Analysis of Ad-Hoc Network Security using Zero knowledge Proof and Wi-Fi Protected Access 2

Sivakumar.G
1PG & Research Department of Computer, INDIA

ABSTRACT

Ad-Hoc is a wireless network using radio frequency to connect the neighbor node. Authentication is the main impact of ad-hoc network to secure the network using the Zero Knowledge proof (zkp) and Wi-Fi Protected Access 2 (wpa2) protocols. Zkp is a secure Authentication but the existing node disconnected unfortunately some weak radio coverage, the existing node want to rejoin the neighbor network it takes long time to rejoin. In ZKP use WPA2 protocol to reduce the time duration and quickly rejoin to the neighbor network using ticket and session key. The WPA2 protocol also provide secure authentication.

Keywords— Ad-Hoc Network, Zero Knowledge Proof (ZKP), Wi-Fi protected Access 2 (WPA2), Authentication, Re-Authentication.

I. INTRODUCTION

Ad-hoc wireless networks, however, do not need any infrastructure to work. Each node can communicate directly with other nodes, so no access point controlling medium access is necessary. Figure 1 shows two ad-hoc networks with three nodes each. Nodes within an ad-hoc network can only communicate if they can reach each other physically, i.e., if they are within each other’s radio range or if other nodes can forward the message. Nodes from the two networks shown in Figure 1 cannot, therefore, communicate with each other if they are not within the same radio range. In ad-hoc networks, the complexity of each node is higher because every node has to implement medium access mechanisms, mechanisms to handle hidden or exposed terminal problems, and perhaps priority mechanisms, to provide a certain quality of service. This type of wireless network exhibits the greatest possible flexibility as it is, for example, needed for unexpected meetings, quick replacements of infrastructure or communication scenarios far away from any infrastructure[1].

Figure 1: Two Ad-hoc wireless network

Mobile Ad-hoc Networks is a collection of two or more nodes equipped with wireless communications and networking capability. These nodes can communicate with other nodes that immediately within their radio range or outside their radio range. The Spontaneous Wireless Ad-hoc Networks does not have any gateway, every node can act as the gateway. The notion of a mobile ad hoc network is a network formed without any central administration which consists of mobile nodes that use a wireless interface to send packet data. Since these nodes in a network can act as routers and hosts.

Confidentiality, integrity and authentication are security features wireless ad hoc network, so these are more important for any form of communication be it wired or wireless. Authentication and Confidentiality is more difficult in a spontaneous wireless network, because that doesn’t have a fixed infrastructure. The major problem in ensuring security service in an MANET lies on managing the keys and providing privacy for data communication [2].

Spontaneous wireless ad hoc networks - are created by a set of mobile terminals placed in a close location that communicate with other mobile terminal,
sharing resources, services or computing time during a limited period of time and in a limited space.

Network management should be transparent/visible to the user. A spontaneous wireless ad hoc network is a special case of wireless ad hoc networks. They usually have no dependence on a centralized administration.

![Spontaneous Network Diagram](image)

Figure 2: Spontaneous Network

Well defined, efficient and user-friendly security mechanisms is required for Spontaneous wireless ad hoc networks. Tasks to be performed include: identification of user, their authorization, assignment of address, name service, operation, and safety. Generally, Certificate Authority (CA) is used by wireless ad hoc networks with infrastructure to manage authentication of node and trust [3]. To transfer image require less security but to transfer confidential/secure information require high security therefore encryption and decryption techniques are required to share information.

In wireless ad hoc networks Certificate Authority (CA) is used to authenticate the user and manage the trust. For this Central Authority needs more computing capacity and time. In such networks, for node authorization and user authentication a dependable media is required, it has some failure. Security in spontaneous is based on the users service needs, and to obtain a distributed certification authority it necessary to build trust networks. The network allows users to join into the network. Hence, the new user is trusted by the certification authority. This allows the network to have a DNS and also distribution of network management.

Zero knowledge proof protocol ensures authentication to trust the node. Zero Knowledge Proofs are cryptographic protocols which do not reveal the secret information during the execution of the protocol, the two parties sender and verifier communicate with each other interactively by many transactions, at the end of the execution of the protocol the verifier will be convinced by the prover that the prover knows the secret without revealing the secret itself to the verifier.

If the node release from the network, and ready to rejoin the network by using re-authentication mechanism. The re-authentication mechanism is done to avoid the malicious nodes[4].

The IEEE 802.11i standard also known as Wi-Fi Protected Access 2 (WPA2) is an amendment to the 802.11 standard specifying security mechanisms for wireless networks.

The WPA2 standard has two components, encryption and authentication which are crucial to a secure wireless LAN. The encryption piece of WPA2 mandates the use of AES (Advanced Encryption Standard) but TKIP (Temporal Key Integrity Protocol) is available for backward compatibility with existing WAP hardware.

### II. ZKP

Zero knowledge proof protocol ensures authentication to trust the node. Zero Knowledge Proofs are cryptographic protocols which do not reveal the secret information during the execution of the protocol, the two parties sender and verifier communicate with each other interactively by many transactions, at the end of the execution of the protocol the verifier will be convinced by the prover that the prover knows the secret without revealing the secret itself to the verifier[5].

If the node release from the network and ready to rejoin the network by using re-authentication mechanism. The re-authentication mechanism is done to avoid the malicious nodes.

When a node want to rejoin an existing ad-hoc network it should prove its identity to its neighbor nodes to access the applications and to utilize the resources. This can be achieved by Zero Knowledge Proof (ZKP) Protocol authentication procedure. If this had not been the case, every time a node that wants to rejoin has to prove its identity to the Central Authority (CA). This requires additional network bandwidth in terms of messages communicated between the node and the CA resulting in overhead.

The key advantage in ZKP is that any valuable information will never be revealed during the communication and also reduction in the computational power by reducing the several rounds of interaction between the nodes since it is non interactive nature.
Properties of ZKP protocol:

Completeness: The completeness property states that if the statement is true, the genuine verifier will be convinced of this fact by an genuine prover.

Soundness: The soundness property states that if the statement is false, no cheating prover can convince the genuine verifier that it is true, except with some small probability.

Zero knowledge: The zero-knowledge property states if the statement is true, no cheating verifier learns anything other than this fact. Most ZKP protocols are 3 pass protocols. This means that three messages are transmitted between A and B; commitment, challenge and response. Randomness and timing is a couple of other properties typically associated with ZKP protocol. Randomness in the commitment and challenge are used to hide the secret information. Timing is used to prevent adversary from taking a long time to calculate an answer.

Network Creation: The legitimate node first joined into the network by providing the identity, ip address, name, password to its neighbor node.
Authenticated Server: Authenticated server generates a ticket and session key for each node. And authenticate the node for service sharing using this ticket and session key.

Service Server: Service server provides the service to user after getting verification message from authenticated server.

Server Control: The legitimate user first joined in the network by proving the identity to neighbor node. Then the user sends his details and wait for the TGS (TICKET Granting Session key). If the authenticated server identify the legitimate user it gets all the client details then grants the TG to client. Based on the TGS key the user request service to the service server. Then the service server gets all User details and verified with the Authenticated server. If the verification is done, service server provide valuable services to the trusted user.

III. WPA2

The IEEE 802.11i standard also known as Wi-Fi Protected Access 2 (WPA2) is an amendment to the 802.11 standard specifying security mechanisms for wireless networks[9]. The draft standard was ratified on June 24th, 2004, and replaces the previous security specifications, Wired Equivalent Privacy (WEP), which was shown to have severe security weaknesses. Wi-Fi Protected Access (WPA)[10] had previously been introduced as an intermediate solution to WEP insecurities. WPA implemented only a subset of IEEE 802.11i. WPA2 makes use of a specific mode of the Advanced Encryption Standard (AES) known as the Counter Mode Cipher Block Chaining-Message Authentication Code (CBC-MAC) protocol (CCMP). CCMP provides both data confidentiality (encryption) and data integrity. The use of the Advanced Encryption Standard (AES) is a more secure alternative to the RC4 stream cipher used by WEP and WPA.

The WPA2 standard has two components, encryption and authentication which are crucial to a secure wireless LAN. The encryption piece of WPA2 mandates the use of AES (Advanced Encryption Standard) but TKIP (Temporal Key Integrity Protocol) is available for backward compatibility with existing WAP hardware.

WPA2 Authentication

One of the major changes introduced with the WPA2 standard is the separation of user authentication from the enforcement of message integrity and privacy, thereby providing a more scalable and robust security architecture suitable to home networks or corporate networks with equal prowess. Authentication in the WPA2 Personal mode, which does not require an authentication server, is performed between the client and the AP generating a 256-bit PSK from a plain-text pass phrase (from 8 to 63 characters).

The PSK in conjunction with the Service Set Identifier and SSID length form the mathematical basis for the PMK (Pair-wise Master Key) to be used later in key generation. Authentication in the WPA2 Enterprise mode relies on the IEEE 802.1X authentication standard. The major components are the supplicant (client) joining the network, the authenticator (the AP serves as the authenticator) providing access control and the authentication server (RADIUS) making authorization decisions.

![Figure 5: 802.1X authentication](image)

The Enterprise mode has the following hardware/software implementation requirements:

Selection of EAP types that will be supported on stations, APs (Access Point), and authentication servers. Selection and deployment of authentication servers typically RADIUS (Remote Authentication Dial In User Service) based authentication servers. WPA2 software upgrades for APs and clients.

WPA2 establishes a secure communication context in four phases. In the first phase the parties, AP and the client, will agree on the security policy (authentication method, protocol for unicast traffic, protocol for multicast traffic and pre-authentication method) to use that is supported by the AP and the client. In the second phase (applicable to Enterprise mode only) 802.1X authentication is initiated between the AP and the client using the preferred authentication method to generate an MK (common Master Key).

In the third phase after a successful authentication, temporary keys (each key has limited lifetime) are created and regularly updated; the overall goal of this phase is key generation and exchange. In the fourth phase all the previously generated keys are used by
the CCMP protocol to provide data confidentiality and integrity.

The way how they transmit data is the major difference between wired and wireless networks. To access to the transmitted data is the main difference between wired and wireless networks. Taping the media that is used in network communication is the only possible way in wired networks and in wireless networks communication is done with air media.

The radio frequency can access the transmitted data by the equipment that is available for a cheap price in the market readily. For the development of security needs for the development stages of wireless technology and its security needs, according to the experts the security is the major issue. The traditional wired networks are in herely more secure than wireless networks, the transmissions which take place in air with the right equipment can easily intercept those transmissions which are broadcasted in the air. To secure the wireless networks is not an easy task. There are a number of security issues that make securing a WLAN difficult.

IV. METHODOLOGY USING ZKP AND WPA2

AES stands for “Advanced Encryption Standard.” This was a more secure encryption protocol introduced in Zero knowledge protocol (ZKP) and Wi-Fi Protected Access 2 (WPA2). Secured protocol uses a hybrid symmetric/asymmetric key encryption scheme for user authentication and to exchange data[11]. AES is used to re-authenticate and share the secure services without any infrastructure. Central authority based authentication schemes have been proposed and with every movement of a node outside the network demands re-authentication of the nodes by the central authority before the node rejoins the network. ZKP and WPA2 reduce the dependences on the Central authority for re-authentication thereby avoiding the attacks and reduce the time duration that are possible during re-authentication and service sharing.

ZKP requires each and every time re-authenticate the some un-signal radio coverage of rejoin nodes. The time duration of re-authentication takes long minutes. Hence here re-authentication WPA2 take place to reduce the time duration and securely re-authenticate the neighbor node. The authentication ZKP will take place to configure the session key and IP address of the nodes and generate the authentication (here authentication is user name and password) of the node. In re-authentication WPA2 will take place analysis the session key and IP address if the session key and IP address match it will automatically rejoins the network. If the Session key and IP address will not match the link move to ZKP authentication then the username and password will not match the attacker node will be disconnected.

![Figure 6: Overall System Architecture](image)

System Design:

The user first joined in the network by proving the identity to neighbor node. Authenticated server gets all details about the client and grants the ticket and session key to client. Using ticket and session key the user request the service to Service server. Service server gets the user details and verify with the Authenticated server. If the verification is done, service server provide valuable services to trusted user. If existing user wants to rejoin the network, WPA2 protocol first re-authenticate the existing user, if the ticket and session key match it will automatically rejoin network without validation. WPA2 protocol reduces time for rejoin the existing node, if the nodes match ticket and session key. In ZKP each and every time, if the ticket and session key match also first verify all the process of ZKP. That is the network by proving the identity to neighbor node. Authenticated server gets all details about the client and grants the ticket and session key to client. Using ticket and session key the user request the service to Service server. Service server gets the user details and verify with the Authenticated server. If the verification is done, service server provide valuable services to trusted user.

V. CONCLUSION

The Zero Knowledge Proof protocol and Wi-Fi Protected Access 2 protocol allows the creation and management of a spontaneous wireless ad hoc network. Secure protocols (ZKP and WPA2) are used to share the secure service. The previous ticket and session key match with WPA2. WPA2 allow to access existing user without any re-authentication, it helps to reduce time for rejoin node. If the existing user doesn’t match ticket and session key ZKP take place for re-authentication. Some procedures are provided for re-authentication and sharing the service: a unique IP address is assigned to each device, ticket and session key is generated for each user. A user without advanced technical knowledge can set up and participate in
a spontaneous network. The security schemes included in the protocol allow secure communication between end users. It consume less energy, power and time during protocol execution.

REFERENCES