IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

SHA-ZHLS: Security Enhancement in MANETs using SHA Algorithm

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

Research Scholar, JNTUK, AP & Department of CSE, Vivekananda Group of Institutions, Hyderabad, TS, India[1]

Department of CSE, JNTUH College of Engineering, Jagityal, TS, India[2]

Department of CSE, Vagdevi College of Engineering, Warangal, TS, India[3]

Abstract: Mobile Ad-hoc Network (MANET) is an important field in while many of the users are using mobile devices for last few years where ad-hoc routing in networks is one of the prominent issues. The routing protocol is aimed to offer best route from source to destination in terms of energy efficiency and security. Zone Based Hierarchical Link State Routing Protocol (ZHLS) is one among in hybrid routing protocols for Mobile ad-hoc network, which is not tolerable large number of internal attacks that come from malicious nodes. A malicious node is drops the routing information, data packets intentionally and disturb the process of the routing protocol. To solve this problem, we proposed a novel approach for effective key management, and prevention of malicious nodes. Security to the routing protocol is incorporated with traditional Secure Hashing Algorithm (SHA-256) symmetric and asymmetric key encryption methods. The performance of the proposed algorithm is analyzed and results shown improvement in terms of the packet delivery fraction, communication overheads and percentage of released packets.

Keywords: MANET, ZHLS, SHA-256, Hashing, Communication Overhead.

1. INTRODUCTION

Mobile Ad hoc Network (MANET) is an accumulation of nodes where every node is act as remote correspondence connectors which frame a dynamic system, free to the current system infrastructure. The one of kind elements of MANETs draw a massive consideration in the digital and general society. The past exploration depends on the cordial environment, channel access and multi bounce directing yet now a day's security in nodes with a hostile situation got a decent worry among the client. This article considered the central idea of security issue in MANET in view of the fundamental usefulness in information conveying. The qualities like element topology, impediments in vitality asset, stockpiling gadget and correspondence channel debilitate the examination group to grow more secure framework to keep the client from information misfortune and dependability.

Routing Protocols in MANETs

Every node is acting as like router in MANETs. The limitation on wireless transmission range requires the routing in multiple hops. That is the reason all nodes are inter dependents from source to destination at the time transmission of packets. These kind networking environments places two fundamental requirements on the routing protocols. The first requirement is to be distributed. And the second requirement in network, while the topology changes are frequent, it should compute multiple, routes without loop while keeping the communication overheads to a minimum. MANET routing protocols are categorized into three categories based on route discovery time:

i) Proactive Routing Protocols
ii) Reactive Routing Protocols
iii) Hybrid Routing Protocols

a. Proactive Routing Protocols:

In MANET Proactive (On Demand) Protocols are maintain routing tables according to the network structure. The routing time in these protocols are very minimal because these protocols are maintaining the total network data is at every node. But in MANETs routes are short lived, when mobility between nodes are high stated that the information of routing table invalidate quickly. Large amount of traffic will be generated at the time of evaluating unnecessary routes. Redundant route will be generating, if in large size networks. Also most of the energy is wasting to only generating routing tables in MANETs.

These protocols are suitable when the node mobility is low or speed node data transmission regularly in MANETs. Some of the examples of Proactive MANET Routing Protocols are Destination-Sequenced Distance Vector (DSDV) [9], Topology Broadcast based on Reverse Path Forwarding (TBRPF)[10], Cluster head Gateway Switch Routing Protocol (CGSR)[11], Landmark Routing Protocol(LANMAR)[12], Optimized Link State Routing (OLSR)[13], Fish-eye State Routing (FSR)[14].

b. **Reactive Routing Protocols**:

In MANET Reactive Routing Protocols find the route whenever need to the destination node. The source node broadcast the route requests in the entire network. The data sender wait for reply from destination node or some list routes which consists of intermediate neighbor nodes from source to destination. This is known as global flood search, which influence some significant of time delay before packet data can transmitted. It also needs some significant amount of control traffic.

Therefore, these reactive protocols are suitable for MANETs even the node mobility or speed node data transmission infrequently. Examples of Reactive MANET Protocols are Dynamic Source Routing (DSR) [15], Dynamic MANET On Demand (DYMO) [16], Temporally Ordered Routing Algorithm (TORA) [17], Ad Hoc On-Demand Distance Vector (AODV) [18]

c. Hybrid Routing Protocols:

Reactive and proactive protocols are work at best level in oppositely different conditions, researchers are concentrating to build hybrid routing protocols, which use to combine the concepts of reactive and proactive protocols. These protocols are using to find solutions for reactive and proactive protocols in MANETs. The main idea behind hybrid routing protocols is use reactive routing mechanisms in some areas of network at certain times and proactive for remaining network.

The Reactive MANET routing protocols are used for locating nodes outside the domain, which helps to increase the bandwidth in a constantly changing the network. The proactive routing protocols are confined to a small domain in the network to decrease the expenses and delays. Some of the examples of these protocols are Zone Routing Protocol (ZRP) [19], Core Extraction Distributed Ad Hoc Routing Protocol (CEDAR) [20], and Zone Based Hierarchical Link State Routing Protocol (ZHLS) [21].

In both wired and wireless networks, the security is a very important aspect. Many researchers are working on it and trying to improving the secure data transmissions over the networks. Any network success depends on trustworthy security. Even MANET also strongly depends on security issues to achieve more trusted transmissions over the network.

However, the MANET characteristics pose both opportunities and challenges in achieving the security goals, such as access control, authentication, confidentiality, availability, integrity, and non-repudiation. To combat the vulnerabilities faced during these attacks, Routing Protocols have to meet the following security requirements:

***Authentication*:** Assurance that an entity of concern or the origin of a communication is what it claims to be or from. Without which an attacker would impersonate a node, thus gaining unauthorized access to resource and sensitive information and interfering with operation of other nodes.

***Confidentiality*:** Protection of any information from being exposed to unintended entities. In adhoc networks this is more difficult to achieve because intermediates nodes (that act as routers) receive the packets for other recipients, so they can easily eavesdrop the information being routed.

Availability: Services should be available whenever required. There should be an assurance of survivability despite a Denial of Service (DOS) attack.

***Integrity*:** Message being transmitted is never altered.

***Non-repudiation**:* Ensures that sending and receiving parties can never deny ever sending or receiving the message.

Access control: In general Access control governs the users in operating to access the data. In networking, access control is the formation of groups of nodes. Only authorized nodes may form, destroy, join or leave groups. Access control also mean the way the nodes log into the networking system to be able to communicate with other nodes.

There are various approaches to the access control: like a) Discretionary Access Control (DAC), b) Mandatory Access Control (MAC) .DAC and MAC are often applied together so that DAC allows the system user subjects to control access of other subjects, while MAC controls and restricts the operation of DACs in the system in general. Role Based Access Control (RBAC) a concept where the accesses to objects are defined with respect to roles, not subjects.

In Public networks, cryptography can be used to provide security in routing protocol by accomplishing confidentiality, integrity, authentication, and non-repudiation for communications. Majorly algorithms of cryptographic are classified into the following types:

i) **Symmetric key algorithms:** A single key is used for both encryption ad decryption processes in these algorithms. Triple Data Encryption Standard (3DES) and Advanced Encryption Standard (AES) are some of the examples.

ii) **Public key algorithms**: A pair of keys called is used for encryption and decryption in these algorithms. Digital Signature Algorithm (DSA) and the Rivest-Shamir-Adleman (RSA) algorithm are some of examples.

iii) **Elliptic curve algorithms**: The effort of elliptic curves is established on computing discrete logarithms in the set of points on an elliptic curve distinct over fixed field in these algorithms. Elliptic Curve Diffie Hellman (ECDH), Elliptic Curve Digital Signature Algorithm (ECDSA) and Elliptic Curve Nyberg Rueppe (ECNR) are some of the examples.

iv) **Hash:** Transform original string into shorter fixed length value or key and their most vital property is irreversibility in these algorithms. Irreversibility and collision resistance are necessary attributes for successful hash functions. Examples of hash functions are SHA-1, SHA-256, SHA-384, MD5, HMAC.

In wired networks, we can achieve authentication, integrity and confidentiality in asymmetric cryptography methodology such as public-key cryptography (PKC). In wireless networks, it is too difficult and cost effective.

Asymmetric key cryptography algorithm is slow and needs more CPU processing power and battery power which is not achievable in MANET as nodes have limited memory, battery power and CPU computation power. Because of its low computational and communication overhead symmetric-key approach is chosen in wireless network. Before communication, two communicating ends must share a secret key with each other in symmetric-key approach. Due to the erratic network topology, it is major challenge to distribute the secret keys into the wireless nodes securely and efficiently.

DOI 10.17148/IJARCCE.2016.5214

In this paper, an overview about MANETs and Hybrid Routing Protocols is given in this section. Section 2 gives the brief explanations of the different existing routing protocols that employed the history of SHA techniques and cryptography algorithms for proving security to sending data packets.

A detailed explanation of the proposed secure routing protocol along with applied SHA 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.

2. LITURATURE SURVEY / EXISTING METHODOLOGIES

Security from various threats in Mobile Adhoc Networks (MANET) is a crucial task while transmitting data from source node to destination node. Dynamic nature of the MANETs is the one of the major features, providing security is the most challenging task to researchers. The MANET weakest factor of routing protocol is to understand security threats objective directing protocols. Most of the researchers are attempting to propose more security to MANET protocols. There is no guarantee that a routing protocol cannot provide security to the network in every operation and each situation.

A protocol can provide protection from specific attacks when incorporate suitable procedures. MANETs are having three kind of protocols likely reactive (on-demand), proactive (table-driven) and hybrid routing protocols. Hybrid routing protocols are more popular and the expectations of the users almost reached up to the mark in MANET routing. Addition of procedure to normal routing protocol means that making more powerful to executing the tasks over the network.

John Edward Silva in 2003 presented the work to verify data integrity the hash values of the documents are calculated and kept in a location. Then at a later time, hash value of the document is recomputed. If the hash values do not match one conclude that the file is corrupted [22]. The same technique is used for time stamping the documents.

Kyu et al. in 2002 implemented SHA-1, HAS-160 and MD5 algorithms in a single chip and proposed two architectures one resource sharing and the second non-resource sharing.SHA-1 module is combined with HAS-160 module [23].

McLoone et al. in 2002 implemented SHA-512 and SHA-384. The proposed the solution to achieve throughput [24]. To provide information data integrity and authentication incorporated an hashing algorithm called as keyed-Hash Message Authentication Code – Secure Hashing Algorithm 512 (HMAC-SHA512) [2] to hybrid routing protocol Zone Routing Protocol (ZRP).
Also discussed the various secure hash algorithm properties mentioned in below table 1.

Table 1: Secure Hash Algorithms Properties

Type of SHA Algorithm	Size of message (bits)	Size of Block (bits)	Size of word (bits)	Size of message digest (bits)
SHA-1	<264	512	32	160
SHA-224	<264	512	32	224
SHA-384	<2128	1024	64	384
SHA-512	<2128	1024	64	512
SHA-512/224	<2128	1024	64	224
SHA-512/256	<2128	1024	64	256

SHA HISTORY

In security systems the data integrity is key issue during data transmission. Cryptographic hash function generates message digest to detect unauthorized modifications in messages. This kind of protection requires complex databases and more sensitive binary systems. The tools which are using for cryptographic hash functions are protecting from tamper data by the malicious user in system files.

Hash capacities can likewise be joined with other standard cryptographic techniques to check the source of information. While hashing calculations are joined with encryption, they deliver uncommon message processes that recognize the source of the information; these exceptional digests are called Message Authentication Codes (MAC). Hash Functions of Cryptography have a few extra properties which makes them suitable to use as a way to check the trustworthiness of a message and as a component of advanced mark plans.

A hash function is a function which takes a self-assertive length input and delivers a fixed length of unique string. All the index values maintain into a hash table.

Some hash function properties are increased trustworthiness to network systems; when correctly implemented. The feasibility of using hash function is to validate integrity and information source. Nowadays several hash functions are using in network systems, including Secure Hash Algorithm (SHA), and Message Digest (MD).

A signature S will be generates for a message M by using a secret key k_s, a public key k_p with function Sign(M, k_s). After signature generation, find for valid signature by using Verify(M,S, k_p), which returns a Boolean value if the signature S valid of the message M. The function Sign(M,Sign(M, k_s), k_p) should be true for pair of keys (k_s, k_p). It is highly impossible to create forged signature for hash function signature. Existential forgeries and Universal forgeries are two kinds of possible forgeries are created by attackers. Existential forgeries are creating without influence computed message M. Universal forgeries are creating by the attacker through computing a valid signature S for given message M and public Key k_p.

This kind of signature used in RSA algorithm [1] from the analogue private key and public key crypto system. For generating the signature, the private key (n,d) is used and for verification of the signature public key(n,e) will be

DOI 10.17148/IJARCCE.2016.5214

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

used. Majorly three drawbacks are identified in RSA key system.

First one is RSA key system is infeasible whenever the effective computation required creating the universal forgery.

Second one is RSA handle only signature messages with limited length, straight forward. But bad solution would be split the message in blocks and signature in each block separately. The final drawback is RSA key system is comparatively slow system.

In May 1993, the NIST in relationship with the NSA was developed Secure Hash Calculation (SHA) and firstly circulated as the Safe Hash Standard. The primary amendment to this calculation was distributed in 1995 because of unpublished defect discovered, and was called SHA-1.The principal variant, later named SHA-0, was drawn back by the NSA. The MD4 hash function and SHA hash function having similar both, however adds some unpredictability to the procedure and the block size utilized was changed. In 1998, two researchers from French first discovered a crash on SHA-0 with the complexity 2^{69}, instead of brute force complexity of $2^{80.}$

It took just five years for the introductory SHA capacity to be broken, and after an additional seven years, the most ideal assault is just 50% of the (logarithmic) complexity nature of the first hash function. Coincidentally, the NSA as of now anticipated this in 1995 and discharged SHA-1. Cryptanalysis on SHA-1 turned out to be significantly more troublesome, as the full 80-round algorithm was relaxed just up 2005, and this assault still has a multifaceted nature of 2^{63}. In the theoretical domain only this attack restrict, and the complexity 2^{63} of still not feasible in current generation systems. In any case, this collisional assault requires not exactly the 2^{80} calculations required for brute force attack on SHA-1.

Apart from the SHA-1 hash, the NIST additionally distributed an arrangement of more complex hash functions for which the yield ranges from 224 bit to 512 bit. SHA-224, SHA-256, SHA-384 and SHA-512 (also referred as SHA-2) are more complex hash algorithms due to added non-linear functions to the compression function.

No attacks better than a brute force attack as of January 2008. In any case, subsequent to the configuration still shows noteworthy closeness with the SHA-1 hash functions, it is not impossible that these will be found in the future. As a result of this, an open rivalry for the SHA-3 hash capacity was declared on November 2, 2007. The new standard is retained to be circulated in 2012. Longer hashes yields SHA-2 functions for providing difficult feasibility to attackers.

In our work, first we implemented the Zone Routing Protocol (ZRP), a hybrid MANET protocol is being implemented in Network Simulator 2 (NS2) and hashing algorithm, keyed-Hash Message Authentication Code – Secure Hashing Algorithm 256 (HMAC-SHA256) is implemented for the Authentication and Data Integrity of the information being sent.

3. ZONE-BASED HIERARCHICAL LINK STATE (ZHLS) ROUTING PROTOCOL

The Zone-based Hierarchical Link State (ZHLS) routing is a one of the hybrid routing protocols which creates two routing tables named as inter zone routing table and intra zone routing table[5]. In this routing protocol, to identify of physical address of the mobility nodes over the network a Global Position System (GPS) employed. The entire network divided into number of non-overlying regions based on the location information of nodes in MANETs. ZHLS routing protocol having two kinds of addressing schemes those are Zone ID and node ID. ZHLS routing protocol does not having any cluster heads like other existing hybrid routing protocols in the network. For flexible routing in the dynamic network topology in this routing protocol, the zone ID and node ID of the mobile is sufficient. 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 [3] 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 transmits 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.

SHA-256 Cryptographic Hash Functions

Description of SHA-256: Secure Hash Algorithm (SHA)-256 is a cryptographic Hash Function having 256 bits of digest length. This algorithm is a keyless hash function that means Manipulation Detection Code (MDC).

DOI 10.17148/IJARCCE.2016.5214

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

In this algorithm, a message handled by blocks 16X32=512 size and 64 rounds for each block required.

Basic Operations of SHA-256: The major operations are used in this algorithm is

a) Bitwise Compliment (¯).
b) Boolean Operations are AND(∧), XOR(⊕), OR(∨)
c) Integer Addition Modulo 2^{32} represented as like A + B

Each operator operates on 32-bit of words. Binary words are interpreted as integer values written in base2 in the last operation.

(I) RotR(A,n) denotes the circular right of n bits of A binary word.
(II) ShR(A,n) denotes the right shift of n bits of binary word A.
(III) A|| B denotes the concatenation of the binary words A and B.

SHA-256 Logical Functions:

Total six (06) logical functions are used in SHA-256, and each function operates on 32-bit words, which are represented as X, Y, and Z. The new result of each function is again 32-bit word.

1. $Ch(X,Y,Z)= (X \wedge Y) \oplus (\overline{X} \wedge Z)$
2. $Maj(X,Y,Z)= (X \wedge Y) \oplus (X \wedge Z) \oplus (Y \wedge Z)$
3. $\sum_0^{\{256\}}(X) = RotR(X,2) \oplus RotR(X,13) \oplus RotR(X,22)$
4. $\sum_1^{\{256\}}(X) = RotR(X,6) \oplus RotR(X,11) \oplus RotR(X,25)$
5. $\sigma_0^{\{256\}}(X) = RotR(X,7) \oplus RotR(X,18) \oplus ShR(X,3)$
6. $\sigma_1^{\{256\}}(X) = RotR(X,17) \oplus RotR(X,19) \oplus ShR(X,10)$

Constants of SHA-256 are sequences of sixty-four constant 32-bit words are used in SHA-256 algorithm [6]. The constant words are represent as $K_0^{\{256\}}, K_1^{\{256\}}, \ldots K_{63}^{\{256\}}$. All the words are mentioning the first 32-bits of partial parts of cube roots of the first 64 prime numbers. All the hex constants are mentioned below:

428a2f98	71374491	b5c0fbcf	e9b5dba5	3956c25b	59f111f1	923f82a4
ab1c5ed5	d807aa98	12835b01	243185be	550c7dc3	72be5d74	80deb1fe
9bdc06a7	c19bf174	e49b69c1	efbe4786	0fc19dc6	240ca1cc	2de92c6f
4a7484aa	5cb0a9dc	76f988da	983e5152	a831c66d	b00327c8	bf597fc7
c6e00bf3	d5a79147	06ca6351	14292967	27b70a85	2e1b2138	4d2c6dfc
53380d13	650a7354	766a0abb	81c2c92e	92722c85	a2bfe8a1	a81a664b
c24b8b70	c76c51a3	d192e819	d6990624	f40e3585	106aa070	19a4c116
1e376c08	2748774c	34b0bcb5	391c0cb3	4ed8aa4a	5b9cca4f	682e6ff3
748f82ee	78a5636f	84c87814	78a5636f	90befffa	a4506ceb	bef9a3f7
c67178f2						

SHA-256 Algorithm Flow:

As per [7], SHA-256 algorithms are generates 256-bits of message digest from given input. Based on [6], the input message is lesser than 256-bits and forming 256-bits message digest with 512-bit mandate operation. The SHA-256 algorithm having the following steps[7]:

1. Message Padding:

Before start the hash computation, initially should padded the message M. The main aim of the message padding is to ensure the message length should be in the multiples of 512 bits.

First append "1" bit at the message end zero bits followed by k, where the smallest nonnegative value k, then the summation of l, k and should be 448mod512. After that, append at the end of the message with block contains the size 64-bits ($l<2^{64}$) which is equal to the binary representation number l. Suppose if the message is having multiples of 512 already also should padded.

2. Generating message Blocks by parsing Padded Message:

After the massage padding, the message can be parsed into N 512-bit blocks which are like $M^{(1),(2)},\ldots M^{(N)}$. All these $M^{(i)}$ message blocks are individually parsed to message expander. Each bit block can be divided into 16 words. Each word consists of 32-bits. $M0^{(i)}$, $M1^{(i)},\ldots,M15^{(i)}$ are expanded into 64 words labeled as W0, W1, … W63 as per SHA-2 standard rule.

3. Initial Hash Value Setting $H^{(0)}$:

The SHA compression function is taking Wt words from message expansion stage. SHA algorithm uses mainly 8 working variables labeled A, B,…, H which are initialized to predefined values $H_0^{(0)} – H_7^{(0)}$ before start of each call to hash function.

$A=H_0^{(0)}$	6a09e667
$B=H_1^{(0)}$	bb67ae85
$C=H_2^{(0)}$	3c6ef372
$D=H_3^{(0)}$	a54ff53a
$E=H_4^{(0)}$	510e527f
$F=H_5^{(0)}$	9b05688c
$G=H_6^{(0)}$	1f83d9ab
$H=H_7^{(0)}$	5be0cd19

These working eight variables are updating the value during the 64-cycle iterative computation each block. This SHA-256 compression algorithm then repeats and begins processing another 512-bit block from message padder. Once all data blocks have been processed, final 256-bit output H_N is calculated as follows

$$H(N)=H_0^{(N)}\& H_1^{(N)} \&\ldots\& H_7^{(N)}$$

4. EXPERIMENTAL RESULTS

The performance of the propose Zone Based Hierarchal Link State Routing Protocol (ZHLS) using SHA algorithm was estimated by means of Network Simulator-2 version 2.35. Network simulator is one of the simulation tool where it simulates wired and wireless systems with some facility for impersonation. With the help of oTcl script to NS-2.35 executable, the different states of will be presented. The outcome can be obtained directly or post-processed by a communicating graphics observer called NAM. The simulation specifications are mentioned below table 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

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

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.

SIMULATION SETUP	
PARAMETER	VALUE
Simulation Tool	NS-2.35
Processor	Intel Core2Duo
RAM	4 GB
Number of units	840
Communication Range	84
Network Zone Partitions range(M)	9, 16,25
Constant Node Speeds	0, 1, 5, 10 m/s
Pause Time	30 Secs
Traffic Type	CBR

Table-2: Simulation Setup

So as to estimate the performance of Zone Hierarchal Link State Routing Protocol (SZHLS) using SHA algorithm, both ZHLS and SHA-ZHLS 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.

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.

The Percentage of total packets dropped that passed through the malicious nodes in ZHLS and SHA-ZHLS are shown in figure1.

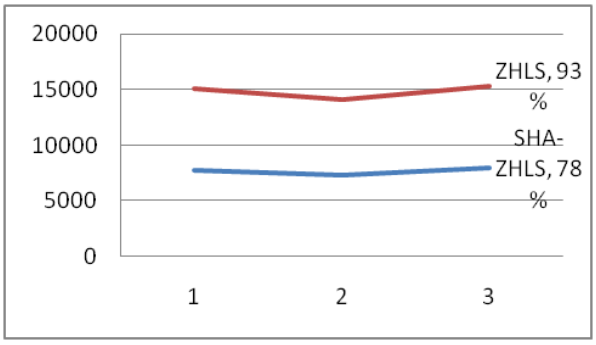

Figure1: Percentage of total packets dropped that passed through the malicious nodes

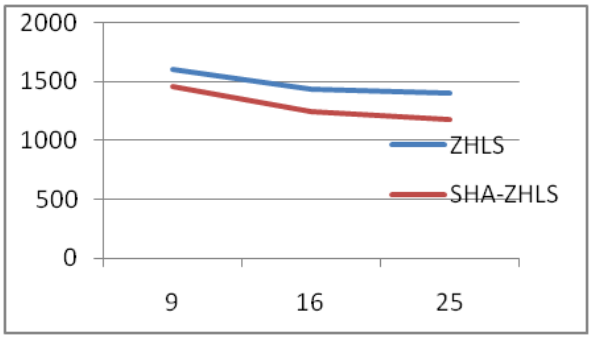

Figure-2: Communication Overhead in network construction for Node 100

Communication overhead of ZHLS and SHA-ZHLS for 100 nodes are shown in the above figure-2. The graph shows that for both schemes the communication overhead maintained smoothly and for SHA-ZHLS it gives the less amount of communication overhead.

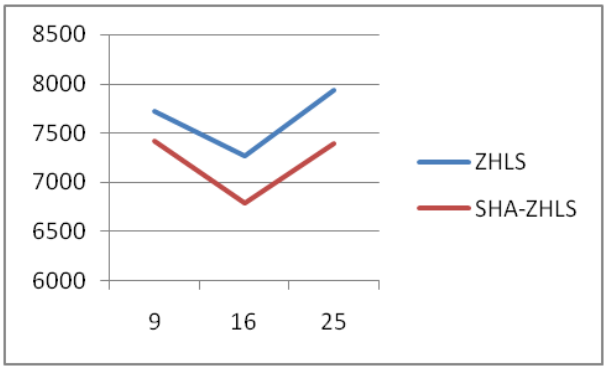

Figure-3: Communication Overhead in network construction for Node 200

The above figure shows that the communication overhead for ZHLS and SHA-ZHLS for 200 nodes. The graph shows that for both schemes the communication overhead maintained smoothly and for SHA-ZHLS it gives the less amount of communication overhead even for 200 nodes.

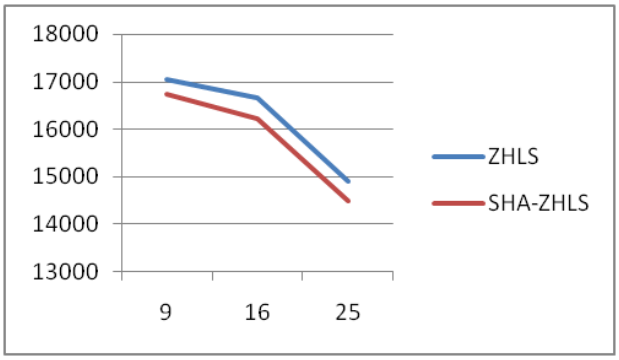

Figure-4: Communication Overhead in network construction for Node 300

The above figure-4 shows that the communication overhead for ZHLS and SHA-ZHLS for 300 nodes. The graph shows that for both schemes the communication overhead maintained smoothly and for SHA-ZHLS using SHA it gives the less amount of communication overhead in terms of packet loss ratio at malicious nodes even for 300 nodes.

DOI 10.17148/IJARCCE.2016.5214

5. CONCLUSION

In the proposed SHA Zone Based Hierarchical Link State Routing Protocol (SHA-ZHLS) proposed a secure routing approach creates healthy environment to user. The cost-effective cryptographic primitives are carefully formfitting to every portion of the protocol functionality to create an effective protocol that is dynamic in distinction to many outbreaks in the network by using this SHA-ZHLS. The simulation results showed that the enhanced protocol attained a reasonable cooperation in efficiency in terms of security and global network performances. The suggested methodology provides an enhanced solution on the way to achieve the security objectives like message authentication, message integrity, and data confidentiality by means of an integrated procedure of hashing. 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.

REFERENCES

1. R L Rivest, A Shamir, and L Adleman, " A Method for obtaining Digital Signatures and public-key cryptosystems" Communication of ACM, Vol. 21, No. 2, 1978, pp. 120-126. doi:10.1145/359340.359342
2. Dilli Ravilla, Chandra Shekar Reddy Putta," Enhancing the Security of MANETs Using Hash Algorithms", Elsevier, Procedia Computer Science 54 (2015) 196 – 206, Eleventh International Multi-Conference on Information Processing-2015 (IMCIP-2015).
3. 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.
4. M V Narayana, Dr.G Narimha and Dr SSVN Sarma, " Secure-ZHLS: Secure Zone Based Hierarchical Link State Routing Protocolusing Digital Signature" International Journal of Applied Engineering Research, ISSN 0973-4562, Volume 10, Number 9 (2015), pp. 22927-22940
5. L. Barolli, A. Koyama, T. Suganuma, N. Shiratori, "GAMAN: A G A Based QoS Routing Method for Mobile Ad-hoc Networks", Journal of Interconnection Networks (JOIN), Vol.4, No.3, pp.251-270, 2003
6. "Federal Information Processing Standards Publication 180-2: Secure Hash Standard," http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf
7. R. V. Mankar, Prof. S. I. Nipanikar, "C Implementation of SHA-256 Algorithm" International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 6, June 2013, page 167-170.
8. Sudhir Agarwal, Sanjeev Jain and Sanjeev Sharma, "A Survey of Routing Attacks and Security Measures in Mobile Ad-hoc Networks", Journal of Computing, Vol.3, Issue1,January,2011.
9. C.E.Perkins and P.Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) For Mobile Computers," Proceedings of ACM SIGCOMM 1994, pp. 233-244, August 1994.
10. R. Ogier, F. Templin, M. Lewis, "Topology Dissemination Based on Reverse-Path Forwarding (TBRPF)", IETF Internet Draft, v.11, October 2003.
11. C.C.Chiang, H.K.Wu, W.Liu and M.Gerla, "Routing in Clustered Multi Hop Mobile Wireless Networks with Fading Channel," Proceedings of IEEE SICON 1997, pp. 197-211, April 1997.
12. M.Gerla, X.Hong, L.Ma and G.Pei, "Landmark Routing Protocol (LANMAR) for Large Scale Ad Hoc Networks", IETF Internet Draft, v.5, November 2002.
13. T.H.Clausen, G.Hansen, L.Christensen, and G.Behrmann, "The Optimized Link State Routing Protocol, Evaluation Through Experiments and Simulation," Proceedings of IEEE Symposium on Wireless Personal Mobile Communications 2001, September 2001.
14. A.Iwata, C.C.Chiang, G.Pei, M.Gerla and T.W.Chen, "Scalable Routing Strategies for Ad Hoc Wireless Networks," IEEE Journal on Selected Areas in Communications, vol. 17, no. 8, pp. 1369-1379, August 1999.
15. D.B.Jhonson and D.A.Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks," Mobile Computing, Kluwer Academic Publishers, vol.353, pp. 153-181, 1996.
16. I. Chakeres and C. Perkins, "Dynamic MANET On-demand (DYMO) Routing Rrotocol", IETF Internet Draft, v.15, November 2008, (Work in Progress).
17. V.D.Park and M.S.Corson, "A Highly Adaptive Distributed Routing Algorithm for Mobile Ad Hoc Networks," Proceedings of IEEE INFOCOM 1997, pp. 1405-1413, April 1997.
18. C.E.Perkins and E.M.Royer, "Ad Hoc On-Demand Distance Vector Routing," Proceedings of IEEE Workshop on Mobile Computing Systems and Applications 1999, pp. 90-100, February 1999.
19. Z.J.Haas, "The Routing Algorithm for the Reconfigurable Wireless Networks," Proceedings of ICUPC 1997, vol. 2,pp. 562-566, October 1997.
20. P.Sinha, R.Sivakumar and V.Bharghavan, "CEDAR: A Core Extraction Distributed Ad Hoc Routing Algorithm," IEEE Journal on Selected Areas in Communications, vol.17, no.8, pp. 1454-1466, August 1999.
21. 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, no. 8, pp. 1415-1425, August 1999.
22. "An Overview of Cryptographic Hash Functions and Their Uses", SANS Institute, 2003.
23. Yong Kyu Kang, Dae Won Kim, Taek Won Kwon, Jun Rim Choi, "An Efficient Implementation of Hash Function Processor for IPSEC", In Proceedings of the IEEE Asia-Pacific Conference on ASIC, pp. 93-96, August. 2002.
24. M. McLoone, J. V. McCanny, "Efficient Single-Chip Implementation of SHA-384 & SHA-512", Proceedings of the IEEE International Conference on Field-Programmable Technology pp. 311-314, 2002.