www.ioirp.com
International Journal of Innovative Research in Computer Science and Engineering (IJIRCSE)
ISSN: 2394-6364, Volume – 1, Issue – 6. May 2015

Survey on One Time Password for Adhoc

[1]Karthik HD, [2]Pallavi R
Department of Computer Science and Engineering. Akshya Institute of Technology, Tumkur, India
karthikhd23@gmail.com

***Abstract*— An ad hoc network is the cooperative engagement of a collection of mobile nodes without the required intervention of any centralized access point or existing infrastructure. In this paper, we illustrate an Ad hoc routing protocol, AODV, based on the concept of "One Time Password" and baptized OTP_AODV. OTP_AODV allows nodes authentication through the use of OTP and prevents replay attack as well as non repudiation of exchanged control messages. The integrity of the exchanged data control is handled by the use of electronic signatures.**

Keywords— AODV, OTP, Security

I. INTRODUCTION

One time password generator is an algorithm which generate new random password every time. It works as a machine or algorithm that catches input from users and produce new password that is diverse from previously generated password. Network security deals with authenticate the user with id and password but this method is vulnerable to many attacks so for secure authentication every time new password is used whether the previous password is stolen or misplace. One time password generator is main element of One Time Password system used for generating the generating random passwords additional elements of this system is client authentication and Server authentication. Popular OTP used are HOTP based on SHA-1.Hash algorithms used are MD4, MD5 but these are susceptible to attacks. Another OTP is based on Ping Pong-128 stream cipher in which Ping Pong-128 algorithm is used to generate the random numbers. One time password is secured because:

- It can't used twice or
- It is not reversible to reach at source back.

It mainly deals with the two elements

- Key
- Counter

OTP system generates one password at a time and provides it to client for authentication.OTP send password to client by SMS service, by phone or by written. Password is secure by the application on client mobile.

"Ad Hoc" is actually a Latin phrase that means "for this purpose." It is often used to describe solutions that are developed on-the-fly for a specific purpose. In computer networking, an ad hoc network refers to a network connection established for a single session and does not require a router or a wireless base station.

For example, if you need to transfer a file to your friend's laptop, you might create an ad hoc network between your computer and his laptop to transfer the file. This may be done using an Ethernet crossover cable, or the computers' wireless cards to communicate with each other. If you need to share files with more than one computer, you could set up a mutli-hop ad hoc network, which can transfer data over multiple nodes.

Basically, an ad hoc network is a temporary network connection created for a specific purpose (such as transferring data from one computer to another). If the network is set up for a longer period of time, it is just a plain old local area network (LAN).

II. OVERVIEW OF ADHOC NETWORK

The Ad Hoc Networks is an international and archival journal providing a publication vehicle for complete coverage of all topics of interest to those involved in ad hoc and sensor networking areas. The Ad Hoc Networks considers original, high quality and unpublished contributions addressing all aspects of ad hoc and sensor networks.

Specific areas of interest include, but are not limited to:

- Mobile and Wireless Ad Hoc Networks
- Sensor Networks
- Wireless Local and Personal Area Networks
- Home Networks
- Ad Hoc Networks of Autonomous Intelligent Systems
- Novel Architectures for Ad Hoc and Sensor Networks
- Self-organizing Network Architectures and Protocols
- Transport Layer Protocols
- Routing protocols (unicast, multicast, geocast, etc.)
- Media Access Control Techniques
- Error Control Schemes
- Power-Aware, Low-Power and Energy-Efficient Designs
- Synchronization and Scheduling Issues
- Mobility Management
- Mobility-Tolerant Communication Protocols
- Location Tracking and Location-based Services
- Resource and Information Management
- Security and Fault-Tolerance Issues
- Hardware and Software Platforms, Systems, and Test beds
- Experimental and Prototype Results
- Quality-of-Service Issues

III. ISSUES IN ADHOC NETWORK

In universal, mobile ad hoc networks are formed dynamically by an autonomous system of mobile nodes that are connected via wireless links without using the existing network infrastructure or centralized administration. The nodes are free to move randomly and organize themselves arbitrarily; thus, the networks wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger Internet. Mobile ad hoc networks are infrastructure-less networks since they do not require any fixed infrastructure, such as a base station, for their operation. In general, routes between nodes in an ad hoc network may include multiple hops, and hence it is appropriate to call such networks as ‘‘multi-hop wireless ad hoc networks’’. Each node will be able to communicate directly with any other node that resides within its transmission range. For communicating with nodes that reside beyond this range, the node needs to use intermediate nodes to relay the messages hop by hop.

The ad hoc networks flexibility and convenience do come at a price. Ad hoc wireless networks inherit the traditional problems of wireless communications and wireless networking:

- The wireless medium has neither absolute, nor readily observable boundaries outside of which stations are known to be unable to receive network frames;
- The channel is unprotected from outside signals;
- The wireless medium is significantly less reliable than wired media;
- The channel has time-varying and asymmetric propagation properties;
- Hidden-terminal and exposed-terminal phenomena may occur.

IV. Overview of One Time Password (OTP)

A one-time password (OTP) is a password that is valid for only one login session or transaction. OTPs avoid a number of shortcomings that are associated with traditional (static) passwords. The most important shortcoming that is addressed by OTPs is that, in contrast to static passwords, they are not vulnerable to replay attacks. This means that a potential intruder who manages to record an OTP that was already used to log into a service or to conduct a transaction will not be able to abuse it, since it will be no longer valid. On the downside, OTPs are difficult for human beings to memorize. Therefore they require additional technology to work. How to generate OTP and distribute? OTP generation algorithms typically make use of pseudo randomness or randomness. This is necessary because otherwise it would be easy to predict future OTPs by observing previous ones. Concrete OTP algorithms vary greatly in their details. Various approaches for the generation of OTPs are listed below:

- Based on time-synchronization between the authentication server and the client providing the password (OTPs are valid only for a short period of time)
- Using a mathematical algorithm to generate a new password based on the previous password (OTPs are effectively a chain and must be used in a predefined order).
- Using a mathematical algorithm where the new password is based on a challenge (e.g., a random number chosen by the authentication server or transaction details) and/or a counter.

There are also different ways to make the user aware of the next OTP to use. Some systems use special electronic security tokens that the user carries and that generate OTPs and show them using a small display. Other systems consist of software that runs on the user's mobile phone. Yet other systems generate OTPs on the server-side and send them to the user using an out-of-band channel such as SMS messaging. Finally, in some systems, OTPs are printed on paper that the user is required to carry.

V. Methods of Generating the OTP

A. Time-synchronized: -

A time-synchronized OTP is usually related to a piece of hardware called a security token (e.g., each user is given a personal token that generates a one-time password). Inside the token is an accurate clock that has been synchronized with the clock on the proprietary authentication server. On these OTP systems, time is an important part of the password algorithm, since the generation of new passwords is based on the current time rather than, or in addition to, the previous password or a secret key. This token may be a proprietary device, or a mobile phone or similar mobile device which runs software that is proprietary, freeware, or open-source. An example of time-synchronized OTP standard is TOTP.All of the methods of delivering the OTP below may use time-synchronization instead of algorithms.

VI. AD HOC On-Demand Distance Vector Routing

The Ad-Hoc On-demand Distance Vector (AODV) routing protocol [1] is one of several published routing protocols for mobile ad-hoc networking. Wireless ad-hoc routing protocols such as AODV are currently an area of much research among the networking community. Thus, tools for simulating these protocols are very important. For my project, I have implemented the AODV protocol as part of a scalable wireless ad hoc network simulation (SWANS). SWANS is built upon a novel Java-based simulation framework called JiST.

VII. The Basic Protocol

Each AODV router is essentially a state machine that processes incoming requests from the SWANS network entity. When the network entity needs to send a message to another node, it calls upon AODV to determine the next-hop. Whenever an AODV router receives a request to send a message, it checks its routing table to see if a route exists. Each routing table entry consists of the following fields:

- Destination address
- Next hop address
- Destination sequence number
- Hop count

If a route exists, the router simply forwards the message to the next hop. Otherwise, it saves the message in a message queue, and then it initiates a route request to determine a route. The following flow chart illustrates this process:

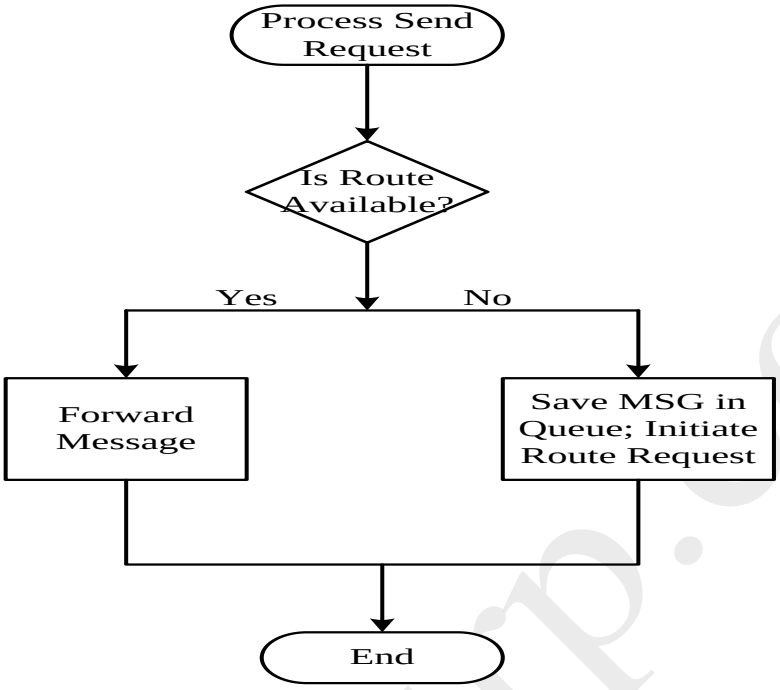

Fig.1: Upon receipt of the routing information, it updates its routing table and sends the queued message(s).

AODV nodes use four types of messages to communicate among each other. Route Request (RREQ) and Route Reply (RREP) messages are used for route discovery. Route Error (RERR) messages and HELLO messages are used for route maintenance. The following sections describe route determination and route maintenance in greater detail.

VIII. AODV Route Discovery

When a node needs to determine a route to a destination node, it floods the network with a Route Request (RREQ) message. The originating node broadcasts a RREQ message to its neighboring nodes, which broadcast the message to their neighbors, and so on. To prevent cycles, each node remembers recently forwarded route requests in a route request buffer (see next section). As these requests spread through the network,

Intermediate nodes store reverse routes back to the originating node. Since an intermediate node could have many reverse routes, it always picks the route with the smallest hop count. When a node receiving the request either knows of a "fresh enough" route to the destination (see section on sequence numbers), or is itself the destination, the node generates a Route Reply (RREP) message, and sends this message along the reverse path back towards the originating node. As the RREP message passes through intermediate nodes, these nodes update their routing tables, so that in the future, messages can be routed though these nodes to the destination.

Notice that it is possible for the RREQ originator to receive a RREP message from more than one node. In this case, the RREQ originator will update its routing table with the most "recent" routing information; that is, it uses the route with the greatest destination sequence number. (See section on sequence numbers).

IX. Prior Study Work

Preeti et al[2]have propose a method to secure AODV protocol. The proposed method uses hashed message authentication algorithm. It does not involve any asymmetric key cryptographic operation and thus provides fast message verification, message authentication and intermediate nodes authentication.

Kimaya et al[3] have described the threats, specifically showing their effects on AODV and DSR. Our protocol, named Authenticated Routing for Ad hoc Networks (ARAN), uses public-key cryptographic mechanisms to defeat all identified attacks

and also detail how ARAN can secure routing in environments where nodes are authorized to participate but untrusted to cooperate, as well as environments where participants do not need to be authorized to participate.

Panagiotis et al[4] have proposed an efficient secure routing protocol for mobile ad hoc networks that guarantees the discovery of correct connectivity information over an unknown network, in the presence of malicious nodes.

Seung et al[5] have been projected to support dynamic scenarios where no wired infrastructure exist. Ad hoc environments introduce two main problems not commonly faced by traditional network routing protocols.

Suresha et al [6] have been is focused on using image processing for securing MANET. And the significance attached to the applications of MANET, security in ad-hoc networks is an important aspect.

Wenjia et al[7] the attempts are to throw light on the work that were focused exclusively for maintaining security in routing protocols in MANET.

Espen Grannes et al[8] have developed a system design for an ad hoc routing protocol combined with access control is proposed, and implemented extending popular routing protocol called BATMAN. The proposed authentication scheme relies on special public key certificates called proxy certificates, and combined with a neighbor trust mechanism both authentication and access control are managed in a secure manner.

Imran et al [9]. have proposed secure routing protocol, CSRP provides security in closed environment where high security is needed and all nodes deployed in the area are from single authority and NASRP provides mainly integrity, non-repudiation and con_dentiality to the communication of the MANET networks.

Rida et al [10]have proposed ASRoP is based on Diffie-Hellman algorithm and SRP authentication protocol that we have exploited to negotiate a secure session using a user password, while eliminating the security concerns often associated with reusable passwords

X. CONCLUSION

One time password is an efficient technique that generate random password each time for users. If user lost their pervious password then there is no need of worry for them because OTP give them new password for each session.OTP prevent user id from replay or eavesdropping attack. Earlier OTP is generated using HMAC , One way hash function and Ping Pong stream cipher , in which input is given to OTP generator as challenge and it generate random password. In our work we propose a overview of adhoc network and also presented method of generating OTP generator using Genetic algorithm with elliptic curve algorithm.

References

[1] Perkins, Charles E., and Elizabeth, M. R.,"Ad-hoc on-demand distance vector routing", In Mobile Computing Systems and Applications, 1999

[2] D.Griffin. “Safer authentication with a one-time password solution”. MSDN magazine. May 2008.

[3] P.Sachan and P.M.Khilar. “Securing AODV Routing Protocoin MANET based on cryptographic authentication mechanism”. International Journal of Network Security & ItsApplications (IJNSA), Vol. 3, No. 5, September 2011.

[4] K.Sanzgiri, B.Dahill, B.N.Levine, C.Shields, E.M.Belding- Royer, D.LaFlamme, “Authenticated Routing for Ad hoc Networks”. IEEE Journal on Selected Areas in Communications, March 2005.

[5] P. Papadimitratos and Z.J. Haas, “Secure Routing for Mobile Ad hoc Networks”. In Proceeding of SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (SCS CNDS), San Antonio, USA, January 2002.

[6] S. Yi, P. Naldurg, R. Kravets, “Security-aware routing protocol for wireless ad hoc networks”. In Proceeding of the 2nd ACM Symposium on Mobile Ad Hoc Networking & Computing (Mobihoc), 2001

[7] Gowda, Sumati Ramakrishna, and P. S. Hiremath. "Review of Security Approaches in Routing Protocol in Mobile Adhoc Network." International Journal of Computer Science Issues (IJCSI) 10, no. 1 (2013).

[8] Graarud, Espen Grannes. "Implementing a Secure Ad Hoc Network." (2011).

[9] Faruk, Imran Hossain. A Novel Approach of Secure Routing Protocol for Mobile Ad Hoc Network. Diss. 2013.

[10] Khatoun, Rida, et al. "ASRoP: Ad hoc Secure Routing Protocol." International Journal of Wireless & Mobile Networks 4.5 (2012).