International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 9 (2015) pp. 22927-22940

http://www.ripublication.com

Secure- ZHLS: Secure Zone Based Hierarchical Link State Routing Protocolusing Digital Signature

M V Narayana[1], G Narsimha[2], SSVN Sarma[3]

[1]Research Scholar, JNTUK Kakinada &Department of CSE, Global Group of Institutions, Hyderabad, AP,India
[2]Department of CSE, JNTUH College of Engineering, Jagityal, AP,India
[3]Department of CSE, Vagdevi College of Engineering, Warangal, AP, India
Mail id:mvnarayanacse@gmail.com

Abstract

Mobile Ad-hoc Network (MANET) is a prominent field in global network issues for last 10 years where ad-hoc routing in networks is one of the essential component. The goal of any routing protocol is to offer enhanced and efficient energy conscious and secure routing systems to Mobile Adhoc Networks. Zone Based Hierarchical Link State Routing Protocol (ZHLS) is one of the hybrid routing protocol in the Mobile ad-hoc network, which is vulnerable to a large number of safety intimidations that come from internal malicious nodes. Malicious nodes deliberately drops routing, data packets and interrupt the exact operation of routing protocol. To overcome this problem, a Secured ZHLS established on proficient key management, safe adjacent node detection, confident routing packets, revealing of mischievous nodes, and prevention of these nodes from harming the system is proposed. Security to the routing protocol is employed using an integrated traditional method of digital signature along with symmetric and asymmetric key encryption methods. The performance of the proposed methodology is analyzed by the packet delivery fraction, communication overheads in the network construction, route acquisition latency, and percentage of released packets when moved through mischievous nodes and compared with the existing ZHLS routing protocol.

Keywords: MANETS, Routing Protocols, ZHLS, Secure-ZHLS, Digital Signature

Introduction

The latest improvements in wireless technology had led to the enlargement of an innovative wireless scheme known as Ad-hoc Network. An ad-hoc network permits wireless devices to communicate with each other straightly. In this system, every node plays a dual role at the same time and works as a host in reality. Formerly, it acquires some data about the neighboring network and associates it with the procedures that are established to tackle the process of sending and receiving data packets. This amalgamation of both the methods are named as a routing protocol. A Mobile ad hoc network is a self-initiating and self-functioning process of moving objects that are linked to each other by means of wireless network with a supportive arrangement of a group of mobile nodes without any centralized structure at an admittance point or prevailing system.

A node can send information to a destination node beyond its broadcasting range and accomplish further nodes as convey points where a node functions as a router. The indiscriminate movement of nodes in MANET fluctuates the network topology promptly at irregular times [12, 13]. Since MANETs are described with its self-organize nature, the energetic alteration of network topology, restricted bandwidth, and uncertainty of linking ability, etc., the consistency of data communication in the network is not definite. The Application of Mobile Ad hoc networking lies in the military, strategic and other security- sensitive tasks and also for the marketable customers. In these applications, secure routing is a significant concern.

The Hybrid routing protocols are defined as a group of innovative algorithms that are obtained from the existing proactive and reactive routing protocols. The hybrid protocols are derived from the proactive and reactive ones, containing the advantages of both the protocols that uses the properties of one kind and enhances it with the participation of the other kind. Proactive routing protocols have maximum overheads and minimum latency whereas reactive routing protocols have minimum overheads and maximum latency. Therefore, a Hybrid routing protocol is recommended to overwhelm the limitations of proactive and reactive routing protocols. These protocols are introduced to maximize the reliability and scalability of the network by permitting the adjacent nodes with the properties. These protocols function in a group as to minimize the expenses caused by route discovery process. This property typically achieved previously determining route of the adjacent nodes and later determine the route to the distant nodes by route discovery process [1].

Zone Based Hierarchical Link State (ZHLS) Routing Protocol

The Zone-based Hierarchical Link State routing (ZHLS) is a hybrid routing protocol that is discussed in this paper. A GPS system is employed with the ZHLS routing protocol as to recognize the physical location of the movable nodes in the network. Depending on the environment information of mobile nodes, the complete network is partitioned into numerous non-overlying regions. ZHLS employs a categorized addressing pattern that comprises of zone ID and node ID. Unlike, the other existing hybrid routing protocols, the ZHLS routing protocol does not function on any cluster heads in the network. In this routing protocol, merely the zone ID and node ID of the

mobile node are sufficient for essentially routing in the network where the routing is flexible even with altered network topology. A mobile node defines the zone ID based on its location and priory given zone map of the topology that is defined by all the other mobile nodes in the network. Therefore, it is presumed that a virtual link exist between the zones if there is at least one physical connection amongst the zones.

A bi-level network topology arrangement is determined in ZHLS [23] i.e. the node level network topology and the zone level network topology. Correspondingly, two categories of link state packets (LSP) in the network topology are defined. They are node level LSP and zone level LSP. The node level LSP comprises of a node ID of the adjacent nodes in the similar zone and the zone ID's of all the other zones in the network. A node occasionally transmit the node level LSP to every other node in the similar zone. Consequently, due to episodic node level LSP interactions, all nodes in a zone are similar to node level LSP. In ZHLS, the gateway node transmits the zone LSP all through system every time a virtual link is damaged or generated. Therefore, all the mobile nodes has its own distinguished zone level and node level topologies for the network.

Prior to sending the data packets, the source primarily examines its intra zone routing table. The routing information exist in the system, if the destination node and source node is in the same zone. Otherwise, the source node initiates a locality request to remaining zone with the help of gateway nodes. Then, a gateway node of the zone where the destination node exist, attains the locality appeal and responds with a locality reply encompassing of the zone ID of the destination. The zone ID and the node ID of the destination node are given in the header of the data packets initiated from the source node. At the time of packet progressing technique, intermediary nodes excluding nodes in the destination zone make use of inter-zone routing table, and an inter-zone routing table is employed when the packet reaches destination.

Motivation

In the literature, many research works have been dedicated to the strategy of optimal routing protocols for ad hoc systems [7, 8, 10]. This led to efficient solutions that minimize energy consumption or that are well suited to dynamic topologies, but do not take into account the security aspect. Due to the deficiency of a pre-specified centralized supervision for route detection procedure, MANETs are susceptible to outbreaks that leads to the deprivation of the performance of the network. Security assaults distract routing actions and generates numerous complications like Denial of Service, Jamming the network or other types of serious attacks in the network.

In order to address the problem of above mentioned security issues, a novel Secure Zone Based Hierarchal Link State (Secure-ZHLS) Routing Protocol is suggested in this paper by employing Digital Signature and Encryption & Decryption techniques into the routing protocols. Security is a very challenging problem for scheming a well-organized and secure routing protocol for MANETs. The infrastructure less and the vibrant environment of MANET demands innovative networking approaches to be initiated as to deliver efficient and secure end to end communication. Securing routing

protocols in ad hoc networks is a very complex and still topical domain due to the binding characteristics of these networks, and their high vulnerability to attacks.

Organization of the Paper

A brief discussion of Mobile Adhoc and Hybrid Routing Protocols along with its limitations are given in this section. Section 2 gives the brief explanations of the different existing routing protocols that employed the digital signature techniques and cryptography algorithms for proving security to sending data packets. A detailed explanation of the proposed secure routing protocol along with applied digital signature techniques is discussed in section 3. The experimental results and performance analysis is briefly given in section 4 followed by section 5 that concludes this paper with robust and secure communication of information using the proposed routing protocol.

Existing Methodologies

Several strategies have been proposed to secure ad hoc routing protocols [2, 3, 4, 5], but most of the proposed solutions are based on very complex cryptographic mechanisms, slow and consuming too many resources [2, 5, 6, 9, 11]. Hence, these solutions are not well appropriate to the ad hoc environment and significantly degrade the performance of the basic routing protocol. Papadimitratos and Haas [14] suggested Secure Routing Protocol (SRP) for on-demand source routing that attains reliability and legitimacy of routing packets by means of Message Authentication Codes (MACs). Although SRP is a fairly modest and light-weight elucidation, numerous inadequacies exist in it. In this SRP protocol, intermediary nodes in the route are not legitimate, consequently leading this protocol to attacks, containing updates and removal of authentic nodes from the route.

In [15] Secure Dynamic Source Routing (SDSR) protocol is suggested that uses digital signatures in addition to accretion of public Diffie-Hellmann and encrypted hashed keys. SDSR can certify route reliability and route cleanliness as well as deliver validation of entirely contributing nodes and exchange of session keys. Shiva et al offered [22] digital signature founded secure data broadcasting in wireless sensor networks. They employed the asymmetric key crypto system (public) for safety. To produce the digital signature MD-5 hash function is used. Changhui et al [19] recommended a methodology that offer a structure with hash based message authentication code to overwhelm the limitations. Hash based message authentication code employs cryptographic hash function such as SHA-1 in amalgamation with the secret key. It gives integrity of data communicated over an unpredictable medium created on the secret key.

S.Thadvai et al. [21] suggested an approach depending on message retrieval that comprises of the message and the signature where the communication cost is lesser for the message recovery technique. Authentication Encryption Scheme (AES) approach is employed to recuperate information. Nikos Komnios et al [20] proposed a two phase revealing methodology of nodes that are not accredited for any detailed

amenities and nodes that negotiated at the time of their actions in MANET. This approach functions in two phases, in phase one the unauthorized nodes are identified with the support of its adjoining nodes. In the second phase the negotiated nodes are spotted by a native agent that gathers and investigates the information. The problem with this methodology is that it depend on the adjacent node for authentication.
Bing Wu et al [2] suggested an approach by means of key management technique in MANET. The third party certification ability is responsible for controlling the credentials such as a novel issue or termination and revocation of certificates. Problem with this technique is that implementation of third party CA is multifaceted. Huang et. al. [16], [17] suggested a key distribution structure called double authentication to distinguish impersonation outbreaks to link state routing apprises. In this system, every router shares two symmetric keys: one key with all its adjacent and one key with all its adjacent of adjacent.

Proposed Methodology

Zone Based Hierarchical Link State Routing Protocol (ZHLS) is one of the hybrid routing protocols in the Mobile ad-hoc network, which is vulnerable to a large number of security threats that come from internal malicious nodes. It is observed from the recent survey that not much work has been done in the hybrid routing protocol in a way to provide security to the information that is passed between the nodes. In this proposed methodology, the author concentrates on providing security to the hybrid routing protocol i.e. the Zone Based Hierarchal Link State Routing Protocol by employing traditional Digital Signature technique. The Symmetric and Asymmetric key encryption technique are introduced while sending and in receiving information between two or more nodes. The detailed procedure of proving security to the information packets is given in this section.

Digital Signature

Digital signature is defined as an approach where the information is validated or authenticated by means of validates, that an obtained information is efficiently received from the sender like a signature on a paper document. A digital signature is a number that reliant on some hidden information acknowledged merely to the signer and additionally to the information of the message being signed. Signatures need to be certifiable if the differences ascends from a party signing a document, an unprejudiced third party must be capable to decide the situation justifiably, without necessitating any admittance to the signer's secret data. Digital signatures have numerous solicitations in information security, comprising of authentication, data integrity, and non-repudiation. The utmost important usage of digital signatures is the certification of public keys in huge network systems. Certification is a trusted third party (TTP) to hit the character of a consumer to a public key, so that at some same time, other individuals can validate a public key deprived of any support from a trusted third party.

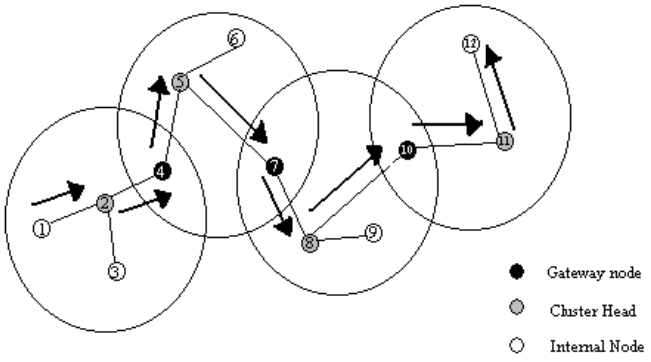

Figure 1: Node level and Zone Level destinations of Node 1

Secure ZHLS Routing Protocol Algorithm

The proposed Secure ZHLS Routing Protocol depends on the notion of Traditional ZHLS routing protocol. This is a hybrid routing protocol that needs to provide security mechanisms for performing security routing. Since ZHLS is depending on the idea of routing zones with constrained zone, it is more reasonable to apply the security mechanism surrounding this part instead of the whole broadcast region. The zones of routing protocol separate the communicating regions into the interior and exterior nodes thus, the information like network topology, hop count, neighbor data can be concealed to other nodes in the network and provide confidentiality to the whole network. The security is provided at the IP layer using this proposed routing protocol.

In the proposed routing protocol, the packets that used for communication can be either data packet or control packet. Two pair of keys are included in the packet amongst the source and destination nodes. They are encrypting and decrypting (either symmetric or Asymmetric) key and a signing and verifying key for signature. The packets are signed using the signature key at the source end and verified using verification key at the destination end. But the data or control Packets that carry secret information are both signed and encrypted. The control packets normally use the symmetric key since it is small in size and data packets make use of asymmetric key for encryption and decryption as it is larger in size. For node X the signing and verifying keys are SKx and VKx whereas the encrypting and decrypting keys are EKx and DKx.

Secure Node Based Links State Routing

In the intra-zone routing from Figure 1 let 1 be the source node and 4 be the destination node where data packet is send from the Source node 1 to destination node 4. Then node 1 looks for the route to the destination node 4 in the zone using its Node LSP routing Table and send the request packet to node 4 along with its Node ID.

$1 \rightarrow 4: [SKREQ, IP_4, \{NID_1, ZID_4\}, cert1]|sign1$

$Wheresign4 = [SKREQ, IP_4, \{NID_1, ZID_4\}, cert1]SK_4$

Here SKREQ is the secure request packet identifier, IP4 is the IP address of destination 4, NID1 is the node ID of node 1, cert1 is 1's certificate appended by signature sign1 using Symmetric Key SK1.

$$4 \rightarrow 1: [SKREP, IP_4, \{NID_1, ZID_4\}, cert4, \{K14\}EK_1]|sign4$$

$$WheresignY = [SKREP, IP_4, \{NID_1, ZID_4\}, cert4, \{K14\}EK_1]SK_4$$

Node 4 on getting this appeal, authenticates the signature using verification key VK1 which is extracted from 1's certificate and generates the session key K14. It is encrypted using the EK1 and send it to node 1 as a reply packet along the path. On receiving the SKREP packet to node 1, it authenticates the packet with VK4, decrypts with DK1 and excerpts the session key. Thus node 1 encrypts with K14, once it acquire session key K14 and send it to destination with the similar path.

Secure Zone Based Link State Routing

The inter zone routing is introduced with an on demand, secure route discovery procedure where source node discovers paths to the preferred inter zone. From Figure 1, it is observed that the data packet is sent from node 1 to destination node 12. Then node 1 looks for the route to the node 12 using the Zone LSP routing Table and Node LSP routing Table with in the zone and sends the request packet to node 12 along with its Zone ID, Node ID. The node 1 initiates with the secure route discover the process to node 12 by broadcasting to its gateway node 4 as shown in Figure 1 a SRD packet.

$$1 \rightarrow broadcast: [SRD, IP_{12}, \{NID_1, ZID_1, NID_{12}, ZID_{12}\}, cert1, N_1, t]|sign1$$

$$Wheresign1 = [SRD, IP_{12}, \{NID_1, ZID_1, NID_{12}, ZID_{12}\}, cert1, N_1, t]SK_1$$

Here SRD is the secure route discovery packet identifier, N1 is the nonce created by node 1 and t is the current time. The nonce N1 is monotonically augmented always when node 1 accomplishes route discovery, N1 and t combined with the IP address of node 1 exclusively identifies the SRD which inhibits the replay attack.

When a gateway of node 1 attains the SRD, it verifies the (IP, N1, t) to validate that the SRD is not handled. If the packet is found to be trustworthy by verifying the certificate of node 1, then it set up a converse path to the source node 1 by estimating adjacent nodes from which it receives the SRD. The gateway node now signs the information of the message that is initially broadcasted by node 1 and affixes the signature and its individual certificate to SRD. It then verifies in its corresponding Zone LSP and Node LSP Routing Table that it has a legal route to node 12 or not, if path exist then it forwards SRD directly to node 12, otherwise it rebroadcasts the packets to its neighbor Zone gateway nodes.

$$4 \rightarrow broadcast: [[SRD, IP_{12}, \{NID_4, ZID_4, NID_{12}, ZID_{12}\}, cert1, N_1, t]|sign1]|sign4, cert4$$

$$Wheresign4 = [SRD, IP_{12}, \{NID_4, ZID_4, NID_{12}, ZID_{12}\}, cert1,1, t]SK_4$$

Each node along with the route reiterates the stages of authenticating the prior node's signature, storing a former node's IP address for setting up the inverse route, eliminating the prior node's certificate and signature, authorizing the initial information of the message, attaching the individual certificate and re-border casting the message, until the SRD attains a node with an effective path to node 12.

$$10 \rightarrow 12: [[SRD, IP_{12}, \{NID_{10}, ZID_{10}, NID_{12}, ZID_{12}\}, cert1, N_1, t]|sign1]|sign10, cert10$$

$$Wheresign10 = [SRD, IP_{12}, \{NID_{10}, ZID_{10}, NID_{12}, ZID_{12}\}, cert1, N_1, t]SK_{10}$$

Node 12 on receiving this SRD packet authenticates it with both VK10 and VK1, approves its authenticity and excerpts EK1. Node 12 generates a secure route reply (SRR) packet and sends it back to the source along the inverse path.

$$12 \rightarrow 10: [[SRR, IP_1, \{NID_{12}, ZID_{12}, NID_{10}, ZID_{10}\}, cert12, N_1, t, \{K112\}EK1]|sign12]$$

$$Wheresign12 = [SRR, IP_1, \{NID_{12}, ZID_{12}, NID_{10}, ZID_{10}\}, cert1, N_1, t, \{K112\}EK1]SK_{12}$$

Here SRR is the secure rout reply packet identifier. The IP address of node 1, the certificate of node 12, nonce N1, accompanying time stamp t directed by node 1 and a session key K112 amongst the node 1 and node 12 that is encrypted with EK1, attached by the signature sign12 of node 12. Nodes that accept the SRR advances the packet back to the antecedent from which they acknowledged the initial SRD. Every node lengthways to converse path back to the source signs the SRR and attaches its individual credential earlier to advancing the SRR to the subsequent hop.

$$10 \rightarrow 7: [[SRR, IP_1, \{NID_{10}, ZID_{10}, NID_7, ZID_7\}, cert12, N_1, t, \{K112\}EK1]|sign12]sign10, cert10$$

$$Wheresign10 = [[SRR, IP_1, \{NID_{10}, ZID_{10}, NID_7, ZID_7\}, cert1, N_1, t, \{K112\}EK1]SK_{12}]SK_{10}$$

Every node verifies the nonce and signature of the earlier node as the SRR is reverted to the source. This evades outbreaks encompassing impression and rerun of the message. Ultimately, the source 1 receives the SRR. On the accomplishment of SRR, node 1 validates node 12's signature and the nonce resumed by node 12 to adapt its authenticity. It then excerpts the session key K112. Node 1 thus encrypt the data packet by means of K112 and send it to node 12 along the identical path.

Experimental Results

The performance of the proposed Secure Zone Based Hierarchal Link State Routing Protocol (SZHLS) was estimated by means of Network Simulator-2 version 2.16a. NS-2 offers an outline for simulation of wired and wireless systems along with some ability for impersonation. States are executed by serving an oTcl script to the NS-2 executable. The outcome can be obtained directly or post-processed by a

communicating graphics observer called NAM. The simulation of Secure Zone Hierarchal Link State Routing Protocol (S-ZHLS) was directed in Network Simulator-2.35, on an Intel Dual Core processor and 4 GB of RAM running Fedora. The proposed approach is employed over the ZHLS protocol description for NS-2.

The nodes are spatially located in the circular area of 840 units. The communication range of each node in set to 84 units. The complete network is divided in 9, 16, 25 Zones (M) and executed the simulation for Nodes N=100, 200, 300. The preliminary locations of the nodes were arbitrary. Node flexibility was simulated where each node moves to an arbitrarily designated position at an aligned swiftness and then suspends for a mentioned pause time period prior to the selection of alternative arbitrary position that repeat the identical steps. The simulation of the proposed methodology is performed for a constant node speeds of 0, 1, 5 and 10 m/s, with pause time fixed to 30 seconds.

So as to estimate the performance of Secure Zone Hierarchal Link State Routing Protocol (SZHLS), both ZHLS and SZHLS are executed and compared with each other under similar mobility conditions and traffic scenarios. The simplest form of ZHLS was employed that does not have any optimization strategy. This facilitates a reliable assessment of results. Four performance metrics are used to evaluate and to relate the proposed protocol with ZHLS beneath a trustworthy atmosphere where some of the nodes in the system are presumed to be benign or malicious. The performance metrics are namely:

- The Average packet delivery fraction: It is defined as the segmentation of the data packets produced by the CBR sources that are provided to the destination.
- The Average routing load in bytes: It is defined as the ratio of overhead control bytes to distributed data bytes. Secure Zone Hierarchal Link State Routing Protocol (SZHLS) has higher control overhead due to the presence certificate and signature entrenched within the packets.
- The Average routing load in terms of packets: This performance measure is identical to the above, but the ratio of control packet overhead to the data packet overhead is deliberated.
- Average route acquisition latency: This is the average delay amongst the sending of a secure route discovery packet by a source for determining a path to a destination and the acknowledgement of primarily corresponding route response.

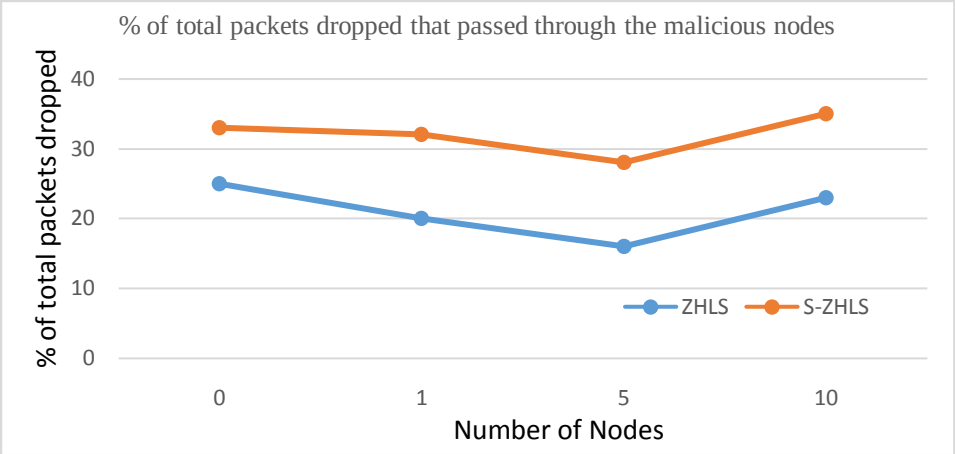

Figure 2: Percentage of total packets dropped that passed through the malicious nodes

Table 1: Percentage of total packets dropped that passed through the malicious nodes

Nodes speed (m/s)	ZHLS	S-ZHLS
0	25	33
1	20	32
5	16	28
10	23	35

As shown in the Figure 2 and Table 1, for the proposed methodology greater section of packets that moved through mischievous nodes were dropped associated to the existing ZHLS. In the existence of 25% mischievous nodes without any node mobility, solitary 23% of packets that move through mischievous nodes are dropped in ZHLS when matched to the proposed SZHLS where 33% of packets that pass through malicious nodes are dropped without any node mobility, solitarily 35% of packets that move through malicious nodes dropped. These outcomes illustrate that nearby 40% of packets that were conceivably changed by malicious nodes stayed hidden and might hypothetically move in the direction of authenticated nodes when employing ZHLS, when compared to the proposed protocol. This is a substantial upsurge in the amount of security level.

Table 2: communication overhead in Network Construction

			N		
			100	200	300
M	9	ZHLS	1605	7775	17057
		S-ZHLS	1462	7417	16732
		% of reduction	8.9%	4.6%	1.9%
	16	ZHLS	1443	7263	16651
		S-ZHLS	1248	6791	16218
		% of reduction	13.5%	6.5%	2.6%
	25	ZHLS	1406	7933	14909
		S-ZHLS	1175	7393	14491
		% of reduction	16.4%	6.8%	2.8%

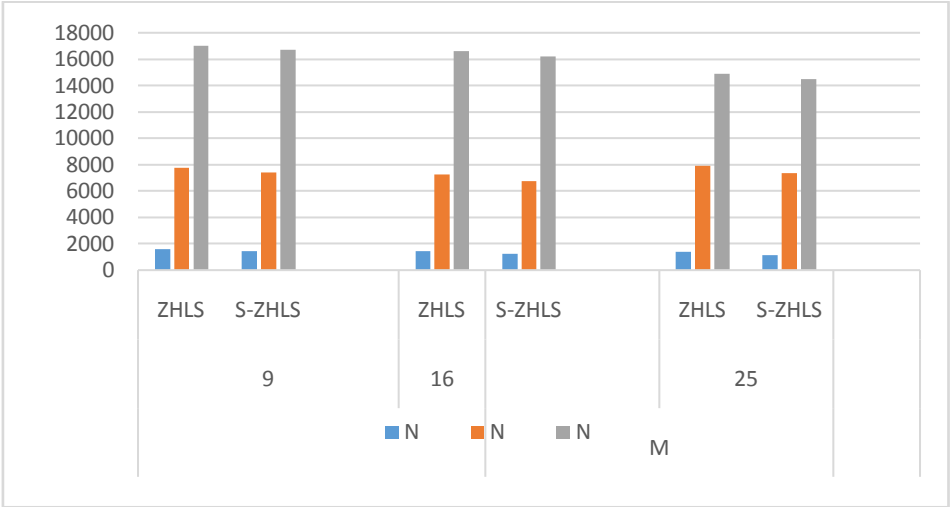

Figure 3: Communication Overheads in the Network Construction

Figure 3 and Table 2 shows that the number of control packets that cause communication overhead in the network topology for the zonal size 9, 16 and 25 respectively. From Table 1, the proposed approach represents the significant percentage of reduction in communication overheads of the Secured ZHLS when compared to Unsecured ZHLS for increasing number of nodes and zonal size. It is also observed that as the as the zone size increases, the significant reduction in communication overheads also increases respectively. Even though, the amount of control bytes communicated by SZHLS is higher compared to that of ZHLS, the amount of control packets communicated between the protocols is coarsely comparable.

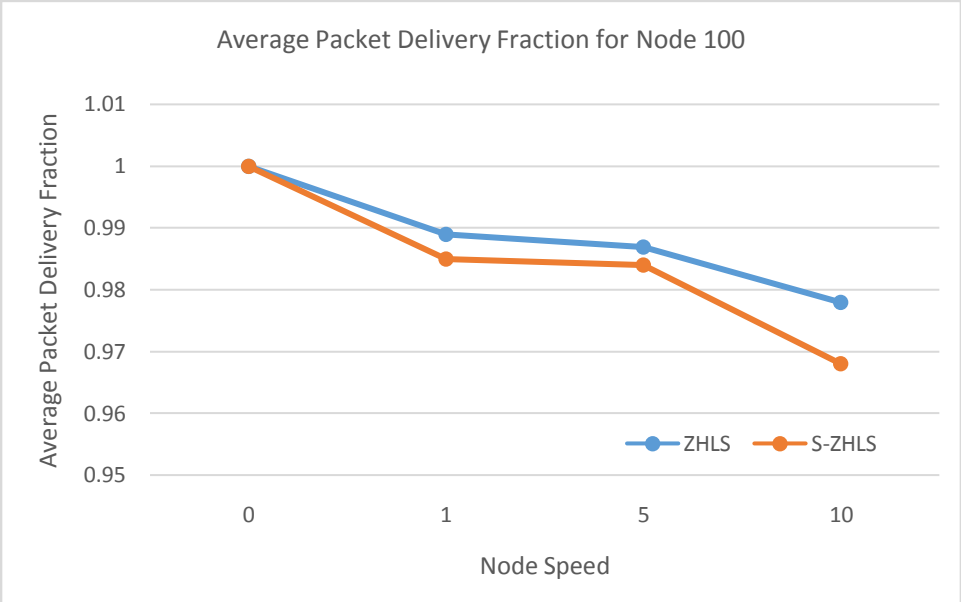

Figure 4: Simulation Results – Average Packet Delivery Fraction

Figure 4 represents that the witnessed outcomes for the average packet delivery fraction for node 100. As represented the packet delivery fraction acquired by means of SZHLS is above 96% in all circumstances and more or less similar to that attained with existing ZHLS. This recommends that SZHLS is extremely operative in determining and sustaining routes for distribution of data packets, in spite of comparatively huge node mobility.

The observed results are analyzed for each of the performance metrics and compared with the existing ZHLS protocol beneath the network and security setup. These metric estimates extent to which the transmission of information is protected and also estimates the fraction of packets that passed through the mischievous nodes that conceivably interrupt secure communication. Thus, proposed Secured ZHLS outperforms when compares to Existing ZHLS routing protocol.

Conclusion

The proposed Secure Zone Based Hierarchical Link State Routing Protocol using Digital Signature provided an approach for secure routing in a managed-open atmosphere. In designing SZHLS, the economical cryptographic primitives are cautiously formfitting to every fragment of the protocol functionality to generate an effective protocol that is vigorous in contrast to numerous outbreaks in the network. The simulation results indicated that the improved protocol achieved a satisfactory compromise between robustness and efficiency in terms of security and global network performances. The proposed methodology provides an improved solution on

the way to accomplish the security objectives like message integrity, data confidentiality and message authentication, by means of an incorporated methodology of digital signature that comprises of both symmetric and asymmetric key encryption techniques. The experimental results showed that average packet delivery fraction, communication overheads in network construction and route acquisition latency are high when compared to the Traditional ZHLS and fraction of packets that passed through mischievous nodes also increased to 40% when compared to the Traditional ZHLS.

References

[1] Mehran Abolhasan, Tadeusz Wysocki and ErykDutkiewicz, "Areview of routing protocols for mobile ad hoc networks", Ad HoccNetworks, Vol. 2, Issue 1, January 2004.

[2] C. Adjih, T. Clausen, P. Jacquet, A. Laouiti, P. Mûhlethaler, and D.Raffo,"Securing the olsr protocol", In Proc. of the 2nd IFIP AnnualMediterranean Ad Hoc Networking Workshop, Mahdia, Tunisia, 25-27June 2003.

[3] E. Atallah, C. Burgod, P.F. Bonnefoi and D. Sauveron, "Mobile Ad HocNetwork with Embedded Secure System", In Proc. Ambient IntelligenceDevelopments Conference, Sophia Antipolis, Springer, France, 20-22September 2006.

[4] S. Buchegger and J. Le Boudec. "Performance analysis of theconfidantprotocol", In MobiHoc, ACM, 2002. pp. 226-236.

[5] M. Guerrero Zapata, N. Asokan, "Securing Ad hoc Routing Protocols",Proceedings of the ACM Workshop on Wireless Security (WiSe 2002), ,September 2002, pp. 1-10.

[6] Y.-C. Hu, D.B. Johnson, A. Perrig, "SEAD: Secure Efficient DistanceVector Routing for Mobile Wireless Ad Hoc Networks", MobileComputing Systems and Applications. Proc. Fourth IEEE Workshop2002, pp. 3 – 13.

[7] T. Clausen and E. Baccelli, "Securing OLSR problem statement",Internet-Draft, draft-clausen-manet-solsr-ps-00.txt, work in progress. 14février 2005.

[8] D.B. Johnson and D. A Maltz, "Dynamic source routing in ad hocwireless networks", In Imielinski and Korth, editors, Mobile Computing,volume 353. Kluwer Academic Publishers, 1996.

[9] P. Papadimitrato and Z. Haas, "Secure Routing for Mobile Ad hocNetwork". Conference SCSCNDS, In Proc. of the SCS CommunicationNetworks and Distributed Systems Modeling and Simulation Conference(CNDS), San Antonio, TX Junuary 27-31, 2002

[10] C.E. Perkins and P. Bhagwat, "Highly dynamic destination-sequenceddistance-vector routing (dsdv) for mobile computers", In Proc.

ACMSIGCOMM' 94 Conference on Communications Architectures,Protocols and Applications, 1994, pp. 234–244.

[11] K. Sanzgiri, B. Dahill, B. Neil Levine, C. Shields, E.M. Belding-Royer"Authenticated routing for ad hoc networks", 10 th IEEE InternationalConference in Network Protocols. ICNP 2002. Paris, France.

[12] S. basagni, M. conti, S. Giordano and I. Stojmenovic, "Mobile Ad Hoc Networking", IEEE press, New York 2004

[13] S. Corson J.Macker, "Mobile Ad hoc Networking (MANET): Routing protocol performance Issues and evaluation consideration"(RFC 2501). http://www.ietf.org/rfc2501.txt

[14] P. Papadimitratos and Z.J. Haas, "Secure Routing for Mobile Ad hoc Networks", In Proc. o/CNDS 2002, San Antonio, TX, USA, 2002.

[15] F. Kargl, A. Geis, S. Schlott, and M. Weber, "Secure Dynamic Source Routing", In Proc. 0/HICSS'05. Hawaii, USA, 2005.

[16] D. Huang, A. Sinha, and D. Medhi, "A key distribution scheme for doubleauthentication in link state routing protocol", In IEEE Performance,Computing, and Communications Conference, pages 19–24, 2005.

[17] D. Huang, A. Sinha, and D. Medhi, "A double authentication schemeto detect impersonation attack in link state routing protocols", In IEEEInternational Conference on Communications, volume 3, pages 1723–1727, 2003.

[18] Bing Wu, Jie Wu, Eduardo Fernandez, Mohammad Ilyas, Spyros Magliveras," Secure and efficient key management in mobile ad hoc networks", Computer Applications 30(2007) 937-954 Elsevier.

[19] ChanghuiHu,Tat Wing Chim,S.M. Yiu,Lucas C.K. Hui, Victor O.K.Li, "Efficient HMAC-based secure communication for VANETs" Computer Networks 56, Elsevier 2012.

[20] Nikos Komnios , Dimitris Vergados, Christos Douligeris, "Detecting unauthorized and compromised nodes in mobile ad hoc networks" ad hoc Networks. 5(Elsevier 2007) 289-298.

[21] Sandeep Thadvai et al "A Novel authenticated encryption scheme with convertibility", Mathematical and Computational Modelling, Elsevier 2012.

[22] Shiva Murthy G.Robert John D'Souza, GollaVaraprasad, "Digital Signature-Based Secure Node Disjoint Multipath Routing Protocol for Wireless Sensor Networks", IEEE sensors Journal vol.12.No.10, October 2012.

[23] M. Joa-Ng and I.-T. Lu, "A peer-to-peer zone-based two-level link state routing for mobile ad hoc networks," IEEE Journal on Selected Areas in Communications,vol. 17, pp. 1415–1425, Aug. 1999.