SPSR: A Lightweight Secure Proactive Source Routing Protocol for Mobile Ad-Hoc Networks

Lavanya.R[1] Dr.M.A.Goutham[2]
[1]M. Tech Student [2]Professor
[1,2]Department of Electronics and Communication
[1,2]AIT, Chikkamagaluru

Abstract— Opportunistic forwarding, by which data is randomly relayed to a neighbor based on local network information, is a fault tolerant distributed algorithm particularly useful for challenged ad-hoc and sensor networks. Opportunistic data forwarding has drawn much attention in the research community of multi-hop wireless networking and more researches are conducted for stationary wireless networks. The reason why opportunistic data forwarding is not utilized in Mobile ad-hoc networks is lack of an efficient lightweight secure proactive source routing (SPSR) scheme with strong source routing capability. A lightweight secure proactive source routing (SPSR) protocol is proposed where SPSR protocol has much smaller overhead, less end to end delay and energy consumption and increase in throughput and packet delivery ratio (PDR). The SPSR protocol is compared with the traditional OLSR protocol for the performance analysis. The tests using computer simulation are conducted in Network simulator version-2 (NS-2) and the appropriate graph is shown.

Key words: SPSR, Mobile Ad-Hoc Networks, PDR

I. INTRODUCTION

Mobile Ad Hoc Network (MANET) is a collection of two or more devices or nodes or terminals with wireless communications and networking capability that communicate with each other without the aid of any centralized administrator also the wireless nodes that can dynamically form a network to exchange information without using any existing fixed network infrastructure. Ad-Hoc is Latin and it means “for this purpose”. Mobile ad hoc networks are infrastructure-less networks since they do not require any fixed infrastructure, such as a base station, for their operation. It is a wireless communication network, where nodes that are not within the direct transmission range of each other require other nodes to forward data. In general, routes between nodes in an ad hoc network may include multiple hops, and hence it is appropriate to call such networks as multi-hop wireless ad hoc networks. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. Some MANETs are restricted to a local area of wireless devices (such as a group of laptop computers), while others may be connected to the Internet. Because of the dynamic nature of MANETs, they are typically not very secure, so it is important to be cautious what data is sent over a MANET. The growths of laptops and 802.11/Wi-Fi wireless networking have made MANETs a popular research topic since the mid 1990s.

A routing protocol is needed whenever a packet needs to be transmitted to a destination via number of nodes. Numerous protocols have been established for the purpose of transmission of data from source to destination. These protocols find a route for packet delivery and deliver the packet to the correct destination. The routing protocols can be divided into three main categories. They are

- Reactive routing protocol (On-demand)
- Proactive routing protocol (Table-driven)
- Hybrid routing protocol

A. *Reactive Routing Protocol*

Reactive routing is a popular routing category for wireless ad hoc routing. It is a relatively new routing philosophy that provides a scalable solution to relatively large network topologies. The design follows the idea that each node tries to reduce routing overhead by only sending routing packets when communication is requested. In these protocols, routes are created as and when required. When a transmission occurs from source to destination, it invokes the route discovery procedure. The route remains valid till destination is achieved or until the route is no longer needed. Some reactive routing protocols include: Dynamic source routing (DSR), Ad-hoc on-demand distance vector (AODV) etc.

B. *Proactive Routing Protocol*

Proactive routing protocols are table-driven and will actively determine the layout of the network. Through a regular exchange of network topology packets between the nodes of the network, a complete picture of the network is maintained at every single node. There is hence minimal delay in determining the route to be taken. In proactive routing protocols each node maintains one or more tables containing routing information to every other node in the network. All nodes keep on updating these tables to maintain latest view of the network. It maintains valid routes to all destinations at all time. Some Proactive routing protocols include: Destination sequenced distance vector (DSDV), Optimized link state routing (OLSR) etc.

C. *Hybrid Routing Protocol*

Hybrid routing protocol in MANETs contains the nature of both proactive and reactive routing protocols. The entire network is divided into overlapping zone of variable sizes. It uses proactive protocols for finding zone neighbors (instantly sending hello messages) as well as reactive protocols for routing purposes between different zones (a route is only established if needed). The hybrid routing protocol includes Zone routing protocol (ZRP).

Security has become a primary concern in order to provide protected communication between mobile nodes in a hostile environment. Unlike the wire line networks, the unique characteristics of mobile ad hoc networks pose a number of nontrivial challenges to security design, such as open peer-to-peer network architecture, shared wireless medium, stringent resource constraints, and highly dynamic network topology. These challenges clearly make a case for building multifence security solutions that achieve both broad protection and desirable network performance. Security attacks in MANET routing can be divided in two main types, passive attacks and active attacks. The intention of a passive attack is typically to listen and retrieve vital information inside data packets, for example by launching a traffic monitoring attack. In such an attack, a malicious node tries to identify communication parties and functionality which can provide information to launch further attacks. The attack type is called passive since the normal functionality of the network is not altered. An active attack is performed by a malicious node with the intention to interrupt the routing functionality of a MANET. This includes modification attacks, impersonation attacks, fabrication attacks, wormhole attacks and selfish behavior. The layers which plays important role in the MANETs are Application layer, Transport layer, Network layer, Data link layer and Physical layer. The above layers can be explained as follows.

1) Application layer: The application layer is used in the design of Graphics User Interface (GUI) and it takes input from the user.
2) Transport layer: The transport layer consists of agents for transporting data packets. The agents are classified as Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). TCP is used for wired connections and UDP is used for wireless connections.
3) Network layer: The network layer is useful in finding the routes towards the destination.
4) Data link layer: The data link layer provides the link between the nodes.
5) Physical layer: In the physical layer, the file is converted to 0's and 1's. Through Local Area Network (LAN) cable, the information is extracted through bits.

II. Related Work

Mobile users can use their cellular phone to check e-mail, browse internet, travelers with portable computers can surf the internet from airports, railway stations, starbucks and other public locations, tourists can use GPS terminals installed inside rental cars to locate driving maps and tourist attractions, researchers can exchange files and other information by connecting portable computers via wireless LANs while attending conferences; at home, users can synchronize data and transfer files between them. Not only are mobile devices getting smaller, cheaper, more convenient, and more powerful, they also run more applications and network services [1]. Among all the applications and services run by mobile devices, network connections and corresponding data services are without doubt the most demanded service by the mobile users. This demonstrates the importance behind the mobile ad-hoc networks and presents a representative collection of technology solutions used at the different layers of networks in particular presenting the algorithms and protocols unique to operation and dynamic configuration of MANETs. Therefore, the main research areas in the MANET literature are presented.

Vehicular ad-hoc networks (VANETs) are highly mobile wireless networks that are designed to support vehicular safety, traffic monitoring, and other commercial applications. Within VANETs, vehicle mobility will cause the communication links between the vehicles to frequently be broken. Such link failures require a direct response from the routing protocols, leading to potentially excessive increase in the routing overhead and degradation in the network scalability [2]. A new hybrid location based routing protocol is designed to address this issue. The new protocol combines the features of reactive routing with location based geographic routing in a manner that efficiently uses all the location information available. The analysis and simulation shows that the protocol is scalable and has an optimal overhead, even in the presence of high location errors. The protocol provides an enhanced yet pragmatic location-enabled solution that can be deployed in all VANET-type environments.

ExOR is an integrated routing and MAC protocol that increases the throughput of large unicast transfers in multi-hop wireless networks. ExOR chooses each hop of a packet's route after the transmission for that hop, so that the choice can reflect which nodes actually received the transmission. This deferred choice gives each transmission multiple opportunities to make progress. As a result ExOR can use long radio links with high loss rates, which would be avoided by traditional routing. ExOR increases a connection's throughput while using no more network capacity than traditional routing. ExOR's design faces the following challenges [5]. The nodes that receive each packet must agree on their identities and choose one forwarder. The agreement protocol must have low overhead, but must also be robust enough that it rarely forwards a packet zero times or more than once. Finally, ExOR must choose the forwarder with the lowest remaining cost to the ultimate destination. Measurements of an implementation on a 38-node 802.11b test-bed show that ExOR increases throughput for most node pairs when compared with traditional routing. For pairs between which traditional routing uses one or two hops, ExOR's robust acknowledgments prevent unnecessary retransmissions, increasing throughput by nearly 35%. For more distant pairs, ExOR takes advantage of the choice of forwarders to provide throughput gains of a factor of two to four.

III. Design of SPSR Protocol

The designing of SPSR protocol includes the following

- Breadth-first spanning tree (BFST)
- Route Update (RU)
- Neighborhood trimming (NT)
- Streamlined differential update (SDU)

A. Breadth-First Spanning Tree (BFST)

SPSR provides every node with a breadth-first spanning tree (BFST) of the entire network rooted at itself. To do that, nodes periodically broadcast the tree structure to their best knowledge in each iteration.

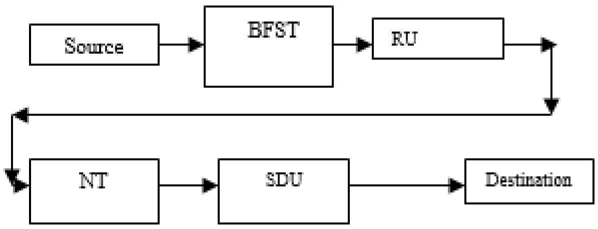


Fig. 1: Block diagram of the system

Based on the information collected from neighbors during the most recent iteration, a node can expand and refresh its knowledge about the network topology by constructing a deeper and more recent BFST. On the other hand, when a neighbor is deemed lost, a procedure is triggered to remove its relevant information from the topology repository maintained by the detecting node. The nodes taken from 0 to 35 are deployed in a network. Each and every node broadcast the packet in the form of tree structure. The relevant information is collected from all the neighboring nodes. Based on this information collected from the neighbors, a node can expand and refresh its knowledge about the network topology. When a neighboring node is lost, a procedure is triggered to remove its relevant information from the network topology.

B. Route Update

The update operation of SPSR is iterative and distributed among all nodes in the network. At the beginning, node v is only aware of the existence of itself; therefore, there is only a single node in its BFST, which is root node v. By exchanging the BFSTs with the neighbors, it is able to construct a BFST within N [v], i.e., the star graph centered at v, which is denoted Sv .In each subsequent iteration, nodes exchange their spanning trees with their neighbors. From the perspective of node v, toward the end of each operation interval, it has received a set of routing messages from its neighbors packaging the BFSTs [3]. A node (route node) checks for the neighboring node details and stores the neighbor information. By exchanging the BFSTs with the neighbors, it is able to construct a BFST. In each subsequent iteration, nodes exchange their spanning trees with their neighbors. At the end of each operation interval, it has received a set of routing messages from its neighbors packaging the BFSTs. The route node requests the other neighboring nodes for all the possible routes between the node 0 to node 35. The information about the source node, destination node and the cost (time taken from source node to destination node) are calculated. This information is updated on the routing table.

C. Encryption

RSA algorithm is used in this context. The RSA algorithm consists of

– Generation of keys
– Encryption
– Decryption

Here the generation of keys and encryption are considered. This algorithm is based on the difficulty of factorizing large numbers that have 2 and only 2 factors (Prime numbers). The system works on a public and private key system. The public key is made available to everyone. With this key a user can encrypt data but cannot decrypt it, the only person who can decrypt it is the one who possesses the private key. It is theoretically possible but extremely difficult to generate the private key from the public key; this makes the RSA algorithm a very popular choice in data encryption. The message is sent along with public key in this context.

D. Neighborhood Trimming

The periodically broadcast routing messages in SPSR also double as “hello” messages for a node to identify which other nodes are its neighbors. When a neighbor is deemed lost, its contribution to the network connectivity should be removed; this process is called neighbor trimming. Consider node v. The neighbor trimming procedure is triggered at v about neighbor u either by the following cases: No routing update or data packet has been received from this neighbor for a given period of time [4]. A data transmission to node u has failed, as reported by the link layer. The periodically broadcast routing messages in SPSR also double as “hello” messages for a node to identify which other nodes are its neighbors. When a neighbor is deemed lost, its contribution to the network connectivity should be removed; this process is called neighborhood trimming. After detecting the shortest path from source to destination using BFST, the remaining nodes are ignored for the further transmission of data. Only the minimum distance is considered.

E. Streamlined Differential Update

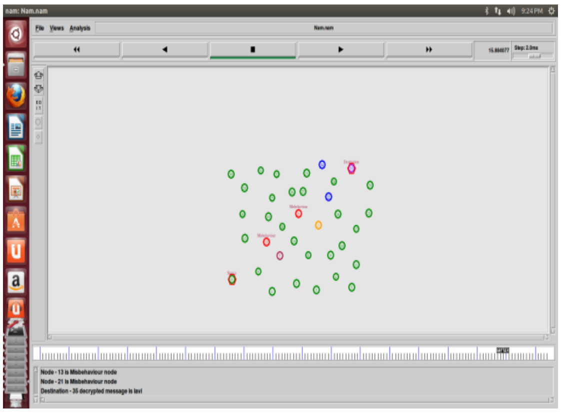
In addition to dubbing route updates as hello messages in PSR, we interleave the “full dump” routing messages, as stated previously, with “differential updates.” The basic idea is to send the full update messages less frequently than shorter messages containing the difference between the current and previous knowledge of a node’s routing module. Both the benefit of this approach and balancing between these two types of messages have been extensively studied in earlier proactive routing protocols. we further streamline the routing update in two new avenues. First, we use a compact tree representation in full-dump and differential update messages to halve the size of these messages. Second, every node attempts to maintain an updated BFST as the network changes so that the differential update messages are even shorter. The information is streamed from source to destination. The basic idea is to send the full update messages less frequently than the shorter messages containing the difference between the current and previous knowledge of a node’s routing module. Both the benefit of this approach and balancing between these two types of messages have been extensively shown in earlier proactive routing protocols.

F. Decryption

The decryption is performed using RSA algorithm. The decrypted message is obtained after streamlined differential update using private key.

IV. Results and Analysis

The results and analysis consists of the results obtained in the execution of BFST, route update, neighborhood trimming and streamlined differential update.



Node - 13 is Misbehaviour node
Node - 21 is Misbehaviour node
Destination - 35 decrypted message is lavi

Fig. 2: Working of SPSR protocol

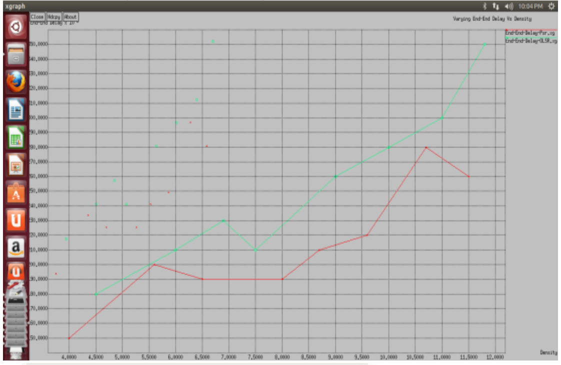


Fig. 3: Graph indicating end to end delay

V. Conclusion

The designing of the SPSR protocol consists of BFST, route update, encryption, neighborhood trimming, streamlined differential update and decryption. The coding for all the steps have been done and executed. The results obtained are shown in the snapshots. The performance evaluation is done and the SPSR protocol is compared with the OLSR protocol and end to end delay is compared. The obtained graph is shown in the snapshot. Thus, from the comparison it can be concluded that SPSR protocol has better data transportation capability and can maintain much topology information compared to OLSR protocol.

References

[1] I. Chlamtac, M. Conti, and J.-N. Liu, “Mobile ad hoc networking: Imperatives and challenges,” Ad Hoc Netw., vol. 1, no. 1, pp. 13–64, Jul. 2003.

[2] M. Al-Rabayah and R. Malaney, “A new scalable hybrid routing protocol for VANETs,” IEEE Trans. Veh. Technol., vol. 61, no. 6, pp. 2625–2635, Jul. 2012.

[3] R. Rajaraman, “Topology control and routing in ad hoc networks: A survey,” ACM SIGACT News, vol. 33, no. 2, pp. 60–73, Jun. 2002.

[4] Y. P. Chen, J. Zhang, and I. Marsic, “Link-layer-and-above diversity in multi-hop wireless networks,” IEEE Commun. Mag., vol. 47, no. 2, pp. 118–124, Feb. 2009.

[5] S. Biswas and R. Morris, “ExOR: Opportunistic multi-hop routing for wireless networks,” in Proc. ACM Conf. SIGCOMM, Philadelphia, PA, USA, Aug. 2005, pp. 133–144.