 2008.
[12] Tracy Camp, Jeff Boleng, and Vanessa Davies. A survey of mobility models for ad hoc network research. *Wireless Communications and Mobile Computing*, 2(5):483–502, 2009.
[13] H. Pucha, S. M. Das, and Y. Hu. Imposed route reuse in ad hoc network routing protocols using structured peer-to-peer overlay routing. *IEEE Transactions on Parallel and Distributed Systems*, 17(12):1452–1467, 2009.

