Escalating Security and performance in Wireless Ad-Hoc Network

Soniya .M, Sangeetha .T, Girija .K, Sabarinathan .P

Abstract— **In Wireless ad-hoc Network Authentication is difficult and challenging because of its frequent topology changes. Owing to the moving of nodes the connection will be loss. Re-authentication is more important when the connectionless node wants to rejoin into the network. This paper proposes a secure self configured protocol is required for user re-authentication, reducing the authentication time and service sharing. Zero knowledge protocol is a secure self-authenticated protocol used for re-authenticate the node. Expedite Message Authentication Protocol can significantly decrease the time for re-authentication and increase the performance. Secured protocol uses a hybrid symmetric/asymmetric key encryption scheme for user authentication and to exchange data. Zero Knowledge Protocol is used to re-authenticate of nodes and secure service sharing without any infrastructure. In existing system 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 rejoin the network. Zero Knowledge Protocol reduces the dependences on the Central authority for re-authentication thereby avoiding the attacks that are possible during re-authentication and service sharing.**

Index Terms— Zero Knowledge Proof (ZKP), Authentication, Re-Authentication, Wireless Ad-hoc network, Spontaneous Network, Central Authority, Expedite Message Authentication Protocol (*EMAP*), Authentication delay.

I INTRODUCTION

"Ad Hoc" is actually a Latin phrase that means "for this purpose."Rather than infrastructure wireless network each node directly share the information with an access point or base station, a mobile ad hoc network, or MANET is a type of wireless ad hoc network [1]. Wireless ad-hoc network is a self-configured network. Each and Every node in wireless ad-hoc network is autonomous. The nodes are free to move arbitrarily and organize themselves Haphazardly. In MANET, breaking of communication link is very habitually, as nodes are free to move to anywhere. Due to the topology changes of network and breaking of paths authentication is more difficult in wireless ad hoc network. Spontaneous ad hoc network is a special kind of Mobile Ad hoc network (MANET). A crucial problem in mobile ad hoc networks is the management and distribution of information. Solution to these problems is Spontaneous ad hoc network.

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

Spontaneous network is Special case of ad hoc network. These types of networks usually have maverick and distributed centralized administration.

The Important characteristics of spontaneous networks are mentioned below:-

1. Network boundaries are badly explained.
2. The network is not planning.
3. There is no pre-configuration.
4. There are no central servers.
5. There are no experts.

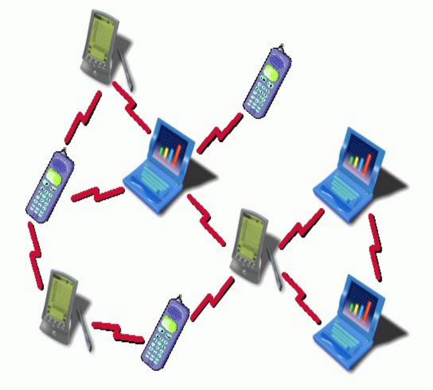


Fig 1.Spontaneous Wireless Ad-Hoc Network

The main goal of spontaneous network is combination of service and devices at one place allowing user to have rapid service without external infrastructure. These networks are executed in mobile, Personal Digital Assistants, laptops, with finite memory space and limited energy.

In wireless ad-hoc network Security is based on node coordination, authentication, confidentiality, anonymity, and privacy also. Transference of photo require less security compared with transference of confidential information. Therefore encryption and decryption techniques are required to share information. In ad hoc networks Certificate Authority (CA) is used to authenticate the node and manage the trust. For this, CA requires high computing and time capacity and it also has to be online always.

Securing a mobile ad hoc network (MANET) is a big challenge because of the nature of the MANET. A certain demanding problem is how to detect and defend attacks on routing protocols practically. Security in wireless ad-hoc networks is hard to attain, mainly because of the vulnerability of wireless links, the finite physical protection of nodes, the dynamically changing topology, the lack of a certification authority, and the absence of a centralized monitoring or management point.

Security of mobile ad hoc networks (MANET) has become a more sophisticated problem than security in other networks, due to the open nature and the lack of infrastructure of such networks.

II RELATED WORK

Jangseong Kim proposed a protocol for re-authentication which is incredibly efficient and scalable for wireless sensor network. This Protocol is based on the membership verification and disclose its performance analysis and security analysis. The protocol has high computational costs.

Shen- Ho Lin proposed Fast Iterative localized Re-authentication, (FIL) protocol which basically overcomes the current issues , delay and speed up the process.

Fanyang proposed a protocol called EAP_AKAY and self adaptive K selection mechanism for load balancing re-authentication in major network schemes. Both client and server end authentication cost is reduced up by this mechanism. It conquer the drawbacks of existing scheme and minimize the total cost. This system is more effective in terms of excellent security and authentication cost.

Guangsong Li proposed a re-authentication system based on ticket for the period of fast handover. Guangsong mainly discourse on re-authentication problem while handover in Wireless Local Area Network. Authentication server send a handover tickets to the mobile station as an evidence of authorization and it produces the equivalent tickets when connecting with a new access point. In proposed system re-authentication delay is reduced and network performance is increased. Compared to all other proactive key pre-distribution systems this systems inflict less trouble over the entities.

III THE PROBLEM

In MANET, due to its moving of node can join or leave the network in a dynamically. So it becomes very arduous to manage the user access as well as hard to define encryption technology. Each and every node in this type of ad-hoc network can be abused easily by sluggish eavesdropping or active intervention. So each node should be able to confront the attacker in any form. There are various methods are available for secure authentication and cipher key management to overcome this vulnerability. The Identity based technology furnish authentication without preliminary information or any public key means that, it gives authentication without information sharing. It avoids third party to affect like the authorized user or re-using the authentication ID. The following authentications are necessary for ad-hoc network.

1. Node Authentication
2. Confidentiality and Integrity

Most of the popular authentication protocols in MANET are based on Authentication management architecture developed on RSA signature Using Trusted Third Party (TTP) based authentication chain of trust based identification scheme. One of most important characteristics of the ad-hoc network is group based applications, for these applications the conventional identification techniques not suitable. Fulfilling these requirements Zero Knowledge Proofs (ZKPs) is implemented, which provides a graceful solution to the problem of self-organized node authentication in MANETs. The problem of re-authentication when a node moves out of a network and wants to rejoin the same network is not addressed by these existing mechanisms.

Motivation: The secure protocol (Zero knowledge proof and Expedite message authentication protocol) that create the network by adding nodes for sharing secure service without data losses and decrease the authentication delay. ZKP perform the re-authentication for avoiding malicious nodes in the network. And reduce the authentication delay using Expedite message authentication protocol.

IV CONTRIBUTION

The proposed protocol in this paper can establish a secure self-configured environment for resources and services sharing and data distribution among users [15] and reducing authentication delay. A node can able to join into network because node knows someone that belongs to it[18]. Thus, the certification authority (CA) is distributed between the nodes that trust the new node and existing node while rejoin into the network. In this paper we use ZKP for re-authentication, EMAP for reducing delay.

Expedite Message Authentication Protocol

EMAP protocol is used for reducing authentication delay. The message authentication is done by three phases: checking the sender's revocation status, verifying sender's certificate, and verifying sender's signature. EMAP protocol used to improve the performance of the wireless ad-hoc network.

Zero Knowledge Protocol

Zero Knowledge Proofs are cryptographic self authenticated protocols which allow A to demonstrate the knowledge of secret to B without revealing any useful information to third party.

If the node move from the network, and wants to return into the network by using re-authentication mechanism (ZKP). The re-authentication mechanism is used to avoid the unauthorized nodes.

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

Step 1: New node j 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 j sends m1 to node L and m2 to node M respectively.

Step 2 : The nodes L and M chooses 2 large prime numbers p1 = 2, q1= 3 and p2 = 3, q2 = 5, then calculates R1 = p1 * q1 = 6 and R2 = p2 * q2 = 15. Node L sends n1 to j and node M sends n2 to j.

Step 3: The new node j computes v1 and v2 such that, v1= $s1^2$mod R1. v2 =$s2^2$ mod R2=15 respectively, Now the 2 public keys of the node j are (v1, R1) = (3, 6) and (v2, R2) = (4, 15).

Step 4: The node j chooses two random numbers r1 = 4 and r2 = 3 and computes x1= $r1^2$ mod R1=4: x2= $r2^2$ mod R2=9. Now j sends x1 to L and x2 to M.

Step 5: The nodes L and M choose the challenge values e1 = 0, e2 = 1, then node L sends e1 to j and node M sends e2 to j.

Step 6: The new node j sends the random number r1 = 4 to node L. Then node L verifies that $r1^2$ = x1 mod R1=4 Likewise node j calculates y2 = r2s2 mod R2=6 and sends to the node M. Then node M verifies that $y2^2$= x2v2 mod R2 = 6.

Once the verification of the node j has been done by the nodes L and M node j allowed to communicate with the other nodes in the network.

V SYSTEM DESIGN

The original user first joined in the network by demonstrating the identity to neighbor node. Authentication server gets all details about the user and yields the ticket and session key to user. Using ticket and session key the user request the service to Service server. Service server gets the user details and verify with the Authentication server. If the verification is done, service server furnish the valuable services to trusted user.

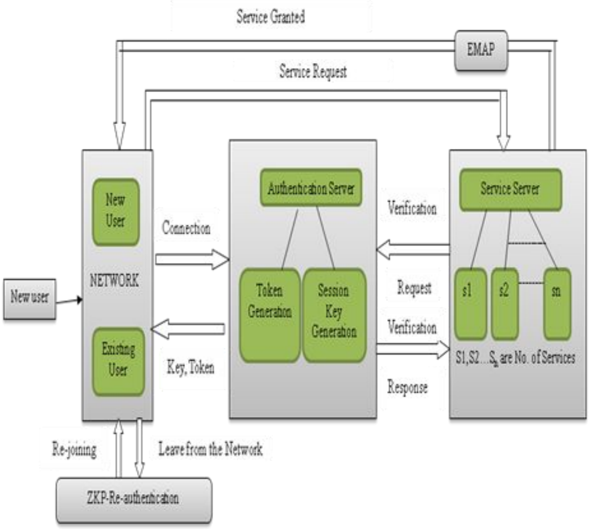


Fig 2. Overall System Architecture

If existing user wants to return into network, Zero knowledge proof protocol re-authenticate the existing user, to check whether the user is authenticated user or not, then rejoin the node into network. EMAP protocol reduces the authentication delay.

VI SYSTEM IMPLEMENTATION

Authentication

The original user first joined in the network by demonstrating the identity to neighbor node. Authentication server gets all details about the user and yields the ticket and session key to user. Using ticket and session key the user request the service to Service server. Service server gets the user details and verify with the Authentication server. If the verification is done, service server furnish the valuable services to trusted user. If existing user wants to rejoin the network, ZKP protocol re-authenticate the existing user, to check whether the user is authenticated or not, then rejoin the node to network. EMAP protocol reduce the authentication delay.

Authentication Server

If the authenticated server identify the legitimate user with encrypted data it gets all the client details, and grants the ticket and session key to client. Based on the ticket and session key the user request service to the Service server.

Ticket Generation

A token to each node in the network is generated by using its IP, ID, password as parameters. It is a 32 bit long character is generated by the algorithm specified. Once the ticket is generated, this ticket is encrypted using DES algorithm. The reversed last ‘n’ bits of the generated token are used as the actual token.

Session Key Generation

The token distribution involves generating a session key to uniquely identify a node that is connected to the network. A random number and a random string is generated for each node. The string is concatenated with a signature unique to the sender. The ASCII values of the concatenated string are added with the random number and the random number is appended to the end of the string. This is the session key. The session key is send to the each node. The set of session key and token is distributed to the node.

Service Server

The service server gets all the User details and verified with the Authenticated server. If the verification is done and the user is trusted user. Then the 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. This mechanism is used to avoid the harmful nodes to enter into the network.

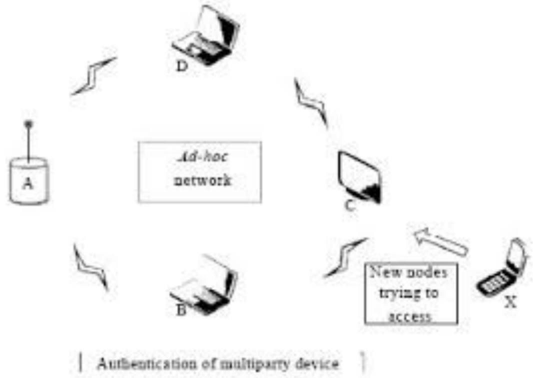

D
A
Ad-hoc network
C
B
New nodes trying to access
X
Authentication of multiparty device

Fig 3.Re-authentication

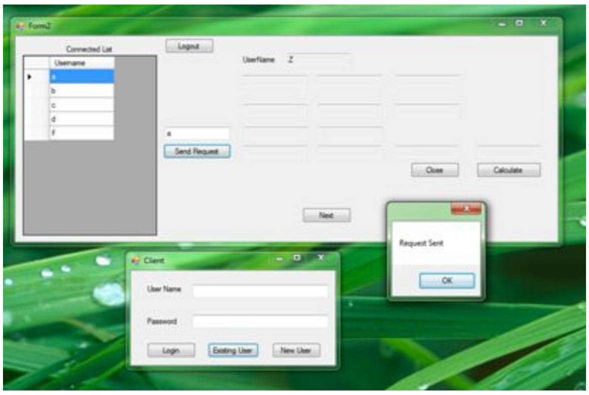
This mechanism is used mainly to avoid the malicious nodes to enter into the network.

Authentication Delay

EMAP uses a fast and secure HMAC function for an efficient revocation checking process. EMAP is used to reduce the authentication delay resulting from checking the

CRL. Authentication of Message is performed by three phases: checking sender's revocation status, verifying sender's certificate, and verifying sender's signature.

VII RESULTS AND DISCUSSION



	Username
▸	a
	b
	c
	d
	f

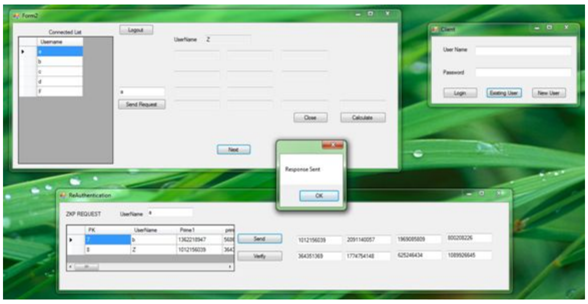
UserName Z

a

Request Sent

Fig 4. Conectionless node

In Fig 4. The node Z trying to rejoin into the network. Z sends a request to its neighbor node 'a'.



UserName Z

a

Response Sent

UserName a

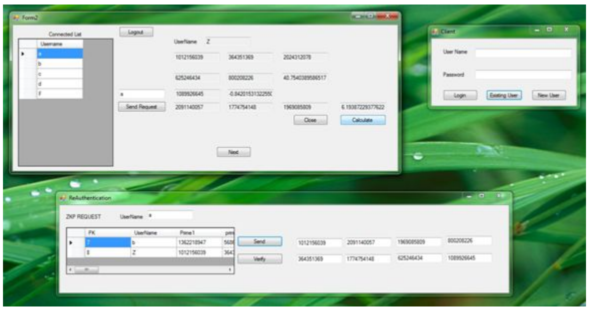
	PK	UserName	Prime1	prim
▸	7	b	1362218947	5608
	8	Z	1012156039	3643

1012156039 2091140057 1969085809 800208226

364351369 1774754148 625246434 1089926645

Fig 5.ZKP response

In Fig 5.The neighbor node 'a' sends a indirect value to node Z.



UserName Z

1012156039 364351369 2024312078

625246434 800208226 40.7540389586517

a 1089926645 -0.8420153132255

2091140057 1774754148 1969085809 6.19387229377622

UserName a

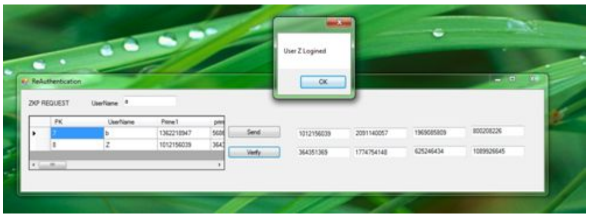
	PK	UserName	Prime1	prim
▸	7	b	1362218947	5608
	8	Z	1012156039	3643

1012156039 2091140057 1969085809 800208226

364351369 1774754148 625246434 1089926645

Fig 5. Verification

In Fig 5.The node Z receives a values and then send the secret values to 'a'



User Z Logined

UserName a

	PK	UserName	Prime1	prim
▸	7	b	1362218947	5608
	8	Z	1012156039	3643

1012156039 2091140057 1969085809 800208226

364351369 1774754148 625246434 1089926645

Fig 6.Rejoining

In Fig 6.The node 'a' verifies the secret. If the secret value is correct 'a' allow the node Z to rejoin into the network.

VIII CONCLUSION

The Zero Knowledge Proof (ZKP) protocol allows the creation and management of a spontaneous wireless ad hoc network. Secure protocol (ZKP) is used to sharing the services and re-authentication of existing nodes. Re-authentication scheme (ZKP) proposed for MANETs without the necessity of Central Authority using ZKP which do not reveal any useful information during the execution of protocol. 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. The security schemes included in the protocol allow secure communication between end users and reducing authentication delay. It ingest less energy, less power and less time for authentication process during protocol execution.

REFERENCES

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

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

[3] A Shidhani, V Leung, "Local fast re-authentication for 3G-WLAN interworking architecture". Security Commun Netw. 1(4), 309–323 (2008). doi:10.1002/sec.30

[4] AA Shidhani, VCM Leung, Pre-authentication schemes for UMTS-WLAN interworking. EURASIP J Wireless Commun Netw 2009. Article ID 806563 (2009)

[5] SH Lin, JH Chiu, SS Shen, Authentication schemes based on the EAP-SIM mechanism in GSM-WLAN heterogeneous mobile networks, in Proceedings of NCM 5th International Joint Conference on INC, IMS and IDC, pp. 2089–2094 (August 2009)

[6] Guangsong Li, Jianfeng Ma, Qi Jiang, Xi Chen, A novel re-authentication scheme based on tickets in wireless local area networks, J. Parallel Distrib. Comput. 71 (2011) 906-914.

[7] R. Lacuesta, J. Lloret, M. Garcia, and L. Pen alver, "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] L. Liu, J. Xu, N. Antonopoulos, J. Li and K. Wu, "Adaptive Service Discovery on Service-Oriented and Spontaneous Sensor Systems," Ad Hoc and Sensor Wireless Networks, vol. 14, nos. 1/2, pp. 107-132, 2012.

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

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

[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 and V.T Gaikwad "Authenticating Protocol for Spontaneous Wireless Ad Hoc Networks" vol. 2,issue 5. May 2013.

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

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

[17] K. Sahadevaiah and P.V.G.D. Prasad Reddy "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. 2011.

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

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

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

Ms. Soniya. M received her B.E degree in Computer Science and Engineering from Anna University of Technology, Trichirappalli in 2012. She is currently doing her M.E in the same stream in Pavendar Bharathidasan College of Engineering and Technology, Trichirappalli.

Ms. Sangeetha T received the BE degree in Computer Science from New Prince Shri Bhavani College of Engineering and Technology; Chennai in 2012.She is currently doing her ME in the same stream in Pavendar Bharathidasan College of Engineering and Technology, Trichirappalli.

Ms. Girija.K received the B.E degree in Computer Science and Engineering from S.K.P Engineering College, Tiruvannamalai in 2012. She is currently doing the M.E in the same stream in Pavendar Bharathidasan College of Engineering and Technology, Tiruchirappalli.

Mr. Sabarinathan.P received the B.E degree in Computer Science and Engineering from Annai Mathammal Sheela Engineering College, Namakkal in 2007 and received the M.E degree in the same stream in 2010 from Dhanalakshmi Srinivasan Engineering College, Perambalur. He is currently working as an Assistant Professor in Pavendar Bharathidasan College of Engineering and Technology, Trichirappalli with 3 years of teaching experience and his area of interest includes MANET and networks.