ZHLS Security Enhancement by integrating SHA256, AES, DH in MANETS

B Barani Sundaram1*, Manish Kumar Mishra2, Dhanabal Thirumoorthy3, Umang Rastogi4, and Balachandra Pattanaik5

1Department of Computer Sciences, Bule Hora University, BuleHora, Ethiopia
2Department of Computer Sciences, University of Gondar, Ethiopia.
3College of Informatics, Bule Hora University, Bule Hora, Ethiopia
4Department of Computer Science and Engineering, Meerut Institute of Engineering and Technology, Meerut, India
5Department of Electronics and Communication Engineering, Bule Hora University, Bule Hora, Ethiopia

Email: bsundar2@gmail.com1*, mishrasoft1@gmail.com2, dhanabalnet@gmail.com3, umang.rastogi@miet.ac.in4, balapk1971@gmail.com5

Abstract. In this century fast growing and progressive change of technology, Mobile Ad hoc Network (MANET) which is a no centralized structure plays great role. The routing protocol in this network is objective to deliver efficient route since sender to receiver. One of the hybrid routing protocols example is Zone Based Hierarchical Link State Routing Protocol (ZHLS) that is can’t allowable huge amount of inside attacks which arise from malevolent nodes. The third party in the routing system may drop the data, as well as disturbs the progression of the routing. To resolve this difficult, ZHLS Security is enhanced by integrating SHA256, AES, DH in MANETS. Security to routing protocols in MANETS is incorporated with different traditional Security mechanisms. My idea behind this thesis is to use integrated security ZHLS protocol by integrating Advanced Encryption Standard (AES) as well as secure hash algorithms to provide the data security. Also, it is, Deffi-Hellman to preserve privacy among the data transmission nodes. In the proposed method, AES is applied to symbol, also authentication to provide the confidentiality of the message in the routing system. This work will be simulated on NS2 environment and it may highly improve the security of data transmission among wireless mobile nodes.

Keywords: SHA256, AES, DH, data communication, AES, Sensor node, MANETS

1. Introduction
MANET MANETS will explain as merely assortment of mobile nodes and transmit the information between nodes through wireless connections. Whereas catching significant features, this depiction does not construct open how MANETs also not permit the measurement of present IP approaches on MANETs. Likewise, the absent of an obvious structural explanation inside the situation of the Internet [1]. Nodes are free to travel randomly; therefore, the topography is normally multi-hop may change erratically at volatile period. Since, the topography is updating continually, it is essential for every pair of adjoining
nodes to integrate in the routing problem to avoid several type of possible attacks which attempt to build utilize of exposures in the routing approach [2].

Several strategies have attained to offer solutions to execute and transmit the data in a well-organized manner. But, the significant troubles during the link failure since the node mobility [3]. Bandwidth restraints, lesser battery energy are the other components which obstruct the competence in the network. Figure 1 shows the link failure among sender and receiver in MANET [3].

In order to have best integrity and confidentiality in securing the wireless network, in this paper, a ZHLS routing protocol by hash function integrated with AES. Through applying these algorithms, we expect high level enhanced security mechanism of the proposed routing protocol [4].

2. Literature Review

In this chapter, we discuss about the overall view of the MANETs routing protocols, challenges and their security solutions according to different surveyors [5].

An attack-resilient adversary node recognition approach is introduced which is capable to notice as well as manage with malevolent attacks [6]. The effectiveness as well as efficiency of the Trust approach is corroborated via widespread experimentations [7]. Heterogeneous remote anonymous verification approach based on L-OOCLS for remote WBAN users to take pleasure in several healthcare services on IoT applications [8]. In this approach, anybody can falsify certificate less verification on any information for any individuality from only publicly recognized information [9].

Lightweight, confidential, as well as denial-of-service-resistant to make sure the information items dispersed are not distorted or fiddled. Depend on several one-way key hash chains, approach offers immediate verification as well as can accept node cooperation [10]. An in-depth security to illustrate that approach is demonstrably safe [11].

Provisioning of Efficient Authentication technique is using Elliptical Curve Cryptography for improving node authentication. This security technique is checking every intermediate hop before data communication in the network [12]. Delay-Efficient Data Scheduling (DEAS) approach creates the collision-free schedule, which diminishes the collection latency. This approach diminishes the sleep delay among nodes, also creating pipelined schedules. However, this approach can’t provide the node reliability [13]. Optimal Capacity-Delay Trade-off strategy significantly concentrates on the collision of the connection of node movement on the capability-delay trade-off in the networks [14]. This method inquired the character of related movement also figured out the primary association among the capability, delay as well as the connected scheme factors that afterwards offer immense assist to derive the capacity-delay trade-off [15].

3. The proposed protocol (ZHLS with integrated security)

In this thesis work, we have proposed security enhancement of ZHLS protocol through the integration of SHA, AES and DH algorithms. In the logic of this protocol, GPS (Global positioning system) will be used to recognize the location of the nodes. The whole network is portioned into amount of regions established on the node positions. This approach contains two types of ID such as Zone ID as well as node ID.

A mobile node defines the zone ID based on its location and priori 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. In Public networks, cryptography can be used to provide security in routing protocol by accomplishing confidentiality, integrity, authentication, and non-repudiation for communications.

The fundamental concept over due this approach is applying digital signature through AES as well as Secure hash (SHA2) techniques. It provide an honesty as well as privacy over the data routed by the protocol as well as Deffi-Hellman method to possess the confidentiality of the sender and receiver of the communication, that can enhances the facilities offered. The security topographies we are joining in our proposed scheme are advanced encryption standard, hashing and Deffi-Hellman algorithms. The Figure 1 demonstrates the flow chart of this approach.
At sender side

Step 1:
1. Seder generates a private key from AES
2. Sender generates public key
3. Sender encrypt the file using AES
4. Sender generate hash code and checks for session key
5. Sender sends encrypted file with session key, private key, hash code to the receiver via ZHLS protocol.

Figure 1: Flow chart for Enhanced ZHLS secured routing
At the receiver side
Step 2:
1. Receive encrypted file and check for session key
2. Receiver generates private key from AES
3. Receiver generates public key
4. Receiver decrypts the file
5. Receiver generates hash code
6. Receiver sends public key to the sender
7. Verify the hash code with the receiver hash
8. code

4. Simulation results
This chapter of the thesis work discusses about the result analysis and implementation of the proposed system with and without integrated security mechanism. The integrated security system is integrated in to the proposed protocol and simulated on the NS2 environment.

Delay: It is the measure of the time taken for a packet to be transmitted from source to destination in the network with respect to correctly received packets.

\[ \text{Delay} = \text{delay of Communication} + \text{delay of propagation} + \text{delay of processing} + \text{delay of Queuing.} \]

Energy efficiency: It is the amount of energy consumed by the overall system performance in packet transmission across the network.

\[ \text{Energy efficiency} = \frac{(\text{Transmission Packet Size} \times \text{Indi Node Strength} \times \text{Node Mobility Range})}{(\text{PackTransSpeed} - (\text{AverageDelay} + \text{ThersholdTimeStamp}))} \]

Data Communication in ZHLS (IARP)
The nodes communicate to each other with in the same zone. During this situation every node nonparallel transmissions linkage request to neighbors reply with node ID as well as zone ID. After receiving entire linkage requests, the node transmits node LSP (link state packet) that contains node Id of its neighbor of the similar zone as well as zone Id of the other zone. Next getting entirely node LSPs of the similar zone, every node recognizes the node equal topography of which zone as well as usage shortest route technique to form its intra-zone routing table. Nodes 1, 2 and 25 are communicating each other with in the same zone. The simulation of data communication in ZHLS is shown in Figure 2.
The delay for secured ZHLS protocol is higher than the normal ZHLS which is computed in percentage in Table 1 the delay at the beginning of the transmission is higher in both cases, and it decreases as number of nodes increase. Once the communication established between source and destination, the delay decreases to some extent because of the familiarity of the communication between sender as well as receiver.

| No. Nodes | 10  | 20  | 30  | 40  |
|-----------|-----|-----|-----|-----|
| Normal ZHLS | 26% | 18% | 12% | 10% |
| Secured ZHLS | 40% | 28% | 24% | 16% |

Figure 2: Data Communication in ZHLS (IARP)

Delay with variable amount of nodes:

The delay for secured ZHLS protocol is higher than the normal ZHLS which is computed in percentage in Table 1 the delay at the beginning of the transmission is higher in both cases, and it decreases as number of nodes increase. Once the communication established between source and destination, the delay decreases to some extent because of the familiarity of the communication between sender as well as receiver.
5. Conclusion

In this approach, we have investigated the security enhancement of the proposed zone Hierarchical routing protocol in MANET. Since ZHLS comprises zone based routing, it provides routing depending on zone id and node id. This system holds two routing mechanisms called inter zone and intra zone routing through IARP and IERP routing approaches. So as to maintain the routing security of the system within the zone and outside the zone which is neighboring zone the proposed scheme uses cryptographic security mechanisms by integrating AES, SHA 256 and Diffi-Hellman in to the proposed protocol.

The result analysis of the simulation ensures that; the security of transmitted packet delivery is ensured through authenticated user between sources to destination. This illustrates that the introduced scheme offers sustainable security mechanism in the ad-hoc network. As we have observed; the enhanced security for ZHLS protocol is more secured than the normal ZHLS routing system and it is the best solution for security problems of the MANETS regardless of its drawbacks those needs further research.
Reference

[1]. Dilli, R., & Reddy, P. C. S. (2016, October). Implementation of security features in MANETs using SHA-3 standard algorithm. In 2016 International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS) (pp. 455-458). IEEE.

[2]. Kumar, M. J. & Baskaran, R (2017), Analyzing a Personalized Network System through NetFlow’, Institute of Integrative Omics and Applied Biotechnology (IIOAB), 7(7), pp. 1-7.

[3]. Rafsanjani, M. K., Asadinia, S., & Pakzad, F. (2010, December). A hybrid routing algorithm based on ant colony and ZHLS routing protocol for MANET. In International Conference on Future Generation Communication and Networking (pp. 112-122). Springer, Berlin, Heidelberg.

[4]. Zain, A., El-Khobby, H. A., Abd Elkader, H. M., & Abdelnaby, M. M. (2015). MANETs performance analysis with dos attack at different routing protocols. International Journal of Engineering & Technology, 4(2), 390.

[5]. Kumar, B. S., Ch, T., Raju, R. S. P., Ratnakar, M., Baba, S. D., & Sudhakar, N. (2013). Intrusion detection system-types and prevention.

[6]. Perkins, C. E., & Royer, E. M. Ad-hoc on-demand distance vector routing. Sun micro system laboratories advanced development group.

[7]. De Paulo, M. A., Nascimento, M. C., & Rosset, V. (2016, October). Improving the Connectivity of Community Detection-based Hierarchical Routing Protocols in Large-scale WSNs. In KES (pp. 521-530).

[8]. Boopathi, G. M., Insozhan, N., & Vinod, S. (2013). Selfish nodes detection using random 2ack in MANET’s. IJESE, 1(4), 3-5.

[9]. Rajeswari, A. R. (2020). A mobile Ad hoc network routing protocols: a comparative study. In Recent Trends in Communication Networks. IntechOpen.

[10]. Nancy, V. (2018). A Security for MANET Interruption Recognition & Preclusion approaches for Network Layer Attacks. International Journal of Applied Engineering Research, 13(12), 10702-10706.

[11]. Kumar, M J & Baskaran, R 2015, ‘Performance Analysis and Comparison of Congestion Control in Wired and Wireless Environment’, International Journal of Control Theory and Applications, vol. 8, no.5, pp. 1743-1757.

[12]. Ahmad, A., & Ismail, S. (2018). User Selective Encryption Method for Securing MANETs. International Journal of Electrical and Computer Engineering (IJECE), 8(5), 3103-3111.

[13]. Ray, I., & Poolsappasit, N. (2008). Using mobile ad hoc networks to acquire digital evidence from remote autonomous agents. International Journal of Security and Networks, 3(2), 80-94.

[14]. Zhang, Y., Liu, W., Lou, W., & Fang, Y. (2006). MASK: anonymous on-demand routing in mobile ad hoc networks. IEEE transactions on wireless communications, 5(9), 2376-2385.

[15]. Thangaraj, S. J. J., & Rengarajan, A. (2016). Unreliable node detection by Elliptical Curve Diffie-Hellman algorithm in MANET. Indian Journal of Science and Technology, 9(19), 1-6.