ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

A QOS-Traffic Based Distributed Routing Protocol Secure Link State Topology Using Zone-Based Hierarchical Link State Routing Protocol

S. Divya [1], D. Kalaivani[2]

M.Phil Scholar, Department of Computer Science, Dr.SNS Rajalakshmi College of Art and Science College, Coimbatore, Tamil Nadu, India

H.O.D, Department of Computer Technology, Dr.SNS Rajalakshmi College of Art and Science College, Coimbatore, Tamil Nadu, India

ABSTRACT: Wireless is a more modern alternative to traditional wired networking that relies on cables to connect networkable devices together. Wireless technologies are widely used in both home and business computer networks. Wireless networks have been developed with various wireless applications, which have been used in areas of commerce, emergency, services, military, education and entertainment. The rapid improvement of Wi-Fi capable mobile devices including laptops and handheld devices, for example the purpose of wireless internet users of smart phone in last three years. The usage of people watching video, playing games and making long distance video or audio conferencing through wireless mobile devices and video streaming applications on infrastructure wireless networks which connects directly to mobile users for video playing and interaction in real time are increased. The evolution and the anticipate future of real time mobile multimedia streaming services are extensively expanded, so the networks are in need of high Quality of Service(QoS) to support wireless and mobile networking environment. In fact, there is an increasing attention from the industry and the research community on such issue. As a result, some hybrid wireless network architectures have emerged combining multi-hop radio relaying and infrastructure support, aiming to provide high capacity wireless networks. Also, an emerging challenge, in this context, lies in introducing the computation grid concept in such hybrid wireless networks environment. One promising trend is to harvest the widespread resources of wireless mobile devices, such as PDAs and laptops, to be beneficially useful within one or more mobile grid clusters. On the other hand, mobile nodes could benefit from the large resources in the fixed grid clusters.

KEYWORDS: Mobile Ad Hoc Network (MANET), Zone-based Hierarchical Link State Routing Protocol, Map Based Movement Model.

I. INTRODUCTION

Mobile Ad Hoc Network (MANET) can be described as an autonomous collection of mobile nodes (users) that communicate over relatively low capacity wireless links, without a centralized infrastructure. In these networks, nodal mobility and the wireless communication links may lead to dynamically changing and highly unpredictable topologies. All network functions such as routing, multi-hop packet delivery, and mobility management have to be performed by the member nodes themselves, either individually or collectively. So, network performance becomes highly dependent on collaboration of all member nodes. MANETs find applications in diverse fields ranging from low-power military wireless sensor networks to large-scale civilian applications, and emergency search/rescue operations.

Hybrid Wireless Communication (HWC) is one of the popular among the people for sharing the resources among the networks. This Hybrid approach is based on the combination of sensor, mobile ad hoc, vehicular ad hoc network for sharing the resources in the distributed network. With the use of this communication people often needs the QOS while transferring the data [1]. In MOBILE ad hoc networks (MANETs) have expanded a great deal of concentration since of its considerable advantages brought about by multihop, infrastructure-less transmission. Due to the error prone wireless channel and the dynamic network topology, consistent data delivery in MANETs, mainly in this challenge environment

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

with high mobility remains an issue. In the real world, a numerous applications need data delivery to multiple destination nodes which is defined as multicasting, where the access of multicast routing is an ideal approach to manage and reduce network traffic and cost of the network including bandwidth. Oftentimes these services are required over extremely in dynamic networks, which is Hybrid approach of above combination of ad hoc network. These networks are dynamic because of the mobility of the nodes in the network and/or the random sleep/awake cycles that are often utilized to minimize energy dissipation of the devices [2].

The rest of this paper is organized as follows. In Section 2 review the existing related work. The proposed models and descriptions are described in Section 3. Finally conclude the paper in Section 4.

II. RELATED WORK

In [1] authors discussed an adhoc network is the cooperative engagement of a collection of mobile nodes without the required intervention of any centralized access point or existing infrastructure. The authors presented Ad-hoc On Demand Distance Vector Routing (AODV) a novel algorithm for the operation of such adhoc networks. Each Mobile Host operates as a specialized router and routes are obtained as needed (i.e. on-demand) with little or no reliance on periodic advertisements. In [2] authors studied about the increasing popularity of wireless communications and the different QoS requirements of new types of service lead to higher demands on cellular mobile networks. With central control and multi-hop communication, relay based cellular networks are seen as an effective way to meet users' increased bit rate requirements while still retaining the benefits of a cellular structure. In [3] authors illustrated about the novel packet delivery mechanism called Multi-Path and Multi-SPEED Routing Protocol (MMSPEED) for probabilistic QoS guarantee in wireless sensor networks. The QoS provisioning is performed in two quality domains, namely, timeliness and reliability. Multiple QoS levels are provided in the timeliness domain by guaranteeing multiple packet delivery speed options. In [4] authors proposed a new cooperative communication protocol, which achieves higher bandwidth efficiency while guaranteeing the same diversity order as that of the conventional cooperative schemes. The proposed scheme considers relay selection via the available partial channel state information (CSI) at the source and the relays. In particular, we discuss the multi-node decode-and-forward cooperative scenarios, where arbitrary N relays are available. The source determines when it needs to cooperate with one relay only, and which relay to cooperate with in case of cooperation, i.e., "When to cooperate?" and "Whom to cooperate with?". An optimal relay is the one which has the maximum instantaneous scaled harmonic mean function of its source-relay and relay-destination channel gains. In [5] authors proposed a distributed optimal relay selection scheme in wireless multi-hop cooperative networks where the wireless channels are modeled as first-order finite-state Markov channels (FSMCs) and adaptive modulation and coding (AMC) is applied. The FSMC model is used to approximate the time variations of the average received signal-to-noise ratio (SNR).

III. PROPOSED ALGORITHM

The proposed architecture accepts the simulation parameters as input which contains the NS2.34 simulation where the optimal secure Zone-based Hierarchical Link State Routing Protocol is applied to the mobile Adhoc network. This overall proposed architecture in figure 1.1 follows a routing procedure form start to end state.

A. *NETWORK TOPOLOGY*

The network simulations are evaluated in networks of N number of nodes. As the number of nodes in the ad hoc network is increased, the dimension of the simulation area is also increased so that a consistent node density is maintained. The simulation areas are 1451m x 1000m, and 1000m x1000m, respectively. All mobile nodes move according to the map-based mobility waypoint model. Node speeds are randomly distributed between zero and some maximum, where the maximum speed varies between 0 and 20 m/s. The pause time is consistently 10 seconds. Each data point represents an average of 10 runs with the same traffic models, but different randomly generated mobility scenarios. The second set of simulations examines the performance of the two routing schemes with different percentages of Internet (wired) traffic. Random traffic connections of TCP and CBR can be setup between mobile nodes using a traffic-scenario generator script. It can be used to create CBR and TCP traffics connections between wireless mobile nodes. In order to create a traffic-connection file, we need to define the type of traffic connection (CBR

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

or TCP), the number of nodes and maximum number of connections to be setup between them, a random seed and incase of CBR connections, a rate whose inverse value is used to compute the interval time between the CBR packets. Directives for GOD are present as well in node-movement. The General Operations Director (GOD) object is used to store global information about the state of the environment, network, or nodes that an omniscent observer.

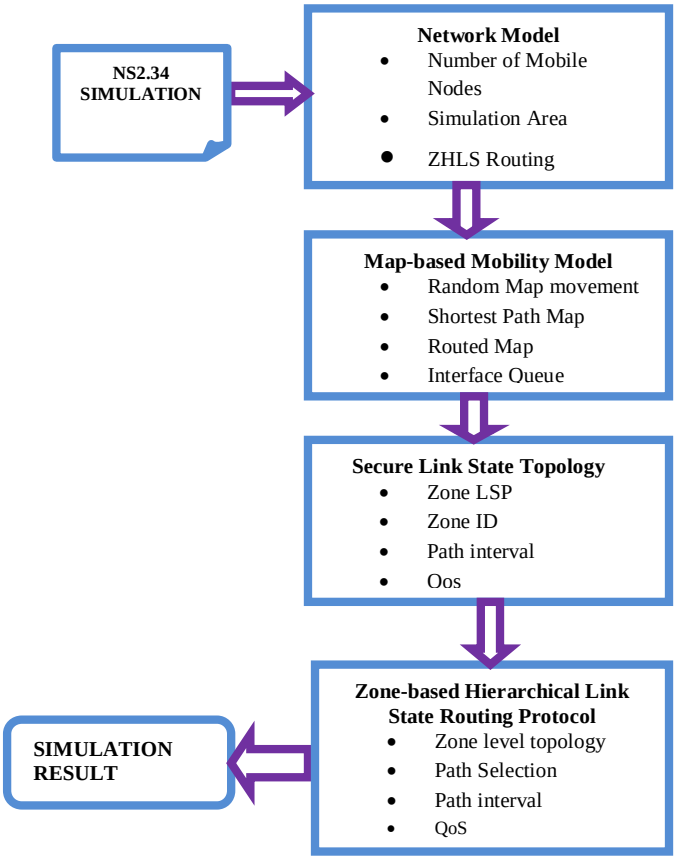

Fig 1.1: Proposed System architecture diagram

B. ***MAP-BASED MOBILITY MODEL***

A map-based mobility model that forces Mobile Nodes (MN) to travel to the edge of the simulation area before changing direction and speed. This model does not suffer from the density waves in the center of the simulation space that Random Waypoint model does. In this model, MNs choose a random direction in which to travel similar to the Random Walk Mobility Model. An MN then travels to the border of the simulation area in that direction. Once the simulation boundary is reached, the MN pauses for a specified time, chooses another angular direction (between 0 and 180 degrees) and continues the process.

C. ***SECURE LINK STATE TOPOLOGY***

The secure link-state protocol (SLSP) is basic functionality is to discover adjacencies and disseminate both topology and name prefix information. Such functionality may appear to be straight-forward to design and implement. However, because SLSP uses data networking (DN) Interest and Data packets to propagate routing updates, the design must shift away from the familiar concepts of pushing packets to given network addresses (i.e., any node can send any packet to any other node). Instead, one must think in terms of data names and data retrieval. More specifically, we need a systematic naming scheme for routers and routing updates. It also need to retrieve routing updates promptly without a priori knowledge of when an update may be generated, since a topology or name prefix change can happen any time. In

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

terms of routing functionality, SLSP distinguishes itself from previous link-state routing protocols in two aspects: (a) providing multiple next hops for each name prefix instead of a single one; and (b) signing and verifying all LSAs to ensure that each router can originate only its own prefix and connectivity information.

D. ***ZONE-BASED HIERARCHICAL LINK STATE ROUTING PROTOCOL***

The Zone hierarchical links state Routing Protocol (ZHLS) was the first Hybrid routing protocol. It was proposed to reduce the control overhead of Proactive routing protocol and to decrease the latency of Reactive routing protocol. It is suitable for the networks with large span and diverse mobility patterns. For each node a routing zone is defined separately. Within the routing zone, routes are available immediately but for outside the zone, ZHLS employs route discovery procedure. For each node, a separate routing zone is defined. The routing zones of neighboring nodes overlap with each other's zone. Each routing zone has a radius ρ expressed in hops. The zone includes the nodes whose distance from the source node is at most ρ hops.

The nodes whose minimum distance to central node is exactly equal to the zone radius ρ are Peripheral Nodes while the nodes whose minimum distance is less than the zone radius ρ are Interior Nodes.

IV. PSEUDO CODE

Algorithm: Secure Distributed Map Detection Algorithm

Step 1: A source node needs a route to destination the protocol starts route discovery. During route discovery, source node broadcast RREQ packets through neighboring nodes.

Step 2: While receiving the RREQ packet each node update their routing table

Step 3: Compare both Neighbor List (NL) and calculate the number of common neighbor nodes (common_node) present between sources to destination

```
For i=0;i<number_of_source_neighbors;i++
For j=0;j< number_of_destination_neighbors;j++
        If (NLS(i) =NLD(J))
        Common _node++;
```

Step 4: Initialize one hop neighbors can reach target node with maximum of 3 hop and minimum of 1 hop. If maximum target_hop_count exceeds 3 then target node and their previous hop may be the attacker node.

Step 5: If target_node_count > node_count_thresh then declare the target node and their previous hop nodes are attacker nodes.

Step 6: Send attacker announcement message to all nodes.

Step 7: Any node receives attacks announcement message it removes attacker node id from its neighbor table and Routing Table.

V. CONCLUSION AND FUTURE WORK

In this paper proposed the implementation for developing the Secure Trust Based Routing Protocol For MANETs algorithm uses NS 2.34 simulator. In MANET, networks are more vulnerable to attacks than wired networks. So security is an important issue in MANET to provide secure communication between mobile nodes. Due to the misbehavior of malicious nodes, performance of MANET degrades. To overcome this problem secure routing protocols need to design which is a more difficult and challenging too. Different approaches are already proposed to secure the routing process in MANET. Secure trust based mechanisms are used in routing protocols to secure the routing information from tampering it by the attacker. But this approach can't be deployed in real MANET network because of high computational cost and it can't identify the attacker nodes. This mechanism only secures the routing information from tampering but can't secure nodes that participate in routing. So the trust mechanism is adopted in routing

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

protocols to secure nodes as well as the data transmission. Different trust based routing protocols are proposed to provide security in MANET by securing nodes in routing path.

REFERENCES

1. Shah R, Rabaey J. Energy aware routing for low energy ad hoc sensor networks. Proceedings of IEEE WCNC'02,Orlando, FL, March, 2002; 350-355.
2. Ye Ming Lu, Vincent W.S. Wong, An energy efficient multipath routing protocol for wireless sensor networks, International Journal of Communication System 20 (7) (2007) 747-766.
3. S. Das, C. E. Perkins, E. Royer, "Ad Hoc On Demand Distance Vector (AODV) Routing", IETF Draft, June 2002.
4. P. Jiang, J. Bigham, and J. Wu, "Scalable QoS Provisioning and Service Node Selection in Relay Based Cellular Networks," Proc. Fourth Int'l Conf. Wireless Comm. Networking and Mobile Computing (WiCOM), 2008.
5. E. Felemban, C. Lee, and E. Ekici, "MMSPEED: Multipath Multi-Speed Protocol for QoS Guarantee of Reliability and Timeliness in Wireless Sensor Networks," IEEE Trans. Mobile Computing, vol. 5, no. 6, pp. 738-754, June 2006.