ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Enhancing Security in Wireless Ad-Hoc Network Using ZKP

M.Soniya[1], P.Sabarinathan[2], S.Visnudharsini[3]

PG scholar, Pavendar Bharathidasan College of Engg and Tech, Tiruchirappalli, Tamilnadu, India[1]

Research scholar, Pavendar Bharathidasan College of Engg and Tech, Tiruchirappalli, Tamilnadu, India[2, 3]

Abstract: Communication in network is based on client server model where an infrastructure is required between two clients or mobile to communicate with each other even though they are closed to each other. In earlier human communication model, two people those are physically closed to each other can talk directly without any server. In spontaneous network there is no server or any infrastructure between nodes to communicate, anybody those who wants to communicate can join, communicate and leave the network without any central server. Authentication in Wireless ad-hoc Network is difficult and challenging because of its frequent topology changes. Due to the mobility of nodes the connection may be loss. When the connectionless node wants to rejoin into the network node re-authentication will be needed. A secure self configured protocol is required for user authentication, validation and data transfer. Zero knowledge protocol is a secure self-authenticated protocol. Secured protocol uses a hybrid symmetric/asymmetric key encryption scheme for user authentication and to exchange data. ZKP 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 reduces the dependences on the Central authority for re-authentication thereby avoiding the attacks that are possible during re-authentication and service sharing.

Keywords: Zero Knowledge Proof (ZKP), Authentication, Re-Authentication, Wireless Ad-hoc network, Spontaneous Network, Central Authority

I. INTRODUCTION

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 [18].

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.

Important features in spontaneous networks [14] are mentioned below:-

1. Network boundaries are poorly defined.
2. The network is not planned.
3. Hosts are not preconfigured.
4. There are not any central servers.
5. Users are not experts.

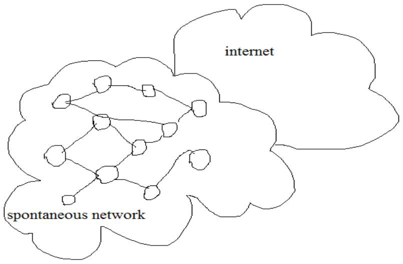

Figure 1. Network Model

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 [20].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.

II. THE PROBLEM

In spontaneous wireless ad hoc network security should be based on the required confidentiality, integrity, node cooperation, anonymity, and privacy. Exchanging pictures between users requires less security than exchanging confidential information between managers. Furthermore, all nodes in network may not be able to execute routing protocol and security protocols. Dynamic networks with group signatures, flexible memberships and distributed signatures are difficult to manage [13]. In mobile ad hoc networks key exchange mechanisms are needed to achieve a reliable communication, node authorization and user authentication.

Cryptographic hybrid key management methods for secure routing in MANET are not enough for spontaneous wireless ad hoc networks because they need an initial configuration (network configuration) or external authorities (central certification authorities) [17]. Symmetric and asymmetric key algorithm [12] does not propose a secure spontaneous network protocol. MANETs need secure routing protocols to prevent the security attacks like MIME, Reply, and clone attack. There exist more secure routing protocols, such as AODV, DSR, DSDV, OLSR etc, but these protocols are either too expensive or have unrealistic requirements. These routing protocol consume more resources, and delay.

MOTIVATION:

The secure protocol (Zero knowledge proof) that create the network by adding nodes for sharing secure service without data losses. ZKP perform the re-authentication for avoiding malicious nodes in the network.

III. CONTRIBUTION

The proposed protocol in this paper can establish a secure self-configured environment for resources and services sharing and data distribution and among users [15]. Based on the service required by the users security is established. A user is can able to join the network because user knows someone that belongs to it. Thus, the certification authority is distributed between the users that trust the new user and existing user while rejoin into the network.

In this paper we use ZKP for re-authentication, asymmetric cryptography, where each device has a public-private key pair for device identification and symmetric cryptography to exchange session keys between nodes. There are no anonymous users, because confidentiality and validity are based on user identification.

ZERO KNOWLEDGE PROOF PROTOCOL

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.

Let us consider an ad-hoc network with n number of nodes, if a new node x wants to rejoin the network, it gets authenticated by the
closest/neighbor nodes B andC , making node x is a valid node. Once node x have been authenticated it starts its communication among the nodes in the ad-hoc network.

Step 1: New node x private keys are s1 = 3 and s2 =7. It chooses 2 random numbers m1 and m2, such that m1 = 5 > s1 and m2 = 9 > s2. Then node x sends m1 to node B and m2 to node C respectively.

Step 2 : The nodes B and C chooses 2 large prime numbers p1 = 2, q1= 3 and p2 = 3, q2 = 5, then calculates n1 = p1 * q1 = 6 and n2 = p2 * q2 = 15. Node B sends n1 to x and node C sends n2 to x .

Step 3: The new node x computes v1 and v2 such that, v_1= s_1^2mod $n_{1.}$ v_2 =s_2^2 mod n_2=15 respectively, Now the 2 public keys of the node x are (v1, n1) = (3, 6) and (v2,n2) =(4,15) .

Step 4: The node x chooses two random numbers r1 = 4 and r2 = 3 and computes x_1= r_1^2mod n1=4: x_2= r_2^2 mod n2=9. Now x sends x1 to B and x2 toC .

Step 5: The nodes B and C chooses the challenge values e1 = 0, e2 = 1, then node B sends e1 to x and node C sends e2 to x .

Step 6: The new node x sends the random number r1 = 4 to node B . Then node B verifies that r_1^2= x_1 mod n1=4 Likewise node x calculates y_2 = $r_2 s_2$ mod n_2=6 and sends to the node C . Then node C verifies that y_2^2= $x_2 v_2$ mod n_2= 6

Once the verification of the node x has been done by the nodes B and C node x allowed to communicate with the other nodes in the network.

IV. SYSTEM DESIGN

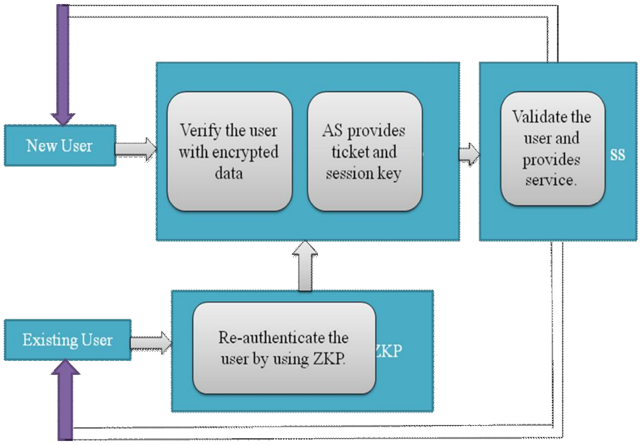
New User
Verify the user with encrypted data
AS provides ticket and session key
Validate the user and provides service.
SS
Existing User
Re-authenticate the user by using ZKP.
ZKP

Figure 2. Overall System Architecture

In proposed model, the legitimate 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, ZKP protocol re-authenticate the existing user then rejoin the node to network.

V. SYSTEM IMPLEMENTATION

Authentication

Authentication process is always occurred prior to mobility management process included location registrations and service delivery, and it also ensures network resources are accessed by authorized clients and prevents resources from any illegal client or damage. Therefore authentication is the first concern in MANET. Authentication process is occurred periodically and frequently, when service access expires, when temporary connection services interrupt, or as a result of handover. Entire authentication procedure from the beginning to the end is called as authentication session.

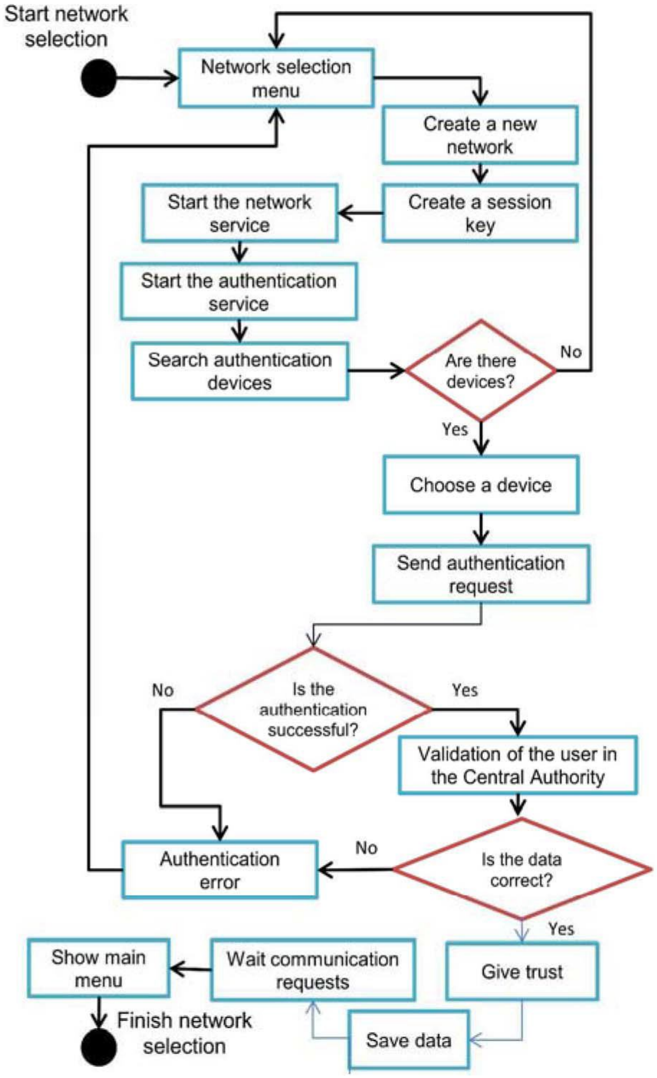

Figure 3. Network Creation

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 TGS 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.

Re-Authentication

Re-authentication happens when an authenticated node wants to rejoin the network after it has lost its connectivity due to mobility.

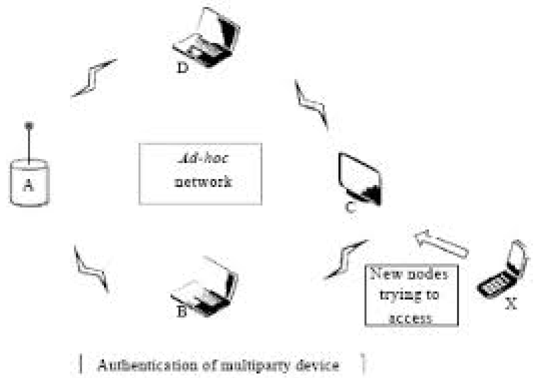
D
A
Ad-hoc network
C
New nodes trying to access
X
B
Authentication of multiparty device

Figure 4.Re-authentication

This mechanism is used mainly to avoid the malicious nodes to enter into the network.

VII.CONCLUSION

The Zero Knowledge Proof protocol allows the creation and management of a spontaneous wireless ad hoc network. Secure protocol (ZKP) is used to share the secure services and re-authentication. Re-authentication scheme proposed for MANETs without the necessity of CA using ZKP which do not reveal any useful information during the protocol execution. 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

[1] Arunkumar R. (December 2012) "Secured Certificate through zkp protocol in wireless ad hoc networks" Volume 1, Issue 10.

[2] Cornelius C., Kapadia A., Kotz D., Peebles D., Shin M. and Triandopoulos N. (June 2008) "Anonysense: Privacy-Aware People-Centric Sensing," Proc. Sixth Int'l Conf. Mobile Systems, Applications, and Services (MobiSys '08), pp. 17-20.

[3] Czerwinski S.E., Zhao B.Y., Hodes T.D., Joseph A.D. and Katz R.H. (Aug. 1999) "An Architecture for a Secure Service Discovery Service," Proc. ACM/IEEE MobiCom '99.

[4] Danzeisen M., Braun T., Winiker S. and Rodellar D. (Mar.2005) "Implementation of a Cellular Framework for Spontaneous Network Establishment," Proc. IEEE Wireless Comm. and Networking Conf. (WCNC '05).

[5] Feeney L.M., Ahlgren B., and Westerlund A., "SpontaneousNetworking: An Application-Oriented Approach to Ad-hocNetworking," IEEE Comm.Magazine, vol. 39, no. 6, pp. 176-181, June 2001.

[6] Herrero L., and Lacuesta R., "A Security Architecture Proposal for Spontaneous Networks," Proc. Int'l Conf. Advances in the Internet Processing System and Interdisciplinary Research, Oct. 2003.

[7] Lacuesta R., Lloret J., Garcia M., and Pen alver L., "A Spontaneous Ad-Hoc Network to Share WWW Access," EURASIP J. Wireless Comm. and Networking, vol. 2010, article 18, 2010.

[8] Laura Marie Feeney, Bengt Ahlgren, Assar Westerlund, Swedish Institute of Computer Science Spontaneous Networking:An Application-Oriented Approach toAd Hoc Networking.

[9] Liu L., Xu J., Antonopoulos N., Li J. and Wu K. (2012) "Adaptive Service Discovery on Service-Oriented and Spontaneous Sensor Systems," Ad Hoc and Sensor Wireless Networks, vol. 14, nos. 1/2, pp. 107-132,

[10] Manish P. and Gang wane. (August 2012) "Implementation Of Zero Knowledge Protocol In Wireless Sensor Network for Identification Of Various Attacks" Volume 2, Issue 8.

[11] Mayrhofer R., Ortner F., Ferscha A. and Hechinger M. (Aug. 2003) "Securing Passive Objects in Mobile Ad-Hoc Peer-to-Peer Networks" Electronic Notes in Theoretical Computer Science, vol. 85, no. 3, pp. 105-121,

[12] M. Mukesh and K.R. Rishi, "Security Aspects in Mobile Ad Hoc Network (MANETs): Technical Review," Int'l J. Computer Applications, vol. 12, no. 2, pp. 37-43, Dec. 2010.

[13] A. Noack and S. Spitz, "Dynamic Threshold Cryptosystemwithout Group Manager," Network Protocols and Algorithms,vol. 1, no. 1, Oct. 2009.

[14] Payal A.Pawade ., Gaikwad V.T(May 2013) "Authenticating Protocol for Spontaneous Wireless Ad Hoc Networks" vol. 2,issue 5.

[15] Raquel Lacuesta. and Jaime Lloret. (2013) "A Secure Protocol for Spontaneous Wireless Ad Hoc Network creation" vol. 24, no. 4, l.

[16] Rekimoto J. (May 2004) "SyncTap: Synchronous User Operation for Spontaneous Network Connection," Personal and Ubiquitous Computing, vol. 8, no. 2, pp. 126-134.

[17] Sahadevaiah K. and Prasad Reddy P.V.G.D. (2011) "Impact of Security Attacks on a New Security Protocol for Mobile Ad Hoc Networks," Network Protocols and Algorithms, vol 3, no. 4, pp. 122-140.

[18] S.Samundeeswari, V.S.Shankar Sriram "NIZKP to achieve Authentication in Ad-Hoc Networks".

[19] Smita Karve., D.N.Rewadkar Smita Karve (November 2013)" Spontaneous Wireless Ad Hoc Networking: A Review" Volume 3, Issue 11.

[20] Xiao Y. Rayi V.K., Sun B., Du X., Hu F. and Galloway M. (Sept. 2007)"A Survey of Key Management Schemes in Wireless Sensor Networks," Computer Comm., vol. 30, nos. 11/12, pp. 2314-2341.