Security and Privacy Issues in High Level MANET Protocol

Kirti Nahak [1], Babita Kubde[2]

[1]Rungta College of Engineering and Technology
Kohka-Kurud road, Bhilai, India
kirti.nahak@gmail.com

[2]Rungta College of Engineering and Technology
Kohka-Kurud road, Bhilai, India
babita_g7@rediffmail.com

Abstract: ***The High Level MANET Protocol is an application level routing protocol that was designed to support nomad workers performing mobile collaborative activities. Due to various security attacks and third party interference, it is necessary that some methods must be there in the MANET to protect it from such advances. In this project, we are going to enhance the security and privacy of the HLMP based MANET. The basic idea behind the project is to use Advanced Encryption Standard (AES) and Message Digest 5(MD-5) algorithms to secure the data and maintain privacy between the sender and receiver which will improve the services provided by the MANET.***

Keywords: HLMP, MD-5, AES, MANET

1. Introduction

The main purpose followed in the design of High Level MANET Protocol (HLMP) was to establish a set of automated high-level procedures, able to create, keep and use a MANET(Mobile Ad hoc network), which includes routing capabilities. The design of these procedures should consider some key requirements to support mobile collaborative work; e.g. the protocol must be fully distributed and able to run on a wide range of computing devices (from a cellular phone to a laptop) . Mobile devices using the protocol should be able to participate in a network and collaborate on-demand with other devices, by sending messages to any other node inside the mesh. The key concept stems on the periodical delivery of a datagram known as ‘‘I’m Alive’’ message. The MANET following HLMP routing protocol will have a tremendous advantages as compared to other mobile collaborative oriented protocols in the field but, still it has some shortcomings in respect to some aspects such as security, privacy, throughput etc. we are going to solve some privacy issues in the MANET to make more secure and maintain the privacy of the users. It will help in avoiding various issues that can be the reason to larger problems.

The node authentication will secure the MANET from unauthenticated nodes receiving or sending messages from or to the MANET. Authenticating a node will provide a trust relation establishment between the nodes. The hash file generation (MD-5) helps in checking whether the message is genuine or altered one. The overall encryption of message and message hash file using Advanced Encryption Standard (AES) provides the security that no eavesdropping or mishandling will occur and maintains the privacy between the receiver and sender of the particular message.

2. Literature Survey

The MANET is a very vast field and lots of research had been done till now to improve its features and extend its services. It has number of benefits and challenges that have to be tackled to use its services in a rewarding manner. There are number of protocols and algorithms to facilitate MANET.

One such application level routing protocol is the HLMP, which was specifically developed for the mobile collaborative systems. Since, the system works without a fixed network a lot of challenges have to be overcome to maintain the network’s existence and services.

From the past researches on HLMP based MANET, we conclude that this type of work have not been done yet on its security and privacy [3].

3. Previous works

Three research papers [3] [4] [5] have published on the topic of HLMP and HLMP-API, solving various issues regarding mobile collaborative systems. Works have been done to develop the routing protocol that allows mobile workers to collaborate when they are not physically close.

4. Methodology

The methodology that will be followed in the project is shown through two flowcharts:

The first flowchart depicts how a new node is added in the MANET and how the connection is established in the nodes of the MANET.

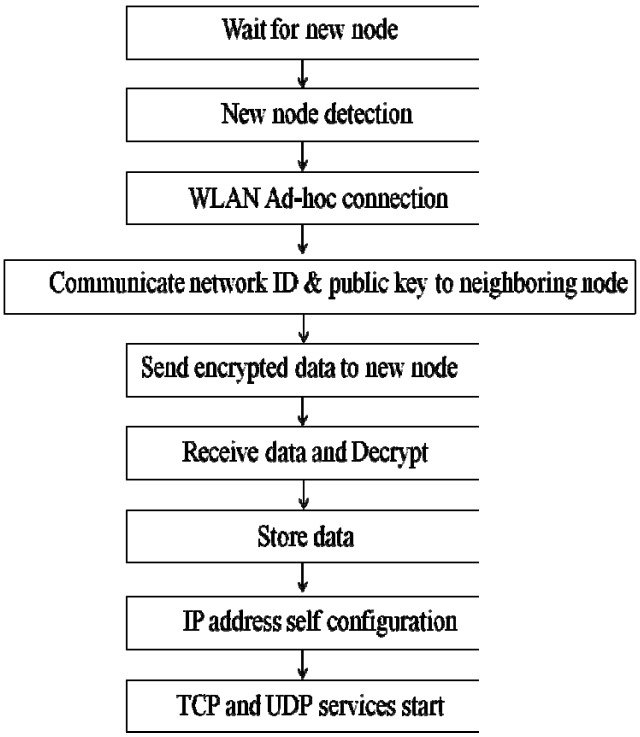

Figure 1: Adding nodes and establishing connection.

The second flowchart shows:

- How a hash file is generated from the message.
- How encryption is done over the data containing both original message and generated hash file.

The receiver's end processing is also shown which includes decryption of the received data and checking of whether the received message is altered or not.

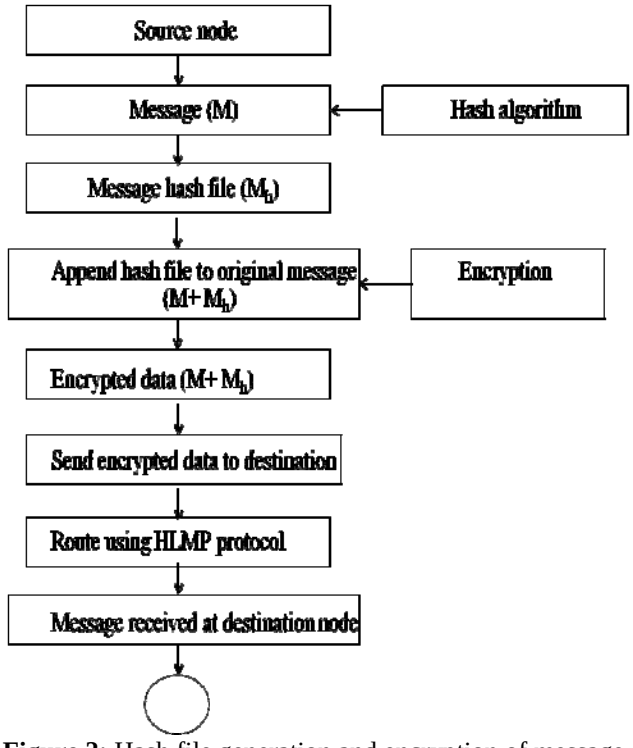

Figure 2: Hash file generation and encryption of message.

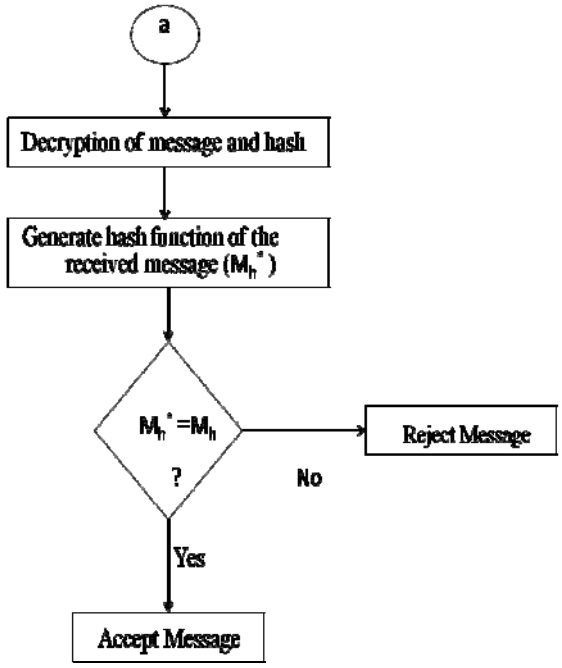

Figure 3: Message decryption and authentication

There are mainly two types of messages sent in a network, multicast messages and unicast messages. The unicast messages are the one that will need more security of encryption to maintain privacy between the two nodes involved in the unicast message transfer.

The algorithm for unicast message in HLMP routing protocol [3] is:

While Ack of M has not been received
{
Path <-minimun path to N;
If there exist a Path
{
Send M to first node in Path;
Wait a Time interval;
}
else
{
Process M as a failed message;
end;
}
}
end

4.1 Addition of a new node and establishment of connection

Whenever a new device wants to access an HLMP MANET, it has to perform a connection procedure. Figure 4 shows the three macro-components of this process: WLAN Ad-Hoc connection, IP address self-configuration, and TCP and UDP services start [3].

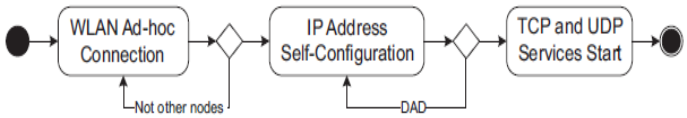

Figure 4: Network connection procedure in HLMP

To the above connection protocol we add an authentication mechanism. On detection of a new node, network ID and group public key is sent to that neighboring node. On receiving the key, node will acknowledge it to the sender, which will then send encrypted network information to the new node and also the information related to the new node is also saved.

4.2 Authentication of the message

The message is appended with hash file generated using MD-5 algorithm as shown in RFC1312 [2]. The hash file is 128 bit message digest of the original message. For a given message, a unique hash function is generated. Thus it is almost impossible to have exactly same hash or message digest for different messages. This provides that the message has not been altered in the network path. Advantage of MD-5 is that it is faster compared to other hash generation algorithm, such as SHA etc.

4.3 Encryption of the message

For encryption purpose we have used Advanced Encryption Standard. After the message is appended with hash file, the new message is passed through the encryption algorithm to generate an encrypted form of the message. This encrypted message is then transmitted to the receiver, where it is decrypted through the decryption algorithm.

The various advantages of using AES are:

- There is no known Brute force attack till now for AES.
- Advanced Encryption Standard not only assures security but also improves the performance.

5. Simulation and Implementation

The complete proposal will be simulated in Network simulator -2 (NS-2), and various performance criterion will be measured regarding security and privacy as well as speed of operation.

6. Expected result

- The nodes in the MANET will be authenticated ones.
- The keys present in the trusted node list will help in the encryption of messages.
- Generation of hash file will help in differentiating genuine message from the altered one.
- The overall encryption will help in maintaining privacy between the nodes involved in the message sending and receiving.
- Using simulation we can find the effectiveness of the methods.

7. Conclusion

When we apply the above discussed methods to the MANET then the message privacy is maintained. The message is kept away from being altered or viewed by the intermediate nodes through message hash file generation and asymmetric encryption. The node authentication leads to having a trusted node list in which we have the public keys and ID of the nodes added up in the MANET, which provides us the benefit of maintaining trust among the nodes.

8. Future Scope

Further work can be done on its current consumption and efficiency management, such that it may be implemented in the smallest devices without much of the power consumption. The algorithm applied in this project solves various issues of the HLMP's security and privacy but not all.

References

[1] Imrich Chlamtac , Marco Conti, Jennifer J.-N. Liu, "Mobile ad-hoc networking: imperatives and challenges", Elseiver.
[2] http://tools.ietf.org/html/rfc1321. (General internet site).
[3] Juan Rodrı guez-Covili, Sergio F. Ochoa, Jose´ A. Pino "High level MANET protocol: Enhancing the communication support for mobile collaborative work" Elseiver, 2012.
[4] Juan Rodríguez-Covili, Sergio F. Ochoa, José A. Pino, "Enhancing Mobile Collaboration with HLMP" in Proceedings of the 2010 14th International Conference on Computer Supported Cooperative Work in Design.
[5] Juan Rodrı´guez-Covili, SergioF.Ochoa, Jose´ A. Pino, Roc Messeguer, Esunly Medina, Dolors Royo, "A communication infrastructure to ease the development of mobile collaborative applications," Journal of Network and Computer Applications 34 (2011) 1883–1893.
[6] James Nechvatal, Computer Security Division, "Report on the Development of the Advanced Encryption Standard (AES)" Publication Date: October 2, 2000.
[7] Alex Biryukov and Orr Dunkelman and Nathan Keller and Dmitry Khovratovich and Adi Shamir , "Cryptology ePrint Archive: Report 2009/374", reference- http://eprint.iacr.org/2009/374.
[8] Daniel J. Bernstein ,"Cache-timing attacks on AES", Department of Mathematics, Statistics, and Computer Science (M/C 249), The University of Illinois at Chicago.

Author Profile

Kirti Nahak: Received the B.E. degree in Computer Science and Technology, from Government Engineering College, Raipur in 2011 and is pursuing M.Tech. in Software Engineering from Rungta College of Engineering and Technology, Bhilai, from 2011. Her current research interest is in the field of MANET security and privacy.