International Journal of Research Studies in Computer Science and Engineering (IJRSCSE)
Volume 1, Issue 3, July 2014, PP 39-43
ISSN 2349-4840 (Print) & ISSN 2349-4859 (Online)
www.arcjournals.org

Secure Source Routing for Wireless Nodes

Jaya Varughese
M.Tech Scholar
Musaliar College of Engineering and Technology
Kerala, India

Shamna S
Associate Professor
Musaliar College of Engineering and Technology
Kerala, India

Abstract: *Opportunistic data forwarding has drawn much attention in the research community of multihop wireless networking, with most research conducted for stationary wireless networks. One of the reasons why opportunistic data forwarding has not been widely utilized in mobile ad hoc networks (MANETs) is the lack of an efficient lightweight secure routing scheme with strong source routing capability. In this paper, a lightweight secure source routing (SSR) protocol is proposed which is used to bypass insecure nodes and make sure transmission takes place only through secure nodes to the destination. SSR can maintain more network topology information than distance vector (DV) routing to facilitate source routing, although it has much smaller overhead than traditional DV-based protocols [e.g., destination-sequenced DV (DSDV)], link state (LS)-based routing [e.g., optimized link state routing (OLSR)], and reactive source routing [e.g., dynamic source routing (DSR)]. Computer simulation in Network Simulator 2 (ns-2) ensure security of transmission with less overhead in PSR protocols.*

Keywords: *Distance Vector, AODV, Source routing, MANET*

1. INTRODUCTION

In computer networking, **source routing** allows a sender of a packet to partially or completely specify the route the packet takes through the network. In contrast, in non-source routing protocols, routers in the network determine the path based on the packet's destination.

Source routing allows easier troubleshooting, improved trace route, and enables a node to discover all the possible routes to a host. It does not allow a source to directly manage network performance by forcing packets to travel over one path to prevent congestion on another.

In the Internet Protocol, two header options are available which are rarely used: "strict source and record route" (SSRR) and "loose source and record route" (LSRR). Because of security concerns, packets marked LSRR are frequently blocked on the Internet. If not blocked, LSRR can allow an attacker to spoof its address but still successfully receive response packets. Policy-based routing can also be used to route packets using their source addresses.

Software Defined Networking can also be enhanced when source routing is used in the forwarding plane. Studies have shown significant improvements in convergence times as a result of the reduced state that must be distributed by the controller into the network

Routing determines what path a data packet should follow from the source node to the destination. Data forwarding regulates how packets are taken from one link and put on another. Opportunistic data forwarding refers to a way in which data packets are handled in a multi hop wireless network. Unlike traditional IP forwarding, where an intermediate node looks up a forwarding table for a dedicated next hop, opportunistic data forwarding allows potentially multiple downstream nodes to act on the broadcast data packet. One of the initial works on opportunistic data forwarding is selective diversity forwarding by Larsson. In this paper, a transmitter picks the best forwarder from multiple receivers, which successfully received its data, and explicitly requests the selected node to forward the data.

- Here a lightweight proactive source routing protocol is used so that each node has complete knowledge of how to route data to all other nodes in the network at any time. When a flow of

data packets are forwarded towards their destination, the route information carried by them can be adjusted by intermediate forwarders. Furthermore, as these packets are forwarded along the new route, such updated information is propagated upstream rapidly without any additional overhead. As a result, all upstream nodes learn about the new route at a rate much faster than via periodic route exchanges.

- Opportunistic data forwarding is taken to another level by allowing nodes that are not listed as intermediate forwarders to retransmit data if they believe certain packets are missing.

In this paper, we propose a lightweight *secure source routing* (SSR) *protocol* to facilitate opportunistic data forwarding in a secure manner in MANETs. A linked list maintained in each source, intermediary and destination nodes regarding the list of nodes to which data is to be transmitted. Each time a packet is received a sequential search is performed through the list and the suitable next hop is detected. Each node is aware of the location of all nodes in the list . Dynamic source routing protocols are quite inefficient in such cases as the route is determined dynamically on demand. This causes considerable delay in transmission.

In the simulation analysis phase a round trip time is calculated and the results are depicted as graphs.

2. PROPOSED SYSTEM- SECURE SOURCE ROUTING WITH SSR

2.1. Design of Secure Source Routing for static nodes

The diagram presents a working scenario with secure transmission from source to destination nodes by making use of PSR in case of static wireless nodes. Here about nine intermediary nodes are present where only three nodes marked SN are secure nodes. The remaining nodes in black circles are insecure nodes. S,D represents the source and destination respectively.

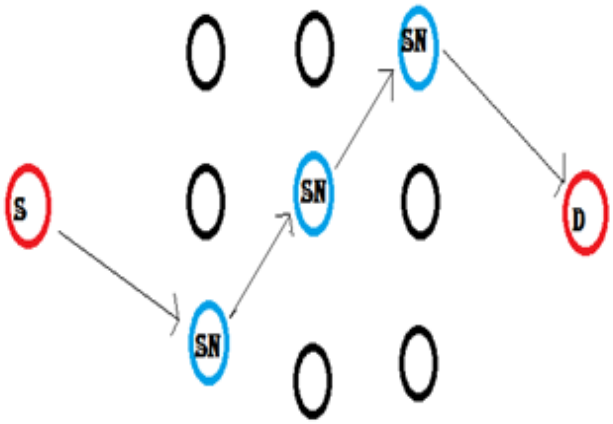

Fig1. *Secure transmission scenario with SSR*

2.1.1. Algorithm in source node

a. Detect all neighbouring nodes.

b. Look up the linked list of neighbouring nodes.

c. Find a match between the neighbouring nodes detected and nodes in the list.

d. Transmit data packet to the first match found.

2.1.2. Algorithm used in intermediary nodes

1. Receive incoming data packet
2. Check its destination address
   2.1. If the destination address is the address of the particular node process the data packet
   2.2. If it is a broadcast packet check whether the packet source was the same node itself , if so discard else broadcast the packet to all neighbouring nodes from the list.

2.3. else forward the data packet after finding the best secure next node from the list.

(if the destination is an immediate successor transmit packet directly or else to the next nearest node after reducing TTL)

3. If TTL is 0 discard packet and send an ICMP destination unreachable query.

2.1.3. Algorithm used in destination nodes

- Receive incoming packets and process the same.

As the mobile nodes are static the route remains the same unless a path failure occurs. In such a case packets are dropped rather than transmitting them through insecure nodes. The lookup process through the node's linked list takes O(n) times and so is performed the first time a packet is being transmitted . In case of mobility where nodes tend to move in a random walk fashion a search needs to be performed each time an update is received from a neighbouring nodes. Updates are sent after specific time intervals in this case.

2.2. Design of Secure Source Routing for dynamic nodes

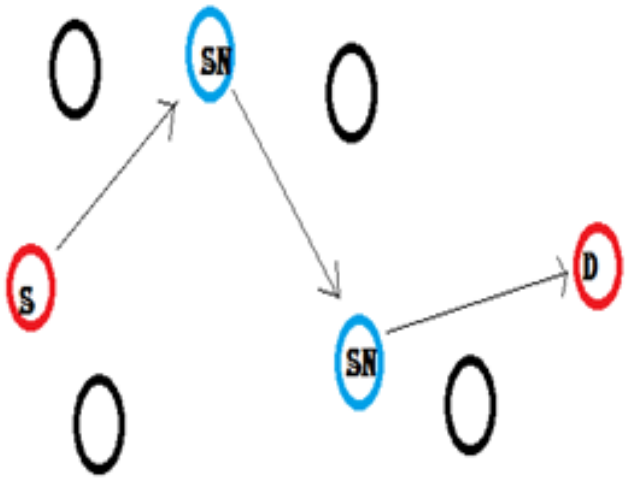

Fig2. *Secure Source Routing in dynamic mobile nodes*

The figure illustrates the case of mobile nodes.

Here wireless nodes tend to move in a random fashion. The source may tend to move near insecure nodes. Even under such circumstances the nodes perform a linear search in the linked lists and transmit only through secure nodes. The insecure nodes unlike when AODV protocols are used are unable to capture the messages being transmitted.

The algorithms used by the source intermediary and destination nodes are the same. But a route update must be performed at periodic intervals. The updated path information is being broadcasted through the network by nearby nodes in the secure path .This has a slightly large overhead. The broadcasted packets are treated in the same manner as specified in the previous algorithm.

3. SIMULATION ANALYSIS

The Experimental set up consists of 9 nodes and a source and destination as shown in the design phase. The data packets use TCP packets with a size of 1500 Mb/s. The graph shows the Round Trip Time (RTT) taken by packets during transmission. The green lines show the RTT of AODV protocol where insecure nodes are never bypassed. The red line shows the RTT of SSR where transmission takes place only through secure nodes. The X axis shows the time at which packets are sent and the Y axis the RTT time of these packets.

The graph clearly shows that SSR has lesser RTT on average compared to AODV systems. The only cases when AODV has better performance that SSR is when insecure nodes have lesser load compared to secure nodes. The Experimental setup incase of mobile nodes consists of 11 nodes

with a source, destination, 2 secure nodes and the remaining insecure nodes. The graph is as follows.

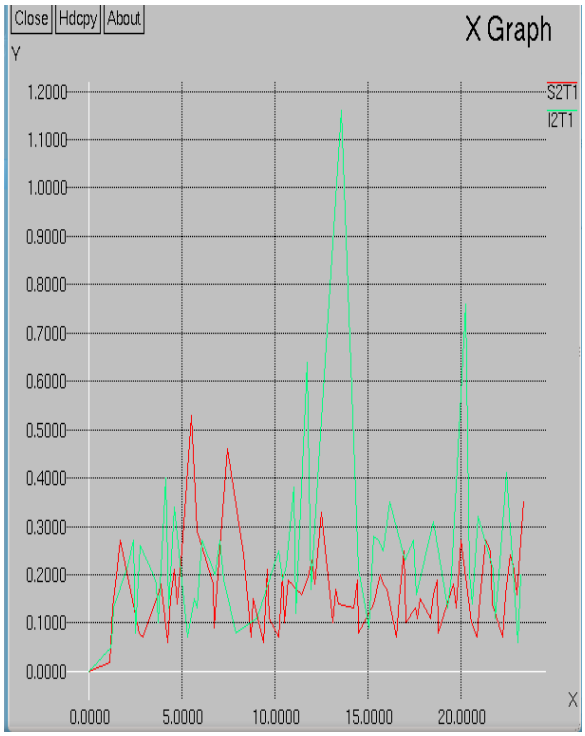

Fig3. *Packets Round Trip Time (static case)*

The red lines show the RTT of SSR where transmission takes place only through secure nodes. The X axis shows the time at which packets are sent and the Y axis the RTT time of these packets. The graph clearly shows that SSR has lesser RTT on average compared to AODV systems. The only cases when AODV has better performance that SSR is when insecure nodes have lesser load compared to secure nodes.

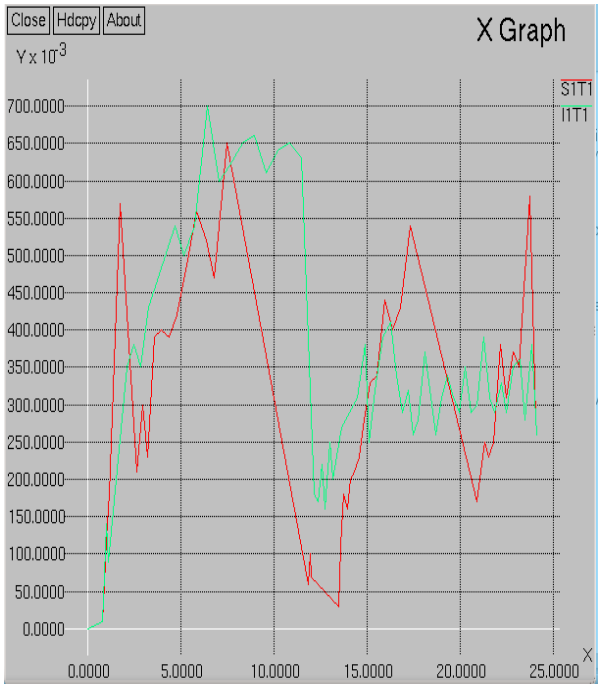

Fig4. *Packets RTT (dynamic case)*

4. CONCLUSION

This paper has been motivated by the need to support opportunistic data forwarding in *MANETs* This is fundamentally different from traditional IP forwarding in proactive routing with more

built-in adaptively, where the routing information maintained at nodes closer to the destination is often more updated than the source node. SSR could be used for secure transmission of data packets from source to destination where the path can be specified as a part of source routing. It is a pure network layer scheme that can be built atop off-the-shelf wireless networking equipment. Nodes in the network use a lightweight proactive source routing protocol to determine a list of intermediate nodes that the data packets should follow en route to the destination. Here, when a data packet is broadcast by an upstream node and has happened to be received by a downstream node further along the route, it continues its way from there and thus will arrive at the destination node sooner. This is achieved through cooperative data communication at the link and network layers. This work is a powerful extension to the pioneering work of ExOR.

REFERENCES

[1] Z. Wang, Y. Chen, and C. Li, "CORMAN: A novel cooperative opportunistic routing scheme in mobile ad hoc networks," IEEE J. Sel. Areas Commun., vol. 30, no. 2, pp. 289–296, Feb. 2012.

[2] Z. Wang, Y. Chen, and C. Li, "PSR: A Lightweight Proactive Source Routing Protocol For Mobile Ad Hoc Networks," IEEE J. Sel. Areas Commun., vol. 63, no. 2, pp. 859–868, Feb. 2014.

[3] G. Aggelou, Mobile Ad Hoc Networks: From Wireless LANs to 4G Networks, McGraw-Hill Professional, Nov. 2004.

[4] E. Baccelli, K. Mase, S. Ruffino, and S. Singh, "Address auto configuration for MANET: Terminology and problem statement," IETF draft, Aug. 2008.

[5] H. Luo, X. Meng, R. Ramjee, P. Sinha, and L. Li, "The design and evaluation of unified cellular and ad-hoc networks," IEEE Trans. Mobile Comput., vol. 6, pp. 1060–1074, Sept. 2007.

[6] Z. Wang, C. Li, and Y. Chen, "PSR: Proactive Source Routing in Mobile Ad Hoc Networks," in Proc. 2011IEEE Conference on Globa Telecommunications (GLOBECOM), Houston, TX USA, December 2011.

[7] Z. Wang, Y. Chen, and C. Li, "A New Loop-Free Proactive Source Routing Scheme for Opportunistic Data Forwarding in Wireless Networks," IEEE Communications Letters, to appear.

[8] C. E. Perkins and E. M. Royer, "Ad hoc On-Demand Distance Vector (AODV) Routing," RFC 3561, July 2003. [Online]. Available: http://www.ietf.org/rfc/rfc3561.txt

[9] M. K. Marina and S. R. Das, "Routing Performance in the Presence of Unidirectional Links in Multihop Wireless Networks," in The Third ACM International Symposium on Mobile AdHoc Networking and Computing.