IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727
PP 28-33
www.iosrjournals.org

Design New Secure Hybrid Hierarchical Link State Routing Protocol (Shhls) For Manet

*[1]K.Thamizhmaran
Department of Electronics & Communication Engineering
Annamalai University
tamil10_happy@rediff.com

Abstract: *Current research developing year's lot of young research's interested in Mobile Ad-hoc Networks (MANET's) a collection of independent mobile nodes dynamically form a network connection temporarily without any base station of static infrastructure. The self-configuring ability of nodes in MANETs made it popular among critical applications like military use or natural emergency recovery. Most of the proposed protocols assume that all nodes in the network are cooperative, and do not address any security issue. To adjust to such trend, it is vital to address its potential security issues. The main objective of this paper is design new secure routing protocol namely, Secure Hybrid Hierarchical Link State (SHHLS) routing protocolto define the path for security and to further improve performance and at the sametime to create energy enhanced way with excellent security. We are implementing secure dynamic on-demand routing protocol in order to achieve security goals for following parameters packet delivery ratio, routing overhead, average energy and throughput. The proposed model test SHHLS with existing Zone Hierarchical Link State (ZHLS) hybrid routing protocol and analysis stimulated through Network Simulated (NS2).*

Keywords*: MANET, Security issues, Routing Protocol, ZHLS, SHHLS, NS2.*

I. Introduction

A mobile ad-hoc network is a collection of all independent mobile nodes that can communicate with each other through radio waves. The mobile nodes that are in the radio range of each other can directly communicate, whereas others need the aid of intermediate linked nodes to route their packets. Each of the nodes has a wireless interface to communicate with each other. These networks are fully dynamically distributed, and can work at any place without the help of any fixed infrastructure as base stations. MANET's provides high mobility and device portability's that enable to node connect network and communication to each other. It allows the devices to maintain connection to the network as well as easily adding and removing devices in the network. User has great flexibility to design such a network at cheapest cost and minimum time. Mobile ad-hoc network consist large number of node, it form temporary network with dynamic topology. In this network each node communicates with each other through radio channel without any central authority. In MANET's each node operates in a distributed peer -to-peer modes, serves as an independent router to forward message sent by other nodes. MANET suffers from a great efficiency loss due to the misbehaving nodes which may be constrained by the resources as battery power and bandwidth of topology. Different approaches have already been proposed to detect and prevent the misbehaviour in MANET. In ad-hoc network nodes are try to disrupt the proper functioning network, Modifying packets, injecting packets or creating routing loops. In this case Security is an important task. There are large numbers of secure routing protocols proposed by many researchers they fulfill different security requirements and prevent specific attacks show in figure 1 MANET.

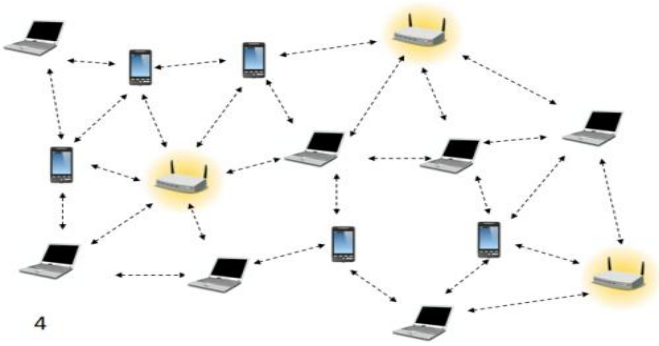

Figure 1 mobile ad-hoc networks

1.1Routingprotocols

They are divided into three categories routing protocol such as: reactive routing protocol, proactive routing protocol and hybrid routing protocol.

Table Driven / Proactive*:* Proactive routing protocols acquire routing information periodically and store them in one or more routing tables. The differences among the protocols in this class are routing structure, number of tables, frequency of updates, use of hello messages and the existence of a central node. Therefore, each protocol reacts differently to topology changes. Flooding of routing information is the mechanism that is often used to discover and update routes

On-Demand / Reactive*:* Reactive routing protocols discover or maintain a route as needed. This reduces overhead that is created by proactive protocols. Flooding strategy is used to discover a route. Reactive routing protocols can be classified into two groups: source routing and hop by hop routing. In source routing, data packet headers carry the path to destination. Hence, intermediate nodes do not care about maintaining the routing information. On the other hand, this kind of protocols may experience high level of overhead as the number of intermediate nodes increases. Also they have a higher chance of a route failure.

Hybrid: This protocols exhibit both reactive and proactive features. Proactive strategy is used to discover and maintain routes to nearby nodes, while routes to far away nodes are discovered reactively. Consequently, overheads and delay that are introduced by proactive protocols and reactive protocols, respectively, are minimized. Hybrid protocols have been known to be more scalable than others fewer nodes take part in routing and topology discovery. Showin figure 2 categories of MANET routing protocols.

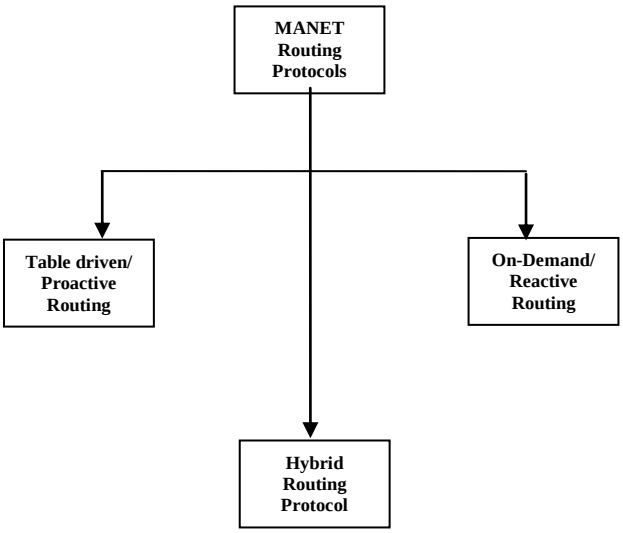

Figure 2 Categories ofMANET routing protocols

II. Literature Survey

Secure quality of service in sudden on-demand distance vector routing was detected by C.E. Perkins et al (2001). Secure economical distance vector routing for mobile wireless sudden networks was done by Y. Hu et al (2002). A cooperative intrusion detection system for ad-hoc networks was implemented Yian Huang, et al (2003). Security in mobile ad-hoc network challenges and solutions was analysis by Yang, et al (2004). Malicious nodes detection in AODV-based mobile ad-hoc networks was addressed by Jongoh Choi et al (2005).A survey of issues and solutions was taken by T. Reddy et al (2006). An acknowledgment-based approach for the detection of routing misbehaviour in MANETs was discussed by Liu et al (2007). Security and QOS self-optimization in mobile sudden networks was done by Z. Shen (2008). Quality of service provisioning in sudden wireless networks was analyzed by H. Chinese et al (2009). The detection of packet dropping attack using improved acknowledgement based scheme in MANETs was done by Aishwarya Sagaret al (2010). Secure routing for wireless mesh network was discussed by Celia li et al (2011). Authentication and intrusion detection in Edouard Manet was done by K.Thamizhmaran et al (2012). Secure intrusion detection system for MANETs was done by Shakshuki et al (2013). Implementation of A3ACK's intrusion detection system under various mobility speeds was highlighted by Abdulsalam Basabaaa et al (2014). However, all these algorithms address only the security problem. It is well known that the topology changes rapidly in MANETs due to the

characteristics of wireless networks. The proposed approach scheme SHHLS is also based on this assumption to provide secure transmission with minimum delay.

III. Problem Identification

Network wide routing in MANETs is a vital task oftransferring data from a source to destination. The dynamicnature of MANETs requires the routing protocols to refreshthe routing tables frequently that suffer from transmissioncontention and congestion that are the results of thebroadcasting nature of radio transmission since a node in aMANET cannot directly communicate with the nodesoutside its communication range, a packet may have to berouted through intermediate nodes to reach the destination.So it also becomes essential to monitor the constraints inintermediate nodes. Consequently, an efficient routingapproach may generate route failures. The simplest schemerouting in MANET is the one to find a route withoutmalicious nodes. This paper aims to provide an unbreakableroute for secured transmission. We design new routing protocolnamed SHHLS. This SHHLS provides better performancecompared to the existing reactive routing protocols and also reduces routing overhead without any misbehaviour at intermediate nodes.

IV. Proposed System

Secure Hybrid Hierarchical Link State (SHHLS) routing protocol like hybrid routing protocol with more secure, is that topology information is transmitted by nodes both table-driven and on-demand.

RREQ - As an optimization SHHLS uses an expanding ring technique when flooding these messages. Every RREQ carries a time to live (TTL) value that states for how many hops this message should be forwarded.

RREP - RREQ if the receiver is either the node using the requested address, or it has a valid route to the requested address.

RERR - When a link breakage in an active and secure route is detected, a RERR message is used to notify other nodes of the loss of the link.

Node 1 after receiving the further detection message broadcast a RREQ message by setting destination address to source nodes address. If it receives a RREP message from the malicious node, it sends a Test packet (TP) to the source node via malicious node, and at the same time it sends an Acknowledgment Packet (AP) to Source Node (SN) though some other route.

Design of Shhls:

1. Source node broadcast RREQ with secure packet (SRREQ) along with the destination ID.
2. For every intermediate receives the SRREQ check.
3. For every node IN receives RREP with secure Check (SRREP).
4. After receiving the reply, source node broadcast a FD message to all mobile nodes.
5. For every mobile node receive further detection message.
6. Source node waits for “wt” time
7. If all the flags are “N”
8. End.

1.1 Simulation Parameter

Table 1 Simulation parameters

Parameter	Values
Examined protocol	SHHLP, ZHLS
Application traffic	CBR
Transmission range	800m
Packet size	512 bytes
Maximum speed	25m/s
Simulation time	700s
Number of nodes	20, 40, 60, 80, 100
Area	800x800m

V. Reselts & Discussion

In this paper discuss SHHLS and ZHLS with follow above simulation parameters.

Table 2 packet delivery ratio

RP / NN	20	40	60	80	100
SHHLS	0.84	0.78	0.72	0.66	0.60
ZHLS	0.90	0.84	0.78	0.72	0.66

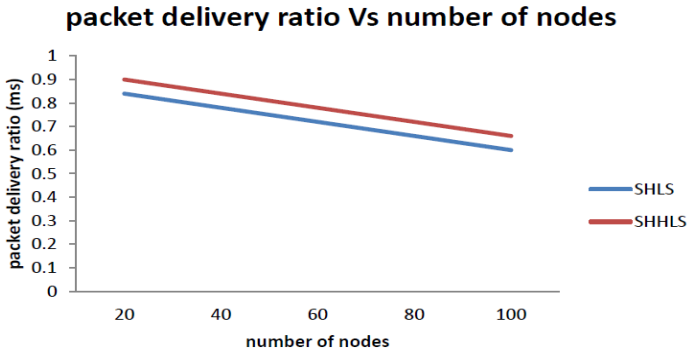

Figure 3 packet delivery ratio Vs. number of nodes

From Figure 3 and Table 2, it is clear that secure proposed scheme SHHLS surpasses ZHLS performance by above 70% when there are 30 and 150 nodes in the network.

Table 3 routing over head

RP / NN	20	40	60	80	100
ZHLS	0.17	0.23	0.29	0.35	0.41
SHHLS	0.14	0.20	0.26	0.32	0.38

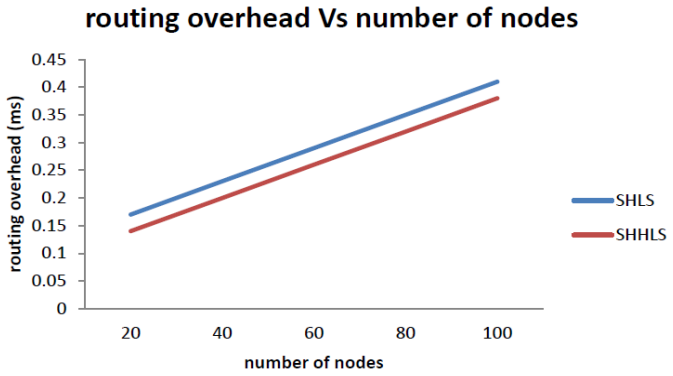

Figure 4 routing overhead Vs. number of nodes

Simulation results of routing overhead shown in Figure 4 and Table 3. It is clear that SHHLS has the lowest overhead of about 30 to 150 number of nodes.

Table 4 throughput:

RP / NN	20	40	60	80	100
ZHLS	0.13	0.25	0.38	0.51	0.55
SHHLS	0.22	0.34	0.47	0.60	0.64

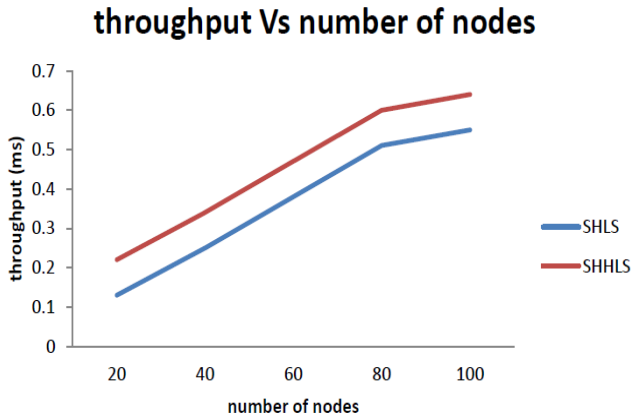

Figure 5 throughput Vs. number of nodes

Figure 5 and Table 4 proves that the proposed SHHLS provides better performance of the throughput when there are 30 to 150 of nodes compared to ZHLS routing protocol.

Table 5 Remaining energy:

RP / NN	20	40	60	80	100
SHHLS	0.88	0.81	0.74	0.67	0.60
ZHLS	0.94	0.85	0.78	0.71	0.64

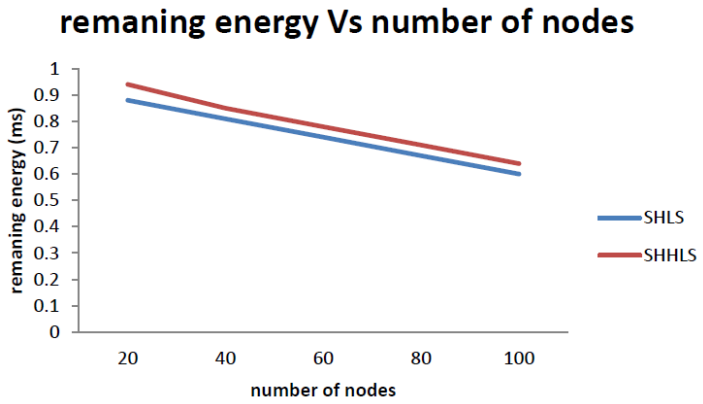

Figure 6 remaining energy Vs. number of nodes

Figure 6 and Table 4 clearly show that the proposed SHHLS increases the remaining energy with increasing number of nodes from 30 to 150 compared to ZHLS.From all the above figures and tables, it is clear that the comparison of the SHHLS illustrate that the proposed algorithm outperforms the ZHLS by providing lowest end-to-end delay, packet drop and routing overhead with increase in the number of nodes.

VI. Conclusion And Future Work

Link breakage, misbehaviour attack and packet dropping have always been a major threat to the security in MANETs. In this research paper, a novel approach named SHHLS protocol newly implemented specially designed for MANETs is proposed in comparison with other popular protocol named ZHLS through simulations. The results demonstrated positive performance of the remaining energy in SHHLS than ZHLS. Although it generates more end-to-end delay in some cases, as demonstrated in this research, it can vastly improve the network's PDR to more than 6% compared to the existing ZHLS routing protocol and improve remaining energy by 3% compared to the existing ZHLS routing protocol when the misbehavior attackers. Eventually, it is arrived to the conclusion that the SHHLS scheme is more suitable to be implemented in MANETs also plan to investigate the following issues in our future research.

1. The same concept can be applied in satellite to reduce more congestion in the route and also to save more energy.
2. The performance of SDORP can be tested in real time network environment instead of software simulation.

Reference

[1]. C.E. Perkins, et al. "Quality of Service in Ad Hoc on-Demand Distance Vector Routing", IETF Internet draft, 2001.
[2]. Y. Hu, et al. "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks", in Proc. 4th IEEE Workshop Mobile Computer System Application, 2002, pp.3–13.
[3]. Yian Huang, et al "A Cooperative intrusion detection System for Ad Hoc Networks" Proceeding of the 1st ACM workshop on security of ad-hoc and sensor networks, pp. 135-147, 2003.
[4]. Yang, et al "Security in mobile ad-hoc Network: challenges and solutions" IEEE wireless Communications, pp. 38-47, 2004.
[5]. Anand Patwardhan and Iorga, Secure routing and Intrusion Detection in Ad-hoc networks, in Proc. 3rd Int. Conf. Pervasive Computer Communication, pp.191–199, 2005.
[6]. T. Reddy, et al. "Quality of Service Provisioning in Ad Hoc Wireless Networks: A Survey of Issues and Solutions", Ad Hoc Networks, Vol. 4, No. 1, pp.83-124, 2006.
[7]. K. Liu, et al. "An acknowledgment-based approach for the detection of routing misbehaviour in MANETs",IEEE Trans., Vol. 6, No. 5, pp.536–550, 2007.
[8]. Z. Shen, et al. "Security and QoS Self-Optimization in Mobile Ad Hoc Networks", IEEE Trans. Mobile Computing, Vol. 7, pp. 1138-1151, 2008.
[9]. H. Wu, et al. "QoS Multicast Routing by Using Multiple Paths/Trees in Wireless Ad Hoc Networks", Ad Hoc Networks, 2009, Vol. 5, No. 2, pp.600-612.
[10]. Aishwarya Sagar and Meenu Chawla, Detection of Packet Dropping Attack Using Improved Acknowledgement Based Scheme in MANET, IJCSI, Vol.7, Iss.4, No.1, pp.12-17, (2010).
[11]. RushaNandy, et al "Study of various attacks in MANET and Elaborative discussion of Rushing attack on DSR with clustering scheme" international Journal Advanced networking and Applications, Vol. 3, pp. 1035-1043, 2011.

[12]. K.Thamizhmaran, et al. "Authentication and Intrusion Detection in MANET", International Journal of Advance Research in Technology, Vol. 3, No. 3, pp.15-21, 2012.
[13]. Shakshuki, et al, EAACK — A Secure Intrusion: Detection System for MANETs, IEEE Trans on industrial electronics, Vol. 60, No. 3, pp. 1089-1098, 2013.
[14]. Prabu, K. and Subramani, A. Energy efficient routing in MANET through edge node selection using ESPR algorithm, Int. J. Mobile Network Design and Innovation, Vol. 5, No. 3, pp.166–175, (2014).

Prof. K. Thamizhmaranhas received his M.E degree from Annamalai University, Chidambaram and Tamilnadu, India in the year of 2010 and 2012 respectively. He is currently working as an Assistant Professor in ECE / Department of Electronics and communication Engg, FEAT, Annamalai University, Annamalainagar, Chidambaram, Tamilnadu., India. His research interested includes area includes Networks security, Ad-hoc Networks, Mobile Communications, Digital Signal Processing. He has published more than 74 technical papers at various National / International Conference and Journals. He is reviewer of 03 international journals and technical committee reviewer of 08 international conferences.He is a member of IAENG, IACSIT, ADSL.